

Archiving and The Federal Rules of Civil Procedure: Understanding the Issues

An ArcMail Technology Research Paper



Introduction

Most organizations have heard of Sarbanes-Oxley or the Health Insurance Portability and Accountability Act (HIPAA), yet the two government regulations do not impact every business. The Federal Rules of Civil Procedure (FRCP) on the other hand affects every business and organization that may ever be involved in a federal legal matter. Unfortunately, recent studies indicate that half of all organizations were not aware that new amendments went into effect on December 1, 2006, nor are they familiar enough with the new rules to understand how they will impact the way they retain information.

Only a few years ago, information was stored in large filing cabinets on paper or other physical forms of storage. Often there was only one copy of a document, which in some respects, made it easier for legal professionals to gather and review all of the information available for the discovery process. With the emergence of the computer and subsequent storage technologies, there may no longer be a such thing as a single original document as information is often sent via email to several parties, stored on local hard drives, network servers, flash drives and back-up appliances. Also, in the case of email, there is always a sender and at least one recipient. The sender only has control of the disposition of their own copy of the sent message; the received message is under the recipients' control. As a result of the emergence of digital storage, there has been a "paradigm shift"ⁱ in what is truly feasible in the review process.

"The shift of information storage to a digital realm has, for a variety of reasons, caused an explosion in the amount of information that resides in any enterprise-profoundly affecting litigation. This massive amount of electronically stored information is distributed broadly among different storage devices, from large mainframe computers to tiny machines capable of storing information equivalent to several warehouses of documents each, all of which are or can be integrated into other systems. These systems are complex, interdependent, and evolve spontaneously, like ecosystems. It is often impossible to find one person, or even one discrete group of people, who completely understand the workings of this new form of "information ecosystem."ⁱⁱ

Beyond the actual number of places that the information is stored, what can also make the discovery process difficult, time consuming and expensive is the capability of searching the information. This is where the famous song, "Let's call the whole thing off" certainly applies because one person's "tomaytoes" is another person's "tomahtoes."

The amendments to the FRCP approved by the U.S. Supreme Court in April 2006, "now require organizations that operate within the U.S. to manage their electronic data so it can be produced in a timely and complete manner."ⁱⁱⁱ Among the electronic data most requested during litigation are emails, and the remainder of this whitepaper will focus on the impact of the FRCP and email archiving.

Litigation on the Rise

Litigation is on the rise. In fact, according to the Third Annual Litigation Trends Survey, companies reporting more than 50 lawsuits represented "23% of the total 2006 survey sample, compared with just 11% in 2005."^{iv} The survey also found that the "percentage of companies with no lawsuits filed against them from 25% to 11%."^v Litigation was not limited to large companies as the survey found that 58 percent^{vi} of the smallest companies had at least one lawsuit filed against them from 2005 to 2006.

Some experts estimate that nearly 80 percent of the information in litigation is now electronic, which would make sense considering the majority of information created inside today's enterprises is in a digital format. What many IT people may not realize is that "in most of these situations, the smoking gun evidence is found in the e-mails or instant messages."^{vii}

Email archiving is critical as many organizations are finding out the hard way. Recently, Morgan Stanley was forced to pay \$12.5 million in fines because the company failed to provide e-mails by claimants in arbitration proceedings and regulators. Morgan Stanley had actually destroyed emails by overwriting back-up tapes and by allowing users to permanently delete emails. UBS Warburg was required to pay a former employee more than \$29.2 million in damages because the court found the company had destroyed emails and lied in court.

Morgan Stanley and UBS Warburg are not among the minority of organizations that are still trying to understand the importance of storing email. In a survey by Osterman Research, one-third of IT managers admitted they could not produce an email more than one year old. The survey found that very few companies have a corporate retention policy, and nearly a quarter of companies delete email manually or automatically after 90 days.^{viii}

Osterman's research, as well as the Litigation Trends Survey Findings, supports the basic idea that most organizations are not ready to meet the requirements outline in the FRCP amendments. The Trends Survey found that only "19% of respondents consider their companies to be well-prepared for e-discovery."^{ix}

The FRCP Amendments

The amendments to the FRCP require that organizations reevaluate how their electronic data is stored so that it can be searched and made available in a timely manner in the event of litigation. Among the amendments are the following:

Rule 16(b)

The addition to Rule 16 requires that organizations complete their discovery process "within 90 days after the appearance of a defendant and within 120 days after the complaint has been served on a defendant." This amendment places a time limit on the e-discovery process, making the ability to quickly search and find information that much more important.

Rule 26(a)(1)

This amendment requires that "a party must, without awaiting a discovery request, provide to other parties: a copy of, or a description by category and location of, all documents, electronically stored information, and tangible things that are in the possession, custody, or control of the party and that the disclosing party may use to support its claims or defenses, . . ."

As a result of this amendment, organizations may be required to disclose every relevant email found on an employee's laptop or mobile device or network server. Only privileged information can be withheld.

Rule 26(b)(2)(B)

While one party involved in the litigation "need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost," the courts may decide otherwise, forcing the party to find the information regardless of how difficult it may be. "On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, . . ."

Rule 26(b)(5)

This rule applies to information that is determined by one of the parties to be privileged information.

The organization responsible for discovery must describe why the information is privileged, and if the information is shared with the other party and deemed privileged by the courts, it must be returned to the court which will review the claim.

Rule 26(f)

This amendment requires both parties to agree to the format that electronically stored information should be delivered.

Rule 33

In the event that answers to an interrogatory are required, the review should include electronically stored information.

Rule 34

Civil Rule 34 indicates that electronically stored information comes in many formats and must be supplied upon request. The rule also allows organizations requesting information to request electronically stored information in a specific format. "Any party may serve on any other party a request (1) to produce and permit the party making the request, or someone acting on the requestor's behalf, to inspect, copy, test, or sample any designated documents or electronically stored information — including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations stored in any medium from which information can be obtained . . ."

Rule 37(f)

Titled "Failure to Make or Cooperate in Discovery; Sanctions," this rule provides a safe harbor for organizations that fail to "provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system."

Source for quotes: <http://www.law.cornell.edu/rules/frcp/>

Destructive vs. Forced Retention policies

Some companies still apply similar rules to email as they do to paper documents, but there is a substantial difference between the two forms of media; email always has at least one sender and one recipient, and once an email is sent, retention control of both copies is often lost.

Consider a company that has implemented a destructive retention policy that requires emails to be deleted after 90 days. Can your company do business only retaining files, conversations, contracts (contracts can now be executed in email) and transactions for only 90 days? The answer is overwhelmingly "no"; and given this fact, even if there is a destructive retention policy in place, employees will do whatever it takes to retain these documents so they can do their jobs, including creating PST files (we call these underground archives), printing emails, saving them on USB or other media and even going as far as forwarding them to their home email accounts. Once it is uncovered that employees are not following the policy, there is no policy.

Consider also that these "underground archives" will typically surface during a discovery and will often come as an unwelcome surprise to the legal staff because they shouldn't exist according to the policy – but they do! Having an email archiving system in place allows your legal staff to have a complete picture, and even in the worst case where there are damaging emails in the archive (you can be sure the other side already has those), the damaging emails can be put in the context of the entire communication, which often paints an entirely different picture than a single damaging email.

Email Back-up versus Archiving

As a result of these new amendments to the FRCP, organizations' email storage and archiving practices are coming under scrutiny. Most individuals and organizations conduct regular back-ups of email, but these traditional back-up processes are not enough to satisfy the new demands of the e-discovery process.

Email back-up programs or systems usually take a snap-shot of email folders at a given point in time. While back-up programs may be set-up to conduct consistent or even ongoing back-up of emails, the storage is not real-time. In addition, back-up defaults are usually set to only store emails for a certain period of time, traditionally 60 to 90 days. Anything beyond that time is usually deleted or over-written with more current data.

Often times email back-ups are not indexed or stored in a convenient manner that allows for simple or complex searching. The traditional storage solutions, such as tape back-up system, have been known to be unreliable and difficult to search. And in the event that an organization needs to pull data from back-up tapes, "the process is typically time-consuming, highly disruptive to IT staff and expensive, particularly if third party forensics firms must be used."

The main difference between email back-up and email archiving is in how the data is captured and stored. In the case of ArcMail Technology's Defender email archiving solution, the email is immediately and automatically captured in a single repository from a single or multiple sources. All email is captured in its original format based upon established corporate policies. Once captured is indexed and stored in such a way that the emails can be quickly searched and reviewed for relevant information.

"One of the most logical methods for storing electronic data such as e-mails and Instant Messages is in an archiving system that can satisfy all e-discovery requirements and preserve information on a long-term basis in support of more strategic corporate objectives. Information captured from a variety of data sources can be indexed and placed automatically into an archive for long-term storage. Automated policies can be applied to extract the information without user intervention or extensive searching of non-indexed backup tapes. Archival systems can also alleviate data overload on e-mail servers by automatically transferring data from user mailboxes to the archive."^x

Osterman Research identified several key benefits of archiving:^{xi}

1. Ease of capture
2. Ease of production
3. Regulatory compliance
4. Storage management and storage optimization
5. Knowledge management and data mining
6. Disaster recovery

ArcMail Technology

ArcMail Technology's philosophy on email archiving is based upon the needs of organizations to protect one of their most important and powerful data sources. Beyond simple communications, organizations are using email as a means to store important files, document transactions and collaborate with colleagues around the world. As a result, the information that is found inside emails and as attachments has become increasingly more important and relevant to business operations; thus the amendments made to the FRCA.

ArcMail's archiving solution, Defender, helps organizations manage and retain this business critical information by automatically capturing an exact copy of all inbound and outbound email on a secure appliance. Defender eliminates the need for large mailbox files and chaotic PST files and makes

searching through emails fast and easy. Just as the FRCP amendments impact every business, including small and medium sized operations, Defender is designed to meet the varying needs of organizations with only a few employees up to several thousand people. The appliance combines archiving functionality with built-in disk storage, helping to alleviate the email storage burden from already over-worked mail servers.

One question that often comes up as a result of the FRCP requirements is, "How much information should be saved?" While ArcMail Defender can store up to 8.7TB of data, the answer may be found in a more balanced strategy.

"The best approach to data retention is to implement a balanced strategy that leans toward saving more rather than less. This approach includes establishing specific policies around data governance that work best for an organization based on FRCP guidelines, regulatory obligations and advice from legal counsel; implementing backup, archiving and other technologies that will help to satisfy these policies; and using the right combination of nearline and secondary storage most effectively."^{xii}

Defender is an email archiving appliance that allows organizations to establish and enforce archiving policies that help to satisfy FRCP guidelines and regulatory obligations.

Conclusion

The amendments to the FRCP have raised the bar for e-discovery. All organizations must consider how the amendments will impact their email storage as no company is immune to the FRCP's enforcement. The amendments place everyone on alert, from the everyday user who must be careful not to delete important emails; to legal who are integral in helping to outline a litigation discovery strategy for companies; to IT departments which now will assuredly be involved as soon as any litigation is initiated against their organizations. The FRCP amendments also apply to both the private, public, government and educational sectors.

With litigation on the rise, it is important that organizations be prepared. Organizations should look for an archiving solution that will enforce company retention policies, immediately and automatically index every email and facilitate the process of search and retrieval to cut down on discovery time. By deploying the ArcMail Defender, organizations can help to satisfy the storage and retention needs of all internal departments, while protecting the company from excessive time and expense typically associated with the discovery process.

ⁱ"The Sedona Conference Best Practices Commentary on the use of Search Information Retrieval Methods in E-Discovery,"

http://www.thesedonaconference.org/content/miscFiles/Best_Practices_Retrieval_Methods___revised_cover_and_preface.pdf, pg. 193, August 2007.

ⁱⁱibid

ⁱⁱⁱFoltyn, Marty, "Getting Up to Speed on FRCP," *EnterpriseStorageForum.com*, June 29, 2007

^{iv}Fulbright & Jaworski, LLP, "Third Annual Litigation Trends Survey Findings," pg. 7, <http://www.fulbright.com/mediaroom/files/2006/FulbrightsThirdAnnualLitigationTrendsSurvey-Findings.pdf>.

^vibid

^{vi}ibid

^{vii}Foltyn, Marty, “Getting Up to Speed on FRCP,” *EnterpriseStorageForum.com*, June 29, 2007

^{viii}ibid

^{ix}Fulbright & Jaworski, LLP, “Third Annual Litigation Trends Survey Findings,” pg. 18, <http://www.fulbright.com/mediaroom/files/2006/FulbrightsThirdAnnualLitigationTrendsSurvey-Findings.pdf>.

^xFoltyn, Marty, “Getting Up to Speed on FRCP,” *EnterpriseStorageForum.com*, June 29, 2007

^{xi}Osterman Research, “The Impact of the New FRCP Amendments on Your Business,” January 2007, pg 8-9

^{xii}Osterman Research, “The Impact of the New FRCP Amendments on Your Business,” January 2007, pg 11