



# MINIMIZING THE PAIN OF **eDiscovery** WITH A PROACTIVE STRATEGY

How a proactive eDiscovery strategy will result in dramatic cost and IT time savings.

By Osterman Research



# Table of Contents

---

## 2 WHY YOU SHOULD READ THIS WHITE PAPER

About This White Paper .....2

---

## 2 KEY DRIVERS IN E-DISCOVERY

The Amendments to the FRCP .....2  
 Federal Rules of Evidence .....3  
 Other Recent Court Rulings .....3  
 Other Drivers for E-Discovery .....3  
 The EDRM .....3  
 Other Issues .....4

---

## 4 WHY IS E-DISCOVERY BECOMING MORE IMPORTANT?

The Growing Quantity of Electronic Content .....4  
 Other Content Stores Are Becoming More Important .....4  
 Organizations Must Be Proactive .....4  
 Examples of E-Discovery Gone Wrong .....5

---

## 5 WHAT SHOULD YOU DO?

Understand What You Need to Preserve .....5  
 Stay Ahead of the Game .....5  
 Establish workable data retention and deletion schedules .....5  
 Leverage technology to help classify data as it is produced .....6  
 Create as complete an e-discovery repository as necessary .....6  
 Understand how data retention requirements are evolving .....6  
 Do you know where your data is located? .....6  
 Make sure that the data you need is accessible in a timely fashion .....6



## WHY YOU SHOULD READ THIS WHITE PAPER

eDiscovery – the application of traditional discovery requirements and processes to electronic content – is rapidly becoming a top-of-mind business consideration for even the smallest of companies and other organizations. The reason is simple: there are about 17 million lawsuits filed each year in the United States alone and most of the lawsuits that require discovery will include a requirement to produce electronic content. Further, the law firm of Pillsbury Winthrop Shaw Pittman LLP estimates that eDiscovery alone represents 35% of the total cost of litigation.

An organization that is faced with the prospect of responding to an eDiscovery request has three options:

1. Do nothing.
2. Satisfy the request by looking for required content on backup tapes, file servers, local PST archives, laptops, smartphones, employees' home computers, etc. in the relatively short amount of time typically allotted to the eDiscovery phase of a lawsuit.
3. Rely on an already-deployed archiving solution and corporate policies about data retention.

An organization that relies on the last option will find eDiscovery to be the least costly option of the three noted above, much less disruptive to IT and business staff members than relying on non-archived data sources, and a much better strategy from an overall information management perspective.

Looking to the future, eDiscovery will only become more difficult, more expensive and more common. As just one example, the American Recovery and Investment Act of 2009 (ARRA) includes a key component known as the Health Information Technology for Economic and Clinical Health Act (HITECH) that will expand the scope of the Health Insurance Portability and Accountability Act (HIPAA). Under the new rules, individuals and lawyers can now collect fines for violations of the HIPAA Security Rule, dramatically increasing the incentive to sue privately when data is breached.

### About This White Paper

This white paper focuses on some of the important considerations around eDiscovery to which decision makers should pay attention. It provides information on some recent court rulings, the role of the US government in changing the nature of eDiscovery, and it also includes advice on how organizations should proceed as they develop their eDiscovery plans. It also includes information on Mimoso Systems, the sponsor of this white paper, and their eDiscovery solutions.

## KEY DRIVERS IN EDISCOVERY

### The Amendments To The Frcp

The Federal Rules of Civil Procedure (FRCP) are a body of rules that were created to govern civil court procedures in the United States district courts. While the United States Supreme Court is responsible for managing the FRCP and updating it, the United States Congress must approve these rules and any changes made to them.

One of the most important drivers for eDiscovery is the set of amendments to the FRCP that went into effect on December 1, 2006. These modifications represented several years of debate at various levels and will have a significant impact on electronic discovery and the management of electronic data for any company that does business in the United States. The changes to the FRCP require these entities to manage their information so that it can be produced in a timely and complete manner when necessary, such as during legal discovery proceedings.

The amendments to Rules 16, 26, 33, 34, 37, 45 and revisions to Form 35 are aimed at Electronically Stored Information (ESI). The amendments were designed to deal with many of the important issues presented by ESI:

- ESI can be incomprehensible when produced separately from the system(s) that created it.
- ESI is normally stored in much greater volume than are hard copy documents because of the ease with which these documents can be copied, such as by sending a single email to multiple recipients.
- ESI is dynamic and often can be modified simply by turning a computer on and off.
- ESI contains metadata that describes the context of the information and provides other useful and important information independently of its presentation in the document itself.

The amendments to the FRCP, which can be viewed as focusing on five major issues that are relevant for corporate decision makers, reflect the reality that discovery of email and other types of ESI is now a routine aspect of most litigation:

- The amendments treat ESI somewhat differently than traditional types of content.
- They require early discussion of and attention to electronic discovery.
- They address inadvertent production of privileged or protected materials.
- They encourage a two-tiered approach to discovery – deal with reasonably accessible information in the near term and then focus later on inaccessible data.

- They provide a safe harbor from sanctions by imposing a good faith requirement.

Unlike many information retention requirements in specific industries, such as those imposed upon broker-dealers, hedge fund managers and investment advisors by the Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA), the FRCP apply to virtually all companies and organizations in all industries, including private, public and non-profit organizations. In short, if an organization can have a civil lawsuit filed against it, then the FRCP should be a key consideration in its data management strategy.

### Federal Rules Of Evidence

The Federal Rules of Evidence (FRE), enacted in 1975, are a body of rules that determine how evidence is presented during trial in the US federal court system. These FRE are focused primarily on the initial presentation of evidence during trials. Individual states may use these rules as the basis for their own rules of evidence, or they may adopt different rules.

### Other Recent Court Rulings

There are a large and growing number of cases and decisions that are relevant to consider in the context of eDiscovery, including the following two examples:

- ***Disability Rights Council of Greater Washington v. Washington Metropolitan Area Transit Authority* 2007 U.S. Dist. LEXIS 39605** Production of email from backup tapes was ordered by the Court at the expense of the producing party. The Court also noted that the Safe Harbor provisions of Rule 37(e) do not apply if data destruction is not suspended after a litigation hold.
- ***Orrell v. Motorcarparts of America, Inc.* 2007 WL 4287750 (W.D.N.C. Dec. 5, 2007)** The court ordered the production of a plaintiff's home computer for forensic examination.

The Orrell case above should be particularly worrisome for the vast majority of companies, since Osterman Research has found that the vast majority of employees who use email at work also check their work-related email from home after hours, on weekends and while on vacation. This means that a large proportion of corporate content may be present on employees' personal desktop computers, laptops, netbooks, smartphones, etc.

Although there are hundreds of cases that can be cited in the context of eDiscovery, Osterman Research believes that these cases focus on five relevant eDiscovery lessons that organizations of all sizes should heed:

- Metadata is an important component of the data that should be evaluated and may need to be presented during eDiscovery.

- A failure to diligently search for and assess relevant content during the eDiscovery phase of a legal action can have serious consequences.
- Data sources that must be searched during eDiscovery can be far-reaching, including employees' home computers.
- The difficulty of accessing ESI will not necessarily protect parties from their obligation to produce this data during discovery.
- Legal protections, such as the Safe Harbor provisions of the FRCP, are not necessarily afforded to parties that do not adequately protect data to which a legal hold has been applied.

### Other Drivers For eDiscovery

The FRCP represents just one aspect of the eDiscovery process. Many US states have already passed, or will soon pass, their own version of the FRCP for civil litigation that takes place within their respective court systems. For example:

- Texas adopted Rule of Civil Procedure 196.4 in 1999, which states, in part, "to obtain discovery of data or information that exists in electronic or magnetic form, the requesting party must specifically request [it] and specify the form in which the requesting party wants it produced."
- Minnesota modified its Rules of Civil Procedure, effective July 1, 2007, establishing procedures for the discovery of ESI.
- New Jersey adopted the new FRCP eDiscovery rules effective September 1, 2006.
- A number of other states are also considering enhancements to their civil procedure laws that will focus more on ESI.

### The Edrm

Started in May 2005, the goal of the EDRM Project was to create a framework for the "development, selection, evaluation and use of electronic discovery products and services"<sup>1</sup>. The EDRM, placed into the public domain in May 2006, is designed to help organizations manage the process of eDiscovery from the initial stages of managing electronic information all the way through to its presentation. Development of the EDRM was critical because it represented a major step forward in the standardization of the eDiscovery process.

<sup>1</sup> <http://www.edrm.net>

The Electronic Discovery Reference Model (EDRM) Project was developed in response to the few standards and lack of generally accepted guidelines for the process of eDiscovery that existed prior to its development. The team that developed the EDRM was facilitated by George Socha (Socha Consulting LLC) and Tom Gelbmann (Gelbmann & Associates), and included 62 organizations, among whom were law firms, software developers, professional organizations, consulting firms and large corporations.

After the development of the EDRM was the EDRM XML project in the 2006-2007 timeframe. The goal of this project was to “provide a standard, generally accepted XML schema to facilitate the movement of electronically stored information (ESI) from one step of the electronic discovery process to the next, from one software program to the next, and from one organization to the next.”<sup>2</sup>

### Other Issues

Authentication is a key part of the eDiscovery process because its goal is to prove that a document is a true and verifiable representation of an electronic document. Authentication for electronic content is even more critical than for paper-based documents, since electronic documents are more easily altered. As a result, in order to prove the authenticity of an electronic document, such as an email, those who submit this evidence must provide affidavits or otherwise demonstrate that an original document was not modified after the fact.

Although electronic evidence is today routinely presented in court proceedings, the authenticity of electronic records is an issue that many companies may not have fully considered. For example, in the case of *Vinhnee vs. American Express Travel Related Services Company, Inc.*, American Express sought payment for more than \$40,000 in charges on two credit cards from a California resident who had previously filed for bankruptcy protection. Because American Express could not demonstrate the authenticity of the electronic statements it presented during trial, it lost the case even without the plaintiff being present.

A key authenticity case is *Lorraine v. Markel American Insurance Co.* [2007 U.S. Dist. LEXIS 33020 (D. Md. May 4, 2007)]. This case involved a dispute between the owner of a ship that had been damaged and the insurer of the ship. Although the insurance company paid for the damages, the ship's owner subsequently found additional problems related to the initial claim and made a second claim, which the insurance company disputed. During arbitration, the damages awarded to the plaintiff were reduced by \$22,000. While both parties presented email evidence during arbitration, Chief Magistrate Judge Paul W. Grimm who presided over the case found that the email evidence presented could not be authenticated. In a part of his ruling, the judge wrote that “the integrity of data may be compromised in the course of discovery by improper search and retrieval techniques, data conversion, or mishandling.” In short, Judge Grimm ruled that for ESI to be approved for use as

evidence, a variety of FRE rules must be taken into consideration, including Rules 104, 401, 403, 801, 901, 902 and 1001-1008.

## WHY IS EDISCOVERY BECOMING MORE IMPORTANT?

eDiscovery is simply the extension of the well-established discovery process to the electronic content that an organization might possess, including email messages, word processing files, instant messages, spreadsheets, presentations, purchase orders, contracts, wiki and blog postings, files stored in document repositories and collaboration systems, and all other electronic content to which an organization has access. Further, eDiscovery extends to all of the venues in which this data might be stored, including desktop machines, laptops, smartphones, servers of all types and employees' home computers and other personally owned devices.

### The Growing Quantity Of Electronic Content

Virtually any business that uses computers receives, generates and stores large and growing amounts of information. For example:

- According to an analysis conducted by the University of California at Berkeley, 93% of all information today is created in an electronic format.
- The American Records Management Association (ARMA) estimates that more than 90% of records created today are electronic and that in excess of 70% of electronic information is never printed.

Unified communications and unified messaging systems will make the problem much worse as it adds additional data to the already crowded mix of data types that organizations must retain and manage.

### Other Content Stores Are Becoming More Important

While email is the logical place for organizations to start in the eDiscovery process because even a small organization will generate tens of thousands of email annually, there are many other sources of discoverable electronic content. These include SharePoint document repositories, file servers, CRM systems and many other systems that generate electronic business records. All of these sources are potentially discoverable in civil litigation.

### Organizations Must Be Proactive

One position on eDiscovery is that an organization should wait until it becomes involved in litigation and then begin the process of searching for relevant content, placing a legal hold on documents that will be required during the case, and so forth. Another position is that organizations should be proactive and implement archiving and other capabilities in advance of litigation.

<sup>2</sup> [http://www.edrm.net/xml\\_2006\\_2007.php](http://www.edrm.net/xml_2006_2007.php)

Osterman Research's view is that a proactive approach to eDiscovery is clearly preferable to one that simply reacts to litigation requirements after they have started. The benefits of being proactive in the context of eDiscovery are several:

- A proactive approach, which includes deploying archiving systems to preserve business records stored in email and other electronic data stores, ensures that an organization will be able to meet its eDiscovery requirements when called upon to do so.
- The new amendments to the FRCP shortened the amount of time available to respond to eDiscovery and related requests. A proactive approach to eDiscovery allows an organization to be better able to meet the time dependencies of an eDiscovery schedule.
- Being proactive means that an organization has already developed a document retention policy and deployed the right solution to preserve documents that must be retained. An organization that is not proactive runs the quite serious risk of not being able to produce data that a court might rule it had an obligation to preserve.
- A proactive approach to eDiscovery is almost always much less expensive and less disruptive to corporate staff than an approach that starts only after notice of a lawsuit has been received. Typically, the cost of just one eDiscovery exercise completed without content retention rules and a robust archiving system will exceed the cost of an archiving system by many times.

### Examples Of eDiscovery Gone Wrong

An important case for any decision maker to consider is *Qualcomm, Inc. v. Broadcom Corporation* (No. 05-CV-1958-B[BLM], 2007 WL 2296441 [S.D. Cal. August 6, 2007]). Although Qualcomm initially prevailed in this case, it was determined after the court ruling that thousands of emails were withheld during the case. As a result, the Court awarded \$8.5 million in attorney's fees and costs against Qualcomm.

## WHAT SHOULD YOU DO?

### Understand What You Need To Preserve

Before any archiving or other eDiscovery solution is deployed, it is critical for any organization to understand the obligations that it faces with regard to the retention and disposal of electronic data. Among these obligations are:

- Local, state, provincial, federal and international obligations to retain certain types of data, such as business records, emails and other content that might be required during an eDiscovery exercise.
- Industry-specific obligations and/or best practices for the retention and disposition of certain types of records.

- Legal obligations and legal precedents to retain certain types of data and to establish retention periods that are appropriate for certain data types.

Cohasset Associates has published the results of a survey<sup>3</sup> that provides some interesting findings on records management and organizations' development of data retention policies:

- Only 56% of organizations have a formal plan that will allow them to respond to discovery requests for their records.
- Only 55% of organizations have records retention schedules for email, instant messages, blogs, collaboration tools and other types of communication; and only 43% have such schedules for electronic documents.
- Only 14% of organizations always follow their retention schedules, while another 50% generally do so.
- Only 16% of organizations has a formal policy focused only retention of voicemail, 15% have such a policy for instant messages and only 7% have a retention policy for blog content.

The survey points out, among other things, that organizations simply are not retaining as much data as they need to preserve, nor are they implementing policies and procedures to protect themselves from the consequences. Plus, there does not seem to be significant progress over time in this regard on the part of many decision makers, despite the fact that the new amendments to the FRCP, recent court decisions and the growing quantity of electronic content that most organizations possess mean that there really should be more progress than has been the case.

### Stay Ahead Of The Game

The following points represent a few key guidelines to consider in developing an eDiscovery strategy:

- **Establish workable data retention and deletion schedules** All organizations, regardless of their size or industry, should establish sound data retention policies for all of the different data types that they manage or will have occasion to manage over the next several years. Different types of business records will be subject to different data retention schedules, and so retention schedules should be sufficiently granular as to accommodate all of these requirements.

While establishing data retention schedules is critically important, an often-overlooked – but no less important – consideration is the deletion of data after it no longer needs to be retained. Retaining unnecessary data can result in a variety of problems, including higher eDiscovery costs because of the volume of data that must be reviewed, increased liabilities associated with

<sup>3</sup> *The 2007 Electronic Records Management Survey* (<http://www.cohasset.com>)

'smoking guns' that might reside in old data stores, and higher storage costs. Some data should probably be deleted after 30 or 60 days.

- **Leverage technology to help classify data as it is produced** Human review of data generated during an eDiscovery exercise, as well as intervention by humans in the data classification process on an ongoing basis, will continue to be a requirement for at least the next several years until automated classification technologies are sufficiently robust. However, there are technologies available today that can classify, process and review email and other electronic documents quite well and can significantly speed classification and eDiscovery processes. These technologies should be employed, where appropriate.
- **Create as complete an eDiscovery repository as necessary** Centralizing data stores and consolidating them into a smaller number of repositories can provide significant benefits during eDiscovery. Migrating old backup tapes into a messaging archiving system can result in faster searches, reduced costs and greater responsiveness to eDiscovery requests. For example, some vendors offer services that will migrate data from tape to an archive. Migrating tapes in this manner can provide a dramatic reduction in the IT costs required to manage backup tapes.

It is important to note, however, that some litigators would advise their clients not to make all data accessible for eDiscovery purposes – each organization will have to determine the most appropriate and least risky strategy.

- **Understand how data retention requirements are evolving**  
As a corollary to the point above, organizations must continually remain aware of the changing nature of data

retention requirements based on new court decisions, new statutory requirements and industry best practices.

- **Do you know where your data is located?**  
There can be a large number of different platforms on which discoverable data is stored, including email servers, instant messaging servers, file servers, desktops, laptops, smartphones, employees' home computers, backup tapes, archives, voicemail systems, mainframe and other host-based systems, 'live' message stores that have not yet been backed up or archived, USB thumb-drives, CD-ROMs and even old diskettes. It is imperative for organizations a) to know where all of its relevant data resides, b) how to access that data without interrupting normal business processes, and c) how to access that data without spending huge amounts on IT, legal or other staff members' time searching for it.
- **Make sure that the data you need is accessible in a timely fashion**  
Although data may exist in an organization, it may not be easily accessible during the timeframes required for eDiscovery. For example, Osterman Research has found in a recent study that the vast majority of organizations allow users to store information in local message stores, such as local hard disks. However, only 31% of these local message stores are backed up to a central location and are accessible to the organization at large for long periods of time. That means that while the data in your organization is technically accessible, it may not be practically accessible.

Clearly, restoring every piece of data is not necessarily a sound practice in every situation. Each organization must decide, based on a variety of factors, what data it should restore and what data it can safely leave inaccessible.

---

## ABOUT MIMOSA SYSTEMS

Mimosa Systems provides information immediacy, discovery and continuity for the new generation of critical enterprise information. It enables fingertip access to vast information by users, powerful and rapid search and retrieval of corporate historical information by auditors, and uninterrupted access to corporate information in the midst of failures and errors.

Mimosa™ is focused on information management of unstructured and semi-structured data, including email and attachments, instant messages, files and documents, and other new data types.

Mimosa delivers next generation information management solutions that unify archiving, data protection and disaster recovery in one solution. Mimosa's next-generation information management solutions help transform everyday business processes and drive benefits across the organization, from CXOs to legal, HR to IT, and most importantly to employees.

Mimosa NearPoint™ for Microsoft® Exchange provides fine-grained and immediate recovery, with self-service archival access to enterprise information. Mimosa NearPoint is the industry's only comprehensive information management solution for Microsoft Exchange, unifying archiving, recovery and storage management. NearPoint assures email continuity and regulatory compliance, while leveraging cost-effective disk technologies to optimize Exchange storage growth.

Mimosa NearPoint for SharePoint provides a holistic solution to managing SharePoint data with integrated

archiving, recovery, and eDiscovery. NearPoint is the only SharePoint management product to combine both archiving and recovery while maintaining easy end-user access to information. In addition, Mimosa NearPoint offers the most comprehensive SharePoint data capture available. Customers can capture all content types and associated metadata and attachments, perform continuous capture via Change Notification, and preserve the relationships between sites and content. NearPoint also provides full-text indexing and global single-instancing on all archived content. This content can then be offloaded from SharePoint to enable storage cost savings while maintaining seamless end-user access via stubbing. Moreover, Mimosa NearPoint also manages the retention and disposition of SharePoint content across the archive in accordance with organizational policies.

Mimosa NearPoint File System Archiving (FSA) provides indexing, archiving, end-user secure search, eDiscovery and content monitoring across platforms and across file and document types.

Mimosa is based in Santa Clara, California with offices in Munich, Germany and Pune, India with an executive team from CA/Cheyenne, Brocade, Veritas and Zantaz that have been responsible for some of the leading storage and e-mail solutions in the market.

Mimosa has a strong partnership with Microsoft Corporation, working together to assure that NearPoint works seamlessly to enhance our customers' use of Microsoft Exchange. Mimosa partners with Microsoft to make it simpler for corporations to manage email, documents and other enterprise content throughout their lifecycle.

