

Why You Need to Understand The New FRCP Amendments

An Osterman Research White Paper

Published November 2007



Why This White Paper Will be Worth Your Time

The new amendments to the Federal Rules of Civil Procedure (FRCP) that went into effect on December 1, 2006 will have a major impact on the way that organizations store, manage and dispose of electronic data.

Unfortunately, most organizations do not understand the new rules well enough to realize the ultimate impact that they will have on their data retention practices. Further, a survey conducted by another firm found that only one out of 14 corporate counsel attorneys believe their companies are prepared for the new amendments, while less than two months before the amendments went into effect more than 50% of these attorneys were not even aware of them.

The new amendments will present significant challenges to organizations of all sizes on several levels:

- Corporate legal counsel will need to learn what impact the FRCP changes will have on their organizations.
- IT managers will wrestle with the potentially significant investments in technology that will be required to adequately preserve electronic data.
- Senior managers will need to evaluate and improve their corporate governance policies and procedures to meet the new requirements.

What are the Federal Rules of Civil Procedure?

The FRCP are a set of mandatory, court-imposed rules that are focused on managing court procedures used in civil suits in United States district courts. While the United States Supreme Court is responsible for creating new amendments within, and interpretations of, the FRCP, the United States Congress is responsible for approving these rules and the changes made to them. It is important to note that although the FRCP amendments apply only to federal lawsuits at this point, it is very likely that most states will adopt their own versions of the amendments during the next few years.

A number of important revisions to the FRCP took effect on December 1, 2006. These changes represented several years of debate at various levels within the courts and elsewhere in government. These rules will have important impacts on electronic discovery and the management of

The newly adopted amendments to the Federal Rules of Civil Procedure (FRCP) will have a major impact on the way that organizations manage electronic data.

electronic data within organizations that operate in the United States, even if they are based elsewhere. In short, the changes to the FRCP require organizations to manage their data in ways that will allow the data to be produced in a timely and complete fashion when necessary, such as during legal discovery proceedings.

There are Several New Amendments to the FRCP

The amendments to Rules 16, 26, 33, 34, 37, 45 and revisions to Form 35 are aimed at the newly stated concept of electronically stored information (ESI). The amendments focus on the important issues presented by ESI:

- ESI is normally stored in much greater volume than are hard copy documents.
- ESI contains information metadata – information that is not stored directly in the content itself – that describes the context of the information and provides other useful and important information. For example, metadata might include reviewer annotations about a word processing document or spreadsheet that is not actually included in the data itself.

The importance of metadata was acknowledged in Comment 12.a. to Principle 12 of The Sedona Principles for Electronic Document Production (2005), which states, “. . . if the producing party knows or should reasonably know that particular metadata is relevant to the dispute, it should be produced.”

- ESI is dynamic, in many cases modified simply by turning a computer on.
- ESI can be incomprehensible when separated from the systems that created it.

The changes to the FRCP reflect the US government's acceptance that discovery of email and other ESI is now a routine aspect of just about every litigated case. However, email and other electronic content has been discoverable for some time – the new amendments simply formalize and recognize the growing importance of ESI.

The amendments treat ESI differently than non-electronic information. The changes also:

Unlike industry-specific rules, the FRCP apply to any organization that might be involved in civil litigation. If an organization can have a civil lawsuit filed against it, then the FRCP should figure prominently in that organization's data management strategy.

- Require parties now to discuss and attend to, early in any proceeding, electronic discovery during their initial Rule 16 pretrial conference.
- Address inadvertent production of privileged or protected materials.
- Encourage a two-tiered approach to discovery – parties should deal with reasonably accessible information and then later with data that is not readily accessible.
- Apart from exceptional circumstances, provide a safe harbor from court-imposed sanctions when ESI is lost during routine and good faith operations of an electronic information system.

In short, if an organization can have a civil lawsuit filed against it, then the FRCP should figure prominently in that organization's data management strategy.

Who Will Most Feel the Brunt of the FRCP Changes?

There are a variety of rules for data retention and production in specific industries, such as those imposed upon broker-dealers by the Securities and Exchange Commission (SEC) and the National Association of Securities Dealers (NASD). However, unlike industry-specific rules, the FRCP apply to any organization that might be involved in civil litigation, an increasingly common occurrence. For example, 61% of businesses in a recent survey had six or more lawsuits commenced against them during 2006, up from 44% of businesses that had six or more lawsuits filed against them during 2005¹.

In short, if an organization can have a civil lawsuit filed against it, then the FRCP should figure prominently in that organization's data management strategy.

Effective December 1, 2006, all cases brought will be subject to the new FRCP amendments. The Supreme Court has also determined that pending cases filed prior to this date should be subject to the new FRCP amendments so long as application of the new FRCP amendments is "just and practicable."²

¹ Third Annual Litigation Trends Survey Findings, Fulbright & Jaworski L.L.P.

² <http://www.supremecourtus.gov/orders/courtorders/frcv06p.pdf>

Why Backups are NOT Archives

Just about all organizations perform regular backups of their email servers, file servers and other data stores. Many organizations also believe that these backups constitute an 'archive' of their business information. However, that is definitely not the case.

A normal backup takes periodic 'snapshots' of a data store so that deleted or destroyed records can be recovered, such as when a patch goes awry, after the failure of a server's hard disk or after some other unexpected problem. Most backups, whether on tape or disk, are retained typically for no more than 90 days as subsequent backups on tape or disk overwrite older backup. While a backup tape, for example, can be preserved indefinitely in order to preserve business records, there are three fundamental problems with this approach to an 'archive':

An archiving system makes production of data in response to a regulatory request or an e-discovery order much simpler than if backup tapes must be searched for the requested information. If backup tapes must be searched for the needed information, the cost can be more than \$3,000 per tape.

- Backups are simply 'raw' content and lack any sort of indexing. If information from a backup tape must be produced during a discovery order, for example, the process to find just the right data is typically time-consuming, very disruptive to IT staff and expensive, particularly if third-party forensics firms must be engaged to find the data. For example, electronic discovery consultants fees start at \$275 per hour and emails can cost up to \$4.00 each to discover³.
- The integrity of backup tapes is by no means guaranteed. There have been many cases in which older tapes were not readable because of logical or physical corruption.
- Because backups are designed only to capture a snapshot of data at a given point in time, information created and deleted between backups will simply not be captured. For example, if an organization is required to preserve communications between senior management and external auditors, an email sent from the CEO to the outside firm at 9:00am and then deleted from the 'Sent' folder at 4:00pm on the same day will never appear in the nightly backup.

While backups are a key part of an organization's data protection activities, they are simply not a substitute for an

³ *Rising Costs of E-Discovery Requirements Impacting Litigants*, March 20, 2007, Law.com

archiving system. In short, a backup is designed to preserve data for short periods in support of the physical infrastructure that an organization maintains, while an archive is designed to preserve information for the long term basis for more strategic goals.

How Message Archiving Can Help You Comply With the FRCP

As discussed above, an archive can provide an organization with a number of important benefits:

- **Ease of producing data when necessary**
An archiving system makes production of data in response to a regulatory request or an e-discovery order much simpler than if backup tapes must be searched for the requested information. If backup tapes must be searched for the needed information, the cost can be more than \$3,000 per tape.
- **Ease of capturing data**
Information can be captured from a variety of data sources, indexed and placed into an archive without any intervention by IT staff or end users. Further, if a discovery hold order is imposed for a particular set of users – a reasonably common occurrence – a new policy can be created instead that will implement this order automatically on a moment's notice, minimizing the potential for spoliation of evidence.
- **Pre-litigation assessment**
It can also help to resolve disputes prior to a legal action by preserving all needed ESI and the context surrounding this data. An archiving system can also help an organization to assess the viability of its legal position at the beginning of a legal action, thereby saving lots of time and expense if the organization determines that its position is not tenable.

Other Benefits of Archiving

While an archiving system offers key benefits to organizations that must address their data governance practices in the context of FRCP compliance, archiving also provides a number of other benefits:

- **Storage management and storage optimization**
Email use is growing dramatically – Osterman Research has found that email use by employees is growing at about 20% annually. Increasing use of email, coupled

While an archiving system offers key benefits to organizations that must address their data governance practices in the context of FRCP compliance, archiving also provides a number of other benefits.

with growing use of attachments, larger attachments and more use of multimedia files means that email storage is becoming a top-of-mind issue for many messaging managers. Osterman Research has found that the growth in email storage is the leading problem for email managers and constitutes more of a problem than spam.

Archives consist of largely static data – if that data is included as part of regular backup and restore, then organizations are repeatedly backing up the same static data, which represents a significant cost in both storage and time. Using this approach requires organizations to buy more and more storage over time.

An appropriately configured archiving system can automatically offload data from email servers, resulting in better email server performance and shorter restore periods after a server crashes.

However, an appropriately configured archiving system can automatically offload data from email servers, resulting in better email server performance and shorter restore periods after a server crashes. Further, an archiving system allows IT to continue to impose mailbox-size quotas on their users, which most organizations do today. However, because data is automatically moved to archival storage based on specific triggering events (e.g., when a mailbox reaches 80% of the quota), users can employ what seems to be a mailbox of unlimited size, eliminating the need to manually move data from the inbox to other repositories in order to stay under the quota limit.

In addition to email, it is also important to consider instant messaging in the context of storage management, since use of these systems will increase rapidly, growing from one-third of all email users at present to near ubiquity by 2009⁴.

- **Satisfying regulatory obligations**

There are a wide variety of regulations that impose data retention and management requirements on organizations operating in the United States. These requirements, which number in the thousands, are very diverse, ranging from the Americans with Disabilities Act to the Toxic Substances Control Act. While most of these regulations impose data retention requirements that do not specifically call out ESI, email, instant messages or other specific data types, the growing quantity of ESI means that business records and other information

⁴ Osterman Research forecast

should be preserved in their native format, since it is decreasingly practical to do otherwise. In the case of instant messages, this should include attachments sent as file transfers through IM networks. The ability to archive both instant message text and the content of IM-borne attachments is important for e-discovery purposes.

- **Knowledge mining**

Three out of four email users in the workplace in a December 2006 Osterman Research survey reported that email is 'extremely important' in helping them to do their work. This is due mainly to the fact that most of the information that employees produce is in some way tied up in email in the form of documents, contacts, email threads and other content. An archiving system allows an organization to preserve this information for long periods so that employees have access to it when they need it.

- **Other benefits of archiving**

An archiving system can also help an organization to recover from a disaster by providing an off-site copy of current data if the archive data is replicated to a remote location.

While backup, archiving and other data retention practices are important components of a proper data management strategy, organizations must adopt a holistic approach to managing data, particularly with regard to the growing quantity of ESI that they manage.

What Should an Organization Do?

Based on the FRCP changes and existing case law, what should an organization do? Here are the key steps that any organization should undertake towards avoiding court imposed sanctions:

- Learn what types of electronic data exist in the organization and that might be needed very early in the litigation process.
- Review and assess existing document retention policies and practices. It makes sense to evaluate these policies now rather than waiting for litigation.
- Pay close attention to e-discovery issues from the earliest stages of litigation.
- Investigate the amount and cost of preserving, restoring, processing and reviewing relevant electronic data.
- Assess the format of production that is appropriate for the organization and each case.

- Determine an appropriate protocol for privilege and waiver claims.

In short, the new FRCP amendments will:

- Require that parties focus on electronic discovery early in the litigation process.
- Necessitate that parties be aware of how and where ESI is stored.
- Allow answers to interrogatories that reference specific electronically stored information.

The amendments raise the importance of data governance practices to a new level, since instead of proper data retention being just a best practice that organizations should follow, retention is now a legal obligation that can carry with it serious consequences if managed in the wrong way.

Summary

The new amendments to the FRCP are very important for both IT managers and business decision-makers to understand and consider. The amendments raise the importance of data governance practices to a new level. In addition to proper data retention being a best practice that organizations should follow, ESI should be carefully managed to avoid costly legal consequences as well. These consequences can range from significant costs for complying with a discovery order, to legal sanctions imposed by a judge for a failure to comply fully with that order. In rare cases, corporate directors can be jailed for criminal spoliation of data.

While backup, archiving and other data retention practices are important components of a proper data management strategy, organizations must adopt a holistic approach to managing data, particularly with regard to the growing quantity of ESI that they manage.

About Microsoft Exchange Hosted Archive

Microsoft Exchange Hosted Archive is a web-based solution that allows an organization to maintain an archive of email and instant messages sent and received by its employees. Exchange Hosted Archive is just one of the hosted services offered by Microsoft.

The Microsoft Exchange Hosted Archive service benefits from the hosted spam and virus protection technologies provided by Microsoft's Exchange Hosted Filtering service. As messages pass through the network, each message is

copied and stored in a secure online repository. Similarly, mail sent within the organization is captured through the Microsoft Exchange Server Journaling function. Instant messaging and other communications, such as Bloomberg Mail, can also be copied directly to the archive. As messages are received, the archiving system assigns a unique serial number and timestamp to each message. Full-text indexing allows stored messages to be searched by header, subject line, and message and attachment content. .

The Exchange Hosted Archive service can help an organization to comply with the discovery obligations imposed by the new FRCP amendments:

- Archived messages can be accessed through a security-enhanced, Web-based interface that allows flexible search queries to identify and export copies of applicable content.
- Legal holds can be placed on archived data easily, thereby minimizing the risk of inadvertent spoliation of evidence.
- Attorney-client privilege can be applied to protect the confidentiality of ACP-marked content within the system.
- The service provides reporting and auditing capabilities that will help organizations to comply with provisions contained in the new FRCP amendments.

The Exchange Hosted Archive service can help an organization to comply with the discovery obligations imposed by the new FRCP amendments.

Microsoft Exchange Hosted Archive also includes a continuity component. In the event of an outage, users can logon to the Web-based system to read, compose, and reply to email in real time even while their primary messaging capability is down. This helps maintain productivity during the downtime as well as helps protect against the loss of data. This is particularly useful for IT staff, as well, since it allows production servers to be taken down for maintenance, upgrades or the application of patches while minimizing the negative impact of such downtime on end users.

About Microsoft Exchange Hosted Services

Microsoft Exchange Hosted Services offer a cost-effective way for enterprises to help ensure the security and availability of their messaging environment, while instilling confidence that their messaging processes satisfy internal policy and regulatory compliance requirements. A seamless extension of Microsoft Exchange Server that operates over the Internet as a service, the complete line of services include hosted filtering for spam and virus protection; hosted archiving to help satisfy compliance requirements and internal policies, hosted encryption to help preserve email confidentiality; and hosted continuity for ongoing access to email during and after primary email environment outages. Microsoft Exchange Hosted Services provide value to corporate customers by eliminating upfront capital investment, freeing up IT resources, and removing incoming email threats before they reach the corporate firewall.

For more information, visit

<http://www.microsoft.com/exchange/services>

© 2007 Osterman Research, Inc. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed without the permission of Osterman Research, Inc., nor may it be resold by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

THIS DOCUMENT IS PROVIDED "AS IS". ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.

THE STAFF OF OSTERMAN RESEARCH, INC. ARE NOT ATTORNEYS AND DO NOT PRACTICE LAW. IN NO WAY SHOULD ANY OF THE SERVICES OR MATERIAL WRITTEN FOR THIS REPORT BE CONSTRUED AS LEGAL ADVICE. NEITHER MICROSOFT CORPORATION NOR OSTERMAN RESEARCH, INC. WARRANTS THE LEGAL VALIDITY OF ANY ADVICE, POLICIES, INTERPRETATIONS, PROCESSES OR RECOMMENDATIONS GIVEN BY OSTERMAN CONSULTANTS. ALL ADVICE, POLICIES, INTERPRETATIONS, PROCESSES AND RECOMMENDATIONS PROVIDED BY OSTERMAN SHOULD BE REVIEWED BY THE REPORT PURCHASER'S LEGAL COUNSEL.