e-Discovery: Implications of FRCP changes on IT risk management

By Bradley J. Schaufenbuel

According to a recent survey of corporate attorneys by Pike and Fischer, only seven percent of respondents feel that their companies are ready to meet the e-discovery requirements of the recently updated Federal Rules of Civil Procedure (FRCP).

According to a recent survey of corporate attorneys by Pike and Fischer, only seven percent of respondents feel that their companies are ready to meet the e-discovery requirements of the recently updated Federal Rules of Civil Procedure (FRCP). Given that ESG Research estimates that 91 percent of organizations with a workforce over 20,000 employees have been through an electronic discovery event in the past twelve months, this statistic is truly astounding.[1] This article describes the FRCP and the recent changes made to it, explores the implications of these changes on the enterprise (with a focus on IT), and lays out a framework for identifying, assessing, and then addressing the risks associated with the facilitation of e-discovery requests under the new rules.

What is the FRCP?

The Federal Rules of Civil Procedure govern the activities of all federal civil courts. Civil procedure is the body of law that sets out the process that courts will follow when hearing cases of a civil nature (a *civil action*, as opposed to a criminal action). These rules govern how a lawsuit or case may be commenced, what kind of service of process is required, the types of pleadings or statements of case, motions or applications, and orders allowed in civil cases, the timing and manner of depositions and discovery or disclosure, the conduct of trials, the process for judgment, various available remedies, and how the courts and clerks must function.

Scope of the FRCP

Because the FRCP applies to all civil cases heard in federal court, any company that is or may be a party to a federal civil lawsuit (which includes almost any organization) should be familiar with the FRCP and prepared to handle discovery requests involving electronically stored information (ESI). Companies are especially susceptible to navigating complex e-discovery requirements for lawsuits involving employment discrimination, securities law violations, unfair trade practice stipulations, and intellectual property cases.

1 Brian Babineau, "Leveraging IT and Electronic Discovery Technology to Meet the Expected Challenges Posed by Recent Changes to the Federal Rules of Civil Procedure", Index Engines, Inc., (October 2006).

Companies are especially susceptible to navigating complex e-discovery requirements for lawsuits involving employment discrimination, securities law violations, unfair trade practice stipulations, and intellectual property cases.

Why the FRCP was amended

Traditionally, the rules of discovery were focused on tangible objects such as paper documents and physical evidence. Electronic information presented unique challenges to the legal system. The volume, transience, and persistence of electronic information differentiate it substantially from paper documents. Also, electronic information is often accompanied by metadata (information about information), which is not typically present in paper information. The application of discovery rules that were designed for paper documents to electronic information resulted in a confusing and often diverging body of common law (judicial rulings that become precedents for subsequent cases). In 2001, the Advisory Committee on Civil Rules formally recognized the problem and initiated a five-year study of the topic. The results of that study were a set of amendments to the FRCP that were designed to standardize and improve the efficiency of the electronic discovery process. These amendments were ratified by the U.S. Supreme Court on April 13th, 2006, and took affect on December 1st, 2006.

What is ESI?

Prior to 2006, the only reference to digital information in the Federal Rules of Civil Procedure was the inclusion of *data compilations* in discovery related rules. Even in this case, there was an expectation that electronic data compilations would be printed out on paper for delivery to opposing counsel. With the December 2006 revisions, this term was replaced with the term *electronically stored information* (ESI). ESI includes e-mail (and associated attachments), databases, text documents, spreadsheets, instant and text messages, and digital voice mail messages, to name a few. ESI can also include non-apparent information, or metadata, that describes the context of the information.

FRCP amendments explained

There are five key themes in the changes to the Federal Rules of Civil Procedure.[2] Firstly, the amendments define and treat electronically sensitive information differently than paper documents. Secondly, the amendments require the parties to a lawsuit to discuss issues that are unique to electronic discovery in initial conference. Thirdly, the amendments address inadvertent production of privileged or protected materials (records that are protected from disclosure to the other party based on the *attorney-client* and *work product* privileges). Fourthly, the amendments encourage a two-tiered approach to discovery which involves dealing with reasonably accessible information first and inaccessible data later. Finally, the amendments provide a *safe harbor* from sanctions by imposing a *good faith* requirement.

The following bullets explain specific rule changes in greater detail:[3]

- **Civil Rule 16 - Pretrial Conferences; Scheduling; Management** - This rule now establishes a process for the parties to a lawsuit and the court to address issues pertaining to the discovery and disclosure of electronically stored information.
- **Civil Rule 26 - General Provisions Governing Discovery; Duty of Disclosure**:
  - **Civil Rule 26(b)(2)** - The amendment requires the responding party to identify the sources of potentially responsive information that it has not searched or produced because of the costs and burdens of accessing the information. If the requesting party moves for production of such information, the responding party has the burden of showing the information is not reasonably accessible.
  - **Civil Rule 26(b)(5)** - The amendment provides a procedure for asserting privilege after production. Upon notification to the recipient of the producing party's post-production privilege claim, the recipient must return, sequester or destroy the information until the claim is resolved.
  - **Civil Rule 26(f)** - Also known as the *Meet and Confer* rule - This rule now requires the parties to a lawsuit to discuss issues of electronic evidence at the discovery planning conference. These issues include preservation of evidence, form of production, and the handling of inadvertent waivers of privilege (accidentally disclosing privileged evidence).
- **Civil Rule 33 - Interrogatories to Parties** - The amendment expressly provides that an answer to an interrogatory (written exchange of questions and answers between parties to a lawsuit) involving review of business records should involve a search of electronically stored information.
- **Civil Rule 34 - Production of Documents and Things and Entry Upon Land for Inspection and Other Purposes** - The amendment adds *electronically stored information* as a category of discoverable information (separate from *documents* and *things*). It also authorizes the requesting party to specify the form of production. Absent court order, party agreement, or a request for a specific form of production,

2 John A. Heer and Michael D. Osterman, "The Impact of the New FRCP Amendments on Your Business," *Osterman Research* (January 2007).

3 "Top Ten Tips to Prepare for FRCP Changes," *LexisNexis Applied Discovery Fact Sheet,* Applied Discovery, Inc., (2006).

Ignorance is no longer bliss.

a party may produce responsive ESI in the form ordinarily maintained or in a reasonably usable form. Rule 34 also includes the notion of sampling data from an entire data set to determine if additional discovery is warranted.

- **Civil Rule 37 - Failure to Make Disclosure or Cooperate in Discovery; Sanctions** - The amendment creates a *safe harbor* that protects a party from sanctions for failing to provide electronically stored information lost because of the routine, *good-faith* operation of the party's computer system.
- **Civil Rule 45 - Subpoena** - This amendment expands the scope of subpoenas to cover non-party production of electronic evidence. The subpoena may specify the form of production.
- **Form 35 - Report of Parties' Planning Meeting** - The amendment adds the parties' proposals regarding disclosure or discovery of electronically stored information to the list of topics to be included in the report to the court.

Organizational impacts of the FRCP amendments

The most significant organizational impacts of the FRCP amendments include:

- **e-discovery time frames:** Organizations no longer have the luxury of virtually limitless amounts of time in which to respond to e-discovery requests. The meet and confer session must take place at least 21 days before the court holds a scheduling conference or enters a scheduling order, which resolves various issues related to discovery and sets a schedule for completion of discovery. Under Civil Rule 16(b), the scheduling conference must occur, or the judge must enter a scheduling order, within 120 days after the complaint has been served on the defendant. That means that organizations have, at most, 99 days to locate electronically stored information that may be subject to discovery.
- **Ignorance is no longer bliss:** Organizations cannot rely on a poorly organized/ad-hoc response to e-discovery requests. Given the need to directly discuss issues of existence, accessibility and form up front, organizations simply must know where and how electronic information is stored and the costs of production prior to the commencement of litigation.
- **Multi-disciplinary approach:** Attorneys can no longer throw individual e-discovery requests and litigation hold demands *over the wall* to the folks in IT. Records management professionals, IT personnel, compliance experts, and legal counsel all need to work together to ensure that a comprehensive framework is developed for handling e-discovery requirements properly and to oversee its ongoing operation.

Consequences of not addressing the e-discovery challenge

If an organization forgoes e-discovery preparation efforts prior to the commencement of actual litigation, the consequences could be severe. Examples include:

- **Adverse inference jury instruction:** If electronic evidence is not produced in a timely manner, a judge may instruct the jury to assume that the missing evidence would have been *adverse* to the party that failed to produce it. This will greatly diminish this party's chances of legal success. Two highly visible examples include *Zubulake v. UBS Warburg* and *Coleman v. Morgan Stanley.* The defendant financial institutions in both lawsuits lost their cases due to their failure to adequately produce e-mail evidence, and the resulting assumption that evidence was willfully destroyed or withheld. Laura Zubulake, a former UBS employee, was awarded $29 million in 2005 in her sexual discrimination lawsuit. And billionaire Ronald Perelman was awarded $1.45 billion in 2005 based on his claim that Morgan Stanley defrauded him in the 1998 sale of his company, camping goods manufacturer Coleman.[4]
- **Fines and penalties:** Delays in responding to a request for information can be costly. In one case, *Serra Chevrolet v. General Motors*, 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.[5]
- In addition to legal setbacks, responding to e-discovery requests in an unplanned and ad-hoc manner can result in significant business interruptions. Resources may need to be diverted from core business functions to litigation support. In order to meet the strict deadlines, the organization may find it necessary to pull valuable resources off critical business projects and place them onto e-discovery tasks.

Identifying and assessing e-discovery risks

An organized approach is needed to identify and assess an organization's e-discovery risks. The following checklist is designed to help an IT risk management professional with this task.

e-Discovery Readiness Assessment Checklist

Policy and Awareness

- Does the organization have a robust records management policy?

4 Cory Levine, "Deliberating on e-Discovery and the Changes to the FRCP," *Wall Street & Technology Magazine,* (CMP Media, February 13th, 2007).

5 Roger Matus, Sean True, and Chuck Ingold, "The New Federal Rules of Civil Procedure: IT Obligations For Email," *InBoxer, Inc.,* (2006).

- Has the records management policy been communicated to all personnel?
- Is the records management policy enforced?
- Does the records management policy include retention schedules for digital and non-digital information?
- Does the records management policy cover all phases of the information life cycle?

Information Technology

- Does the organization maintain a digital information inventory?
- Does the organization know where its information assets are located (including duplicates, back-ups, etc.)?
- Does the organization's technology automate/support compliance with its records management policies?

Roles and Responsibilities

- Does the organization define roles and responsibilities for information stewards/data owners?
- Does the organization define roles and responsibilities for information custodians/caretakers?
- Has the IT department assigned a knowledgeable point person for coordinating e-discovery requests?

Process and Capabilities

- Does the IT department have a formal written procedure for responding to e-discovery requests?
- Does the IT department have a formal procedure for retaining information in response to a *legal hold*?
- Does the IT department have access to e-discovery searching and forensics expertise (on-staff or off)?

The greater the number of affirmative answers, the more adequately equipped the organization is to effectively and efficiently handle e-discovery requests.

Addressing e-discovery related risks

Given the stringent requirements of the amended Federal Rules of Civil Procedure and the consequences of being unable to adhere to the discovery time frames it lays out, an organization's IT department simply must be better prepared for and more responsive to e-discovery requests. To address the risks associated with the inability to produce electronic information in a timely manner, organizations need a robust action plan. The following steps should be undertaken as part of a comprehensive e-discovery preparation initiative:

- **Rally the troops:** Create an e-discovery task force to oversee organizational readiness and litigation support efforts. This task force should include members of the legal department, IT, records management professionals, compliance officers, enterprise risk managers, and business folks. This is not simply an IT issue and should not be treated like one.

The key to being able to qualify for the FRCP safe harbor is repeatability.

- **Get organized:** Take an information inventory. Record where data is located, how it is stored, and how it can be retrieved. Know the cost (in time and resources) of restoring it. Know who the owners and custodians of information are. By knowing where electronic evidence lies, a firm can minimize its search time and volume and dramatically reduce the materials passed on for legal review, as well as the subsequent costs for that review. The more material that the legal review team has to sift through, the longer it will take, and with lawyers' rates in the hundreds of dollars per hour, this type of litigation support is the largest addressable cost in e-discovery, asserts Barry Murphy, a senior analyst with Forrester Research (Cambridge, Massachusetts).
- **Revamp (or create) records management policies:** If an organization's records management policies are non-existent or outdated, it is time to revisit them. Make sure that they contain all of the elements listed in the checklist above. More importantly, make sure that they are signed off by senior management, supported by IT systems, and consistently followed.
- **Put repeatable practices in place:** FRCP Rule 37(f) protects companies from sanctions for deleting records as part of "routine, good-faith operation." This so-called safe harbor provision protects companies that delete records as part of ordinary business activities. The key to being able to qualify for the FRCP safe harbor is repeatability. If the organization has a destruction policy in place that is not met on every single record, the courts may levy penalties based on the fact that if one record was not subject to a company's destruction policy, many more may have unknowingly been preserved as well, industry sources say. Further, if a single backup tape is accessed for electronic records against policy, then the policy becomes moot and all backup tapes may become admissible evidence.
- **Be prepared:** Put processes and procedures in place for responding to preservation requests and for implementing *litigation holds*. Oftentimes electronically stored information is automatically destroyed on a periodic basis through back-up tape recycling, scheduled purges, etc. To make sure that data related to pending litigation is not destroyed after a litigation hold is announced, organizations should have a predefined procedure to quickly cancel all scheduled destruction of data that is any way related to the case.
- **Think ahead:** Start planning for the long term. Incorporate e-discovery requirements into future technology implementation projects within the information life cycle management space.

Risks associated with IT facilitation of e-discovery can be mitigated to a great extent without a substantial investment in new technology.

Technology solutions

Despite vendor claims to the contrary, most of the risks associated with IT facilitation of e-discovery can be mitigated to a great extent without a substantial investment in new technology. That being said, investments in the following technology categories can provide significant benefit to an organization's e-discovery efforts:

- E-mail archival and search products: Since e-mail is increasingly becoming the subject of electronic discovery requests and for most organizations represents the most significant challenge in terms of production, products that help organizations to capture, archive, and retrieve e-mail messages and attachments can greatly aide the e-discovery process.
- Information Lifecycle Management (ILM): According to the Storage Networking Industry Association (SNIA), ILM is "comprised of the policies, processes, practices, and tools used to align the business value of information with the most appropriate and cost effective IT infrastructure from the time information is conceived through its final disposition. Information is aligned with business processes through management policies and service levels associated with applications, metadata, information, and data."
- Enterprise Content Management (ECM): According to the Association for Information and Image Management (AIIM) ECM is "the technology used to capture, manage, store, preserve, and deliver content and documents related to organizational processes. ECM tools and strategies allow the management of an organization's unstructured information, wherever that information exists."

Outsourcing

Sometimes it may not make sense to handle e-discovery requests in-house, especially if the required expertise is lacking within internal staff, e-discovery processes are largely undefined, there aren't enough resources to spare to carry out the required activities, or significant portions of the IT infrastructure have been outsourced to a third party. Quite simply, a company should outsource its e-discovery tasks if it is not ready to address them itself internally. If enabling technology is involved, it is not always necessary to deploy that technology in-house, especially if the company is not prepared to manage it. Information archiving and searching activities are especially well suited for outsourcing.

Conclusion

The recent amendments to the Federal Rules of Civil Procedure will have a huge impact on the e-discovery practices of organizations of all sizes and types. These changes may pose significant risks to the IT departments of organizations who are ill-prepared to support litigation involving electronic evidence. However, if properly identified, assessed, and addressed, these risks can be mitigated to an acceptable level.

Other works consulted

—Kenneth J. Withers, "Electronically Stored Information: The December 2006 Amendments to the Federal Rules of Civil Procedure," *Northwestern Journal of Technology and Intellectual Property*, Volume 4, Number 2, Pages 171-211, (2006).

—Stacy Jackson, "Getting Ahead of the Federal Rules Changes," *Law Journal Newsletters, e-Discovery Law & Strategy*, (LM Properties, Inc., February 2006).

—AHIMA e-HIM Work Group on e-Discovery, "New Electronic Discovery Civil Rule," *Journal of AHIMA*, Volume 77, Number 8, Pages 68A-H, (September 2006).

—Michele C.S. Lange, Esq., "New FRCP Rules: What Does it Mean for You," *Minnesota State Bar Association Computer and Technology Law Blog* , (December 1, 2006).

—Joel Wuesthoff, "Managing the e-Discovery Engagement Under the Revised Federal Rules of Civil Procedure (FRCP)," (Ibis Consulting, Inc., 2006).

—Robert B. "Barry" Wiggins, "e-Discovery: A Practical Guide to What You Need to Know," *Morgan Lewis Resources Legal Logistics*, (July 19, 2006).

—Joel Wuesthoff, "The Federal Rules of Civil Procedure (FRCP) Changes – The Top Ten Things to Know about Them and Electronic Discovery," (Ibis Consulting, Inc., July 2006).

—Russ Yoshinaka, Esq., "Best Practices for Ensuring You – and Your Data – Are Prepared for the Changes to the Federal Rules of Civil Procedure (FCRP)," (Zantaz, Inc., 2006).

—Deborah Johnson, "Ready or Not, Here They Come: The New Rules for e-Discovery Answer Some Old Questions and Pose New Ones," (Orchestria, Inc., 2007).

—Ed Moyle, "IT & Legal: Planning Together for e-Discovery," "Ask the Compliance Expert," *Compliance Resources*, (Fios, Inc.,2006).

—Karen A. Schuler, "Best Practices Discovery Checklist – The Federal Rules of Civil Procedure Amendments," (Onsite3 Corporation, January 2007).

About the Author

Bradley J. Schaufenbuel, CISSP, CISM is Senior Manager of IT Risk at a global financial services company and a member of the Chicago chapter of ISSA. He can be reached via e-mail at bradley@schaufenbuel.com.