The Federal Rules of Civil Procedure

Meeting the IT and Legal Challenges of the New E-Discovery Rules

1. Executive Summary

Recent changes to the Federal Rules of Civil Procedure (FRCP) require that legal and IT departments work more closely than ever before. The new rules require organizations to understand and manage information in a new way that bridges the gap between the business view of information and the IT view of information. To accomplish this, among other things, organizations should create a detailed sources profile of their Electronically Stored Information (ESI). This will help organizations identify the sources that they will produce information from during e-discovery. To get started, organizations should evaluate their current approach to email management and archiving.

2. Introduction

Organizations today face new information management challenges from many different sources. The volume of information generated across the enterprise is growing, its value is increasing, and the pressure to make it more available – at lower and lower costs – is a reality that CIOs and IT departments face daily. At the same time, organizations face new legal and regulatory requirements that create novel corporate governance, compliance, organizational, and technological challenges.

The way that enterprises create, use, disseminate, and rely upon information technology and electronic information has not gone unnoticed by lawmakers, regulators, and the courts. In fact, in many ways, the information technology world is becoming a regulated world, with legal requirements beginning to impact the complete lifecycle of digital information use and management.

Nowhere is this truer than in the world of electronic discovery. The process of finding, preserving, and producing electronic information in the context of lawsuits, investigations, audits and other matters forces – for better or for worse – cooperation and collaboration between very different groups with very different mandates – and the fate of the organization itself can rest on how well they manage this complex relationship.

May 2007

WHERE LAW & TECHNOLOGY MEET

KAHN CONSULTING INC.

P.O. BOX 1045 • HIGHLAND PARK IL • 60035
PHONE: 847.266.0722 • FAX: 847.266.0734 • EMAIL: INFO@KAHNCONSULTINGINC.COM

While e-discovery has been a hot topic in the business, legal and IT worlds for some time, it has lately taken on a new dimension. Recent amendments to the Federal Rules of Civil Procedure that govern e-discovery require unprecedented alignment between legal and IT departments, and fundamentally require organizations to view e-discovery as a critical **organizational capability**, not simply a problem owned solely by the legal department.

This paper examines the new rules and evaluates their impact on today's organizations as they prepare for, and respond to, the new world of electronic discovery.

3. Introduction to the New E-Discovery Rules

3.1 What are the Federal Rules of Civil Procedure?

"The amendments to the Federal Rules of Civil Procedure for Electronic Discovery will have the greatest impact on organizational behavior and investment priorities on information management for compliance in the next 18-24 months."

IDC/Kahn Consulting, Inc. Survey, February 2007[1]

The Federal Rules of Civil Procedure (FRCP) are court rules for civil lawsuits (i.e., non-criminal cases) conducted in US federal courts.[2] The rules are divided into thirteen major sections that address the mechanics of the civil legal process, such as how litigation commences, how litigants interact with the court, and the collection and handling of evidence.

After several years of discussion and drafting, the FRCP were significantly amended to address issues specific to the treatment of electronic information (referred to as "Electronically Stored Information," or ESI, by the Rules). After subsequent approval by the US Supreme Court, the amendments went into effect on December 1, 2006.

So, if the FRCP are simply rules for lawsuits, then why should a CIO or IT professional care about them? To be sure, the majority of the FRCP address issues that only have a direct impact on lawyers and the way they do their jobs when it comes to litigation. However, the FRCP also contain many rules regarding the way that information must be managed when it is used as evidence. Fifty, or even fifteen years ago, when most of that evidence was in paper form, its management generally did not require special expertise or technology. However, today, when most of the evidence is in electronic form, compliance with the FRCP is virtually impossible without the involvement of the IT department. In other words, the FRCP are important to IT departments because they dictate the expectations that the legal department – and the organization itself - will have regarding ITs' capabilities.

3.2 Why were the FRCP Amended?

The purpose of the amendments is to "reduce the costs of discovery, to increase its efficiency, to increasing uniformity of practice . . ."

Civil Rules Advisory Committee Report[3]

Since the FRCP were originally enacted in 1938 (at the direction of Congress), they have been amended dozens of times to address the ever-changing legal landscape.[4] They were first amended in 1970 to address electronic data, for example.[5]

Beginning in the late 1990s, the committee responsible for the FRCP began to consider further amendments to address emerging issues regarding e-discovery. Many cases were beginning to address the issue, with widely divergent and "not consistent"[6] outcomes. At the highest level, the Committee cited three reasons that rules specific to electronic evidence were required; three reasons why "the discovery of electronically stored information raises markedly different issues from conventional discovery of paper records," as outlined below:

- The sheer volume of ESI potentially discoverable in any given case.
- The ease with which ESI can be changed or deleted.
- The reliance of ESI on IT systems for access and readability.[7]

As a result of these and other factors, the Civil Rules Advisory Committee undertook to amend the FRCP to address ESI – a process that bore fruit in 2006.

4. Responding to the New E-Discovery Rules

4.1 Overview

The new e-discovery rules address many different aspects of the legal process surrounding e-discovery.[8] There are many excellent legal resources available that evaluate the rule changes in detail, and provide information regarding general e-discovery legal obligations.[9] The intent of this section (and indeed this paper) is not to provide a legal dissection of the new rules, but rather to provide high-level insight into the impact of the new rules on IT, business, and legal management of the e-discovery process.

Past or Present?

When the new e-discovery rules were enacted, it was made clear that they would apply not only to matters initiated after that date but also to certain "proceedings then pending." Legal departments should review pending matters to evaluate any impact that the amendments may have on them. Although it is unclear exactly how the courts may deal with this issue, at least one court has ruled that the amendments would apply only to future discovery in a pending case, and not retroactively to production that was carried out prior to December 1, 2006.

4.2 ESI Sources Profiling

Taken together, several sections of the new e-discovery rules demonstrate that organizations require a new kind of understanding about the electronic information they store and manage.

For example, consider an e-discovery request for, "all email messages between X dates and containing X keywords; all manufacturing and testing data related to X product; and all revenue information related to X product."

In many organizations, a lawyer faced with such a request would have a difficult time quickly and efficiently finding, retrieving, reviewing, and producing the ESI requested. Asked about manufacturing data, for example, a business manager might respond with a business function view that sheds little light on the actual systems that control the information "behind the scenes." The stratification and organizational structure of IT might make it difficult for the lawyer to match the information provided by the business manager to that provided by the IT manager. In many cases an IT professional may know relatively little about the business function of the information in the systems he/she manages, or at least may know only what is required to manage the system. Within the IT function itself, functional divisions may further complicate the attorney's quest for clarity. For example, the person responsible for the email servers might know little about how the system is archived, and vice versa.

In sum, most organizations have a gap between understanding their ESI from a business perspective and understanding it from an IT perspective. This is a gap that organizations frankly need to close in order to comply with the new e-discovery rules.

4.2.1 Why Sources Information Is Critical

This gap in understanding is critical because the new e-discovery rules require organizations to perform various activities cannot be properly performed without detailed ESI source information.

More specifically, the new rules require organizations to:

1) Specify the systems containing ESI that are "reasonably accessible" versus those that are "not reasonably accessible," and thus may not be subject to the production requirements, because of "the burdens and costs required to search for, retrieve, and produce whatever responsive information may be found."[12]
2) "[I]dentify, by category or type, the sources containing potentially responsive information that it is neither searching nor producing"[13] because it has deemed such information to be not reasonably accessible.
3) Enable the opposing party to "inspect, copy, test, or sample" ESI as required by the court, and to translate, "if necessary, [that information] into reasonably usable form"[14]

In addition, without a detailed ESI sources profile, legal departments will have a difficult time complying with several requirements of the new rules. A detailed profile of ESI sources is essential to the legal department so that it can:

1) "[D]evelop a discovery plan that takes into account the capabilities of their computer systems."[15]
2) Prepare to "meet and confer" with the opposing side in litigation regarding discovery.[16]

3) "[B]ecome familiar with [relevant] systems," so it can "discuss those systems" with the opposing side during the course of discovery.[17]

4.2.2 ESI "Sources" Best Practice Recommendations

Legal and IT need to work together to develop a detailed profile of ESI Sources that includes the following information, at a minimum.

- The types of ESI commonly requested in litigation.
- The names, titles, and contact information for the business and IT owners of the systems that manage and/or house ESI.
- The physical locations of IT systems that contain ESI.
- The preferred system or systems for producing ESI of a given type, including the rationale as to why one system is preferred over others (i.e., it is more readily accessible, contains authoritative copies of ESI, etc.)
- The format of the ESI in the system.
- A listing of systems containing ESI which will not be routinely preserved or produced from, and the rationale behind the list.
- Information about techniques, issues, best practices to be used when preserving or producing from specific systems.
- Architectural and network topology information as appropriate.

Interpretation Issues

Many provisions of the new rules provide judges with significant leeway to interpret and apply the rules in specific cases. Because of this, there are widely divergent opinions about what the impact of many of the rules will be "in the real world." For this reason, law departments should pay close attention to emerging case law.

In one recent case, the court applied the new rules to production of ESI.[18] In the case, the plaintiffs had produced many electronic documents by printing them, scanning them, and producing the resultant images. The defendants argued that the loss of searchable metadata resulting from this process "contravene[d] the intent" of the new rules. In examining the issue, the court noted that, although the rules allow production in forms other than the form the data is normally kept in, it "should not produced in a form that removes or significantly degrades" its searchability. In the court's view, the production process used by the plaintiff ran afoul of the latter principle, and as such the court left the door open to mandating a different process moving forward.

4.3 The Legal Hold Process and Production v. Preservation

Although the new e-discovery rules did not fundamentally change the duty to preserve ESI prior to e-discovery, the new rules highlight a critical difference between **production** obligations and **preservation** obligations that IT departments must understand, especially when it comes to the identification of ESI sources.

The law is clear that the obligation to preserve information does not begin only once an organization has received formal notification from a court or regulator. Rather, an organization must suspend any and all disposition or alteration of information once a lawsuit, audit, or investigation is threatened, imminent, contemplated, or pending.

An obligation to **preserve** ESI "may arise from many sources, including common law, statutes, regulations, or a court order in the case."[19] Organizations typically fulfill this obligation in part through the Legal Hold process. An obligation to **produce** ESI, however, occurs in the context of a matter, following a request or order. In other words, regardless of whether or not any party or body has asked an organization to preserve and/or produce information, it may have the legal obligation to preserve it, and ensure that it is not destroyed, altered, and so on.

So, what is the significance of this distinction? There are two key issues deriving from the new discovery rules.

4.3.1 Inaccessible Sources

> *"Whether good faith would call for steps to prevent the loss of information on sources that the party believes are not reasonably accessible . . . depends on the circumstances of each case."*
>
> *Civil Rules Advisory Committee Commentary*[20]

The new rules may obviate the need, in some circumstances, for organizations to produce ESI from sources that are "not reasonably accessible."[21] This may lead some organizations to assume that they therefore do not have to make such sources subject to a Legal Hold, when in fact the concept of inaccessibility is one that generally applies to the discovery phase of a matter, and not to the preservation obligation.

For example, organizations should not assume that they have no obligation to preserve information on backup tapes prior to the discovery phase of a trial because they are planning on producing the same information from another source. Rather, the organization should conduct a detailed legal analysis of the sources of potentially responsive information and prepare a Legal Hold and discovery strategy that ensures that both preservation and production obligations can be met.

4.3.2 Good Faith Operations

> *"Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system."*
>
> *Civil Rules Advisory Committee Commentary*[22]

In the past, organizations have been sanctioned or otherwise faced undesirable consequences when they allowed responsive ESI to be destroyed or altered through the routine operations of the systems that managed or housed the information. For example, in the case of Applied Telematics v. Sprint, an organization was sanctioned because it allowed ESI to be "destroyed during routine deletions of computer information," even though such deletions were not done "willfully, maliciously, or in bad faith."[23]

The new e-discovery rules address this issue head on, and create what some commentators have called a "safe harbor" that may protect organizations from sanctions resulting from what would otherwise be considered good faith, routine operation of computer systems.

However, organizations should sail cautiously, if at all, into this "safe harbor," as it is currently unclear how this rule will be applied by the courts. In fact, the relevant Committee Commentary states that good faith may involve "[intervening] 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," and further states that the rules do not allow a party to "exploit the routine operation of an information system to thwart discovery obligations by allowing that operation to continue in order to destroy specific" ESI.

4.3.3 Preservation and Legal Hold Best Practice Recommendations

- Develop a comprehensive Legal Hold strategy that clearly identifies triggers, timelines, responsible parties, responsive systems, and procedures for disseminating Hold Notices and related communications to all affected parties.
- Ensure that Legal Hold procedures consider the preservation of information that might otherwise be designated as source the organization does not plan to produce from.
- As part of a Legal Hold strategy, identify systems that contain potentially responsive ESI and document their operational procedures, including business continuity and archiving schedules.
- Ensure that Legal and IT are in sync on the operation of backup and archiving operations, including the overwriting of backup media and backup schedules.

5. Email Archiving Considerations

"Respondents appear to be confused about the critical differences in the technology capabilities between backup and archival solutions. . . The inability to recognize these critical capabilities could potentially impact a company's ability to identify and produce the relevant information under the protracted timelines of e-discovery and compliance audits."

IDC/Kahn Consulting, Inc. Survey, February 2007[24]

It is well known that email provides one of the most active battlegrounds when it comes to e-discovery. This is not surprising given its incredible volume, the plethora of candid communications, and the tendency of many organizations to manage email outside of regular records and information management programs. In any case, most organizations grappling with the new e-discovery rules would do well to start their efforts by getting their email environment in order. More specifically, the way in which organizations retain, preserve, and archive email can play a major role in e-discovery success or failure.

With that in mind, here are some considerations for evaluating and managing email archiving environments.

1) **Backup versus Archive**. Ensure that systems designed for business continuity of the email system are used for business continuity and that systems designed for archiving email are used for archiving email. In other words, backup tapes should not be used for business archiving purposes. One of the best things an organization can do in the short term is to address this issue with the goal of avoiding the need

to go to backup tapes for e-discovery purposes. This will involve addressing legacy tapes (to the extent they exist) while ensuring that existing preservation obligations are met; as well as addressing the separation of backup and archiving environments moving forward.

2) **Administrative Interfaces**. Email archiving systems should enable a robust administrative interface adequate to support e-discovery. The interfaces should be functional for legal professionals and support the searching, filtering, workflow, and other capabilities required to support e-discovery. In addition, email archiving systems should provide robust integration capability with systems used to support and manage e-discovery process, such as search tools and case management systems. Archiving systems that support open standards may provide broader functionality in this regard.

3) **Architecture**. Organizations must be clear about the desired role of their email archive. Is it the system from which they plan to produce email (i.e., as opposed to the online mail servers or other systems), or is there a combined production strategy requiring production from other systems? Clarity here is critical for e-discovery "meet and confer" and other purpose. If the archive will be the primary source for email ESI, then it must support (or otherwise connect to) robust e-discovery functionality, including search, forensically-sound capture and preservation.

4) **Archival Storage Performance.** Storage systems used for archiving must be able to support the level of performance required for production of ESI, while maintaining performance levels for routine business use of the system. Production of ESI may require searching, processing, copying, and production of massive quantities of information in short periods of time. Failure to meeting production timelines established by courts and regulators can result in fines and other sanctions.

5) **Authenticity of archived information.** Archives must provide the ability to protect the integrity and authenticity of the information they manage. The evidentiary quality of ESI is largely dependant upon the systems that house and manage the information. As such, organizations should evaluate storage technologies designed to protect the authenticity of information while preserving performance levels, such as Write Once, Read Many (WORM) capability on magnetic disk.

6. Conclusion

The new e-discovery rules require an unprecedented alignment of the legal and IT functions within today's organizations. Organizations simply cannot hope to fulfill their e-discovery obligations without this alignment. Although many organizations will undoubtedly feel some growing pains associated with this alignment, it is important for organizations to take the long view. After all, perhaps the greatest long-term benefit of this alignment is the potential for a much-improved information management foundation – one that is oriented not only around legal requirements but also business goals. This is a foundation that that will help organizations to not only respond to the new e-discovery rules, but to other current and future rules, regulations, and laws, and moreover, to better leverage information to achieve their strategic business goals.

7. Endnotes

[1] "Highlights from the 2006 Compliance East Survey: What Do End Users Need to Know?" International Data Corporation, February 2007.

[2] Note that some state courts have similar rules that, in many cases, are substantially similar to the Federal Rules. In addition, several states have taken action to ammend state rules and provide guidelines to address e-discovery.

[3] Civil Rules Advisory Committee Report, Page 25.

[4] Charles Wright and Arthur Miller, "Federal Practice and Procedures," 2002.

[5] Civil Rules Advisory Committee Report,Page 25.

[6] Civil Rules Advisory Committee Report,Page 23.

[7] Civil Rules Advisory Committee Report,Page 23-24.

[8] Throughout this paper, the phrase "new e-discovery rules" is used to refer to the Dec. 1, 2006 amendments to the Federal Rules of Civil Procedure.

[9] The Kahn Consulting, Inc. Library provides several such resources. Available at: http://kahnconsultinginc.com/library/library.html

[10] Rule Amendment Order P 3.

[11] In re Payment Card Interchange Fee & Merchant Discount Antitrust Litigation, 2007 U.S. Dist. LEXIS 2650 (E.D.N.Y. Jan. 12, 2007).

[12] FRCP Rule 26(b)(2)(B) and Committee Commentary.

[13] FRCP Rule 26(b)(2)(B) Committee Commentary.

[14] FRCP Rule 34(a).

[15] FRCP Rule 26(f) Committee Commentary.

[16] FRCP Rule 26(f) Committee Commentary.

[17] FRCP Rule 26(f) Committee Commentary.

[18] In re Payment Card Interchange Fee & Merchant Discount Antitrust Litigation, 2007 U.S. Dist. LEXIS 2650 (E.D.N.Y. Jan. 12, 2007).

[19] FRCP Rule 37(f) Committee Commentary.

[20] FRCP Rule 37(f) Committee Commentary.

[21] FRCP Rules 26(b)(2)B).

[22] FRCP Rule 37(f) Committee Commentary.

[23] Applied Telematics v. Sprint, 1996 U.S. Dist. LEXIS 14053 (D. Pa.).

[24] "Highlights from the 2006 Compliance East Survey: What Do End Users Need to Know?" International Data Corporation, February 2007.

8. About Kahn Consulting

Kahn Consulting, Inc. (KCI) is a consulting firm specializing in the legal, compliance, and policy issues of information technology and information lifecycle management. Through a range of services including information and records management program development; electronic records and email policy development; Information Management Compliance audits; product assessments; legal and compliance research; and education and training, KCI helps its clients address today's critical issues in an ever-changing regulatory and technological environment. Based in Chicago, KCI provides its services to Fortune 500 companies and government agencies in North America and around the world. Kahn has advised a wide range of clients, including Time Warner Cable, Ameritech/SBC Communications, the Federal Reserve Banks, International Paper, Dole Foods, Sun Life Financial, Kodak, McDonalds Corp., Hewlett-Packard, United Health Group, Prudential Financial, Motorola, Altria Group, Starbucks, Mutual of Omaha, Merck and Co., Cerner Corporation, Sony Corporation, and the Environmental Protection Agency. More information about KCI, its services and its clients can be found online at: www.KahnConsultingInc.com.

WHERE LAW & TECHNOLOGY MEET

KAHN
CONSULTING INC.

www.KahnConsultingInc.com info@KahnConsultingInc.com 847-266-0722

P.O. BOX 1045 • HIGHLAND PARK IL • 60035
PHONE: 847.266.0722 • FAX: 847.266.0734 • EMAIL: INFO@KAHNCONSULTINGINC.COM