

Strategies for Preparing for E-Discovery

The amendments to the U.S. Federal Rules of Civil Procedure regarding the discovery of electronically stored information make it imperative for organizations to develop an enterprise-wide strategy to manage its volume.

Brian Dirking and Raghu R. Kodali

The 2006 amendments to the U.S. Federal Rules of Civil Procedure (FRCP) have changed information management requirements – not just for lawyers and others involved in discovery, but also for IT professionals and records managers, who now have to be prepared to produce electronic content for discovery and litigation.

Many organizations are overwhelmed by these requirements and, in trying to prepare for the worst, they sometimes take actions – such as retaining all electronic content indefinitely – that may be counter-productive. Developing a strategy and a plan of action for handling e-discovery will help organizations mitigate their risk and save them a significant amount of money in the event of litigation.

The FRCP guide civil litigation in U.S. federal courts and are commonly adopted in state and other courts, so they are very influential throughout the United States for all civil procedures.

Some of these rules address the process of *discovery*, which is the pre-trial phase in a lawsuit in which each party can request documents and other evidence from opposing parties. *E-discovery* deals with discovery of electronically stored information (ESI), including documents and e-mails.

The discovery process affects many individuals in an organization. For an IT person, it means restoring backup tapes to show evidence on file shares, content management systems, e-mail systems, or other applications. For legal

counsel, it means having a review process to determine what discovered content is relevant to the case. But for records managers, this work will have begun long before any lawsuit with managing records for retention, placing legal holds, and finalizing disposition.

During the past 30 years, the volume of ESI has risen to the point that it now surpasses the volume of information stored on paper. ESI presents special issues for discovery:

- ESI can be replicated at a very low cost, resulting in tremendous volume.
- Electronic content can be easily changed and deleted.
- ESI can be backed up, creating more volume as content is copied.
- Electronic content may require certain software to access and read.
- ESI can reflect relationships based upon how it is distributed.
- ESI may have associated metadata.
- ESI can be searched.

At the Core

This article

- ▶ Describes the Federal Rules of Civil Procedure (FRCP) regarding electronically stored information
- ▶ Discusses common approaches for meeting the challenges of the FRCP requirements
- ▶ Tells how an enterprise-wide records management system minimizes e-discovery risks and costs

FRCP Changes

The growing volume and relevance of ESI led to the 2006 amendments to the FRCP. The amendments to rules 16, 26, 33, 34, 37, and 45, and revisions to Form 35 are specific to ESI.

Rule 16

A judge must enter a scheduling order that limits the time to complete discovery. This order should take into account the handling of ESI discovery early in the litigation. This order also addresses any agreements that the parties reach to facilitate discovery by minimizing the risk of waiver of privilege or work-product protection.

Rule 26

An organization must provide a copy of, or a description by category and location of all documents, ESI, 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. This rule is amended to direct the parties to discuss discovery of ESI and to add to the discovery plan the parties' proposal for the court to enter a case-management or other order adopting such an agreement.

Rule 34(b)

This rule requires organizations to produce ESI in its native format with its metadata intact and to prove chain of custody. While the duty to preserve evidence is narrowed only to relevant data, the potential consequences are great. For example, if a defensible process is not demonstrated, opponents may be granted access to an organization's entire network.

Rule 37(f)

This rule provides a "safe harbor" for data destruction. This means that organizations face no penalties for deleting ESI in keeping with routine operation of IT systems if the party took "reasonable" steps to preserve it. However, any destruction must be due to routine operation and done in good faith; a systemized framework must be

in place, and this systemized framework must have integrated litigation hold procedures to prevent destruction during litigation.

Form 35

Form 35 is amended to call for a report to the court about the results of the discussion in rule 26. In many instances, the court's involvement early in the litigation will help avoid difficulties that might otherwise arise.

The Cost of E-Discovery

The amended rules signal organizations on how to prepare for e-discovery. The main reason for so much concern around e-discovery is that it is costly. It is costly because it requires organizations to retrieve content from servers, archives, backup tapes, and other media.

In 2002, in *Murphy Oil v. Fluor Daniel*, Fluor Daniel spent \$6.2 million to restore and print e-mail from 93 backup tapes. That same year, in *Rowe Entertainment v. William Morris Agency*, the William Morris Agency reported a cost of \$9.75 million to restore e-mail from 200 tapes – plus hundreds of thou-

sands dollars more to retrieve and review 250,000 e-mail messages.

E-discovery is also costly in terms of legal review. Once the content is restored, a legal team will review it for relevance to the case – typically at a cost of \$1,800 to \$2,500 per gigabyte. For an organization storing 25 terabytes (25,000 gigabytes), a discovery review of 25 percent of its information would cost between \$11 million and \$16 million.

In some cases, an organization is unable to execute a discovery order because it is unable to locate all content in a timely manner, or it is unable to place holds on all content and some of it is deleted during the lawsuit. The inability to do this correctly also has a cost, and it can be considerable.

In *Coleman Holdings, Inc. v. Morgan Stanley & Co.*, Morgan Stanley was unable to properly restore and produce evidence, causing the judge to shift the burden of proof to Morgan Stanley, ultimately resulting in a decision of \$600 million in compensatory damages and \$850 million in punitive damages against Morgan Stanley.

To address these costs, many organi-

zations are looking at e-discovery solutions that will enable them to review the found content and take it through litigation. But organizations can also lower costs for archiving and restoring, legal review, and sanctions by simply cutting down how much content it retains. Less stored content means less content on which to perform discovery.

mation, regardless of medium or characteristics, made or received by an organization in pursuance of legal obligations or in the transaction of business,” organizations still need to have a retention policy to determine when this content can be deleted.

It is important to note that, as stated in the FRCP, it is acceptable to destroy

project. Its findings:

- Of the 75 million pages of text they reviewed during the three-year period, more than 50 percent of the documents were out-of-date and should have been deleted.
- The cost of reviewing out-of-date documents amounted to \$12 million.

It is important to note that, as stated in the FRCP, it is acceptable to destroy documents. An organization is not required to keep every piece of electronic information it generates.

Retention Management

The amended FRCP make it clear that *any* electronic information is now discoverable and admissible. This includes everyday documents and e-mails used for a range of communications – from project plans to lunch plans. This much broader definition means a much larger pool of electronic content is subject to discovery. Organizations take a variety of approaches to deal with this new reality – some of which should be avoided.

Avoid the “Destroy Everything” Approach

Because all ESI is now discoverable, organizations may be tempted to destroy that information as soon as possible to reduce the cost of discovery. But, some information must be kept for regulatory and compliance reasons. For example, many organizations are governed by regulatory bodies that require business information to be retained for a specific period of time. Some of that information might also be important to support the organization in case of litigation. Destroying the wrong information can lead to fines and unfavorable judicial decisions.

Although not all ESI will be considered a “record,” which according to the *Glossary of Records and Information Management Terms* is “Recorded infor-

documents. An organization is not required to keep every piece of electronic information it generates. However, courts look for a program of destruction that is consistently applied.

Some organizations may “cherry pick” through content to remove content that is deemed most risky. But in litigation, it will be necessary to prove that the deletion of this content was consistent with a policy that has been applied rigorously. Without audit trails and certificates of destruction, it can be difficult to prove compliance with an organization’s policies.

Avoid the “Keep Everything” Approach

To avoid this situation, many organizations are simply choosing to keep everything. But experience proves that the cost of restoring backup and archive tapes, as well as the cost of discovery and the inability to identify content and place immediate holds, can make this policy economically disastrous in the event of litigation.

One frequently cited example of the tremendous expense of keeping everything is from a large chemical company’s internal study. To persuade business unit leaders of the need for effective document retention and disposition, the company’s legal department conducted an internal cost assessment of a three-year litigation

Avoid Automated E-Mail Deletion Policies

To reduce the amount of content being retained, some organizations provide strict policies around retention, declaring, “We will retain e-mail no more than 30 days.” Then, to provide a defensible audit of this policy, they set up an automated system to delete e-mails after 30 days.

This approach is attractive in its simplicity, but it does not address the business needs to retain some information. Most projects last more than 30 days, and when users discover that key e-mails or other documents that pertain to the project have suddenly been removed, they may adopt other means to retain that content. They may, for example, move e-mails to a personal mailbox file, forward them to a personal e-mail account, or print them out and keep them in file drawers. Now the content is completely out of the hands of the organization’s records manager and the IT person, who will be required to attest to the destruction of these items of potential evidence.

Set a Business-Savvy Retention Policy

The key is to have a retention program that is flexible enough to keep content for the right retention period. Retention periods are historically

thought of in terms of calendar events. A document that was created in 2000 may no longer be required in 2008, and so it will be destroyed.

But retention periods for business content are driven by business events, such as the length of a project, the duration of a contract, or the termination of an employee. And the retention policies

- Delete revisions
- Revise

These different actions can be applied to retained information over the course of its lifecycle as it moves from its active use to inactive status to its deletion. But the flexibility to do more than merely set a date for deletion is critical as the need for

administered through a single interface.

- A catalog of discoverable content is created.
- Holds can be placed instantly across these different systems, ensuring that evidence is not deleted during litigation.

Retention policies offer an important opportunity for records managers who can bring their awareness of content types and lifecycles to bear on everyday business.

that match up to these content types must reflect the lifecycle of the content.

Organizations may choose to keep project information for three years after the end of the project. A workflow event that signals the end of a project, such as the publishing of a report, may commence the retention period for the associated e-mails and files. An organization may create a retention policy that a contract will be retained for five years after the end of the contract period. The end of the contract, then, could then trigger a lifecycle action for that document.

There are many types of events that could trigger a retention policy:

- Content expired (e.g., a contract)
- Usage statistics (e.g., document has not been accessed in six months)
- Business event (e.g., environmental impact filing)
- Content lifecycle event (e.g., new revision checked in)

There are, likewise, many actions an organization can take based upon the retention policy:

- Delete
- Notify author
- Archive
- Move

business-savvy retention policies becomes more obvious.

Retention policies offer an important opportunity for records managers who can bring their awareness of content types and lifecycles to bear on everyday business. Professionals who can distinguish their skills to work successfully with business users and to provide a strong and defensible retention management system will find themselves in demand.

The Benefits of In-place Management

Many organizations have tried to enforce retention management by having employees change their authoring procedures and begin using an enterprise-wide records management system. This results in a tremendous cost for training employees to use the system. And this approach often fails as people revert to their more familiar ways of authoring.

A new approach is what is known as “in-place management.” Authors create content using their familiar tools and systems, but retention management is enforced on that content where it lives, from a centralized server. This approach has a number of ramifications:

- Retention policies are centrally

- Disposition can be performed from a central console.

By categorizing content, creating a catalog of the content, creating a retention plan, implementing a hold methodology, and having disposition procedures, an organization will benefit in many ways through preparation. These include:

- *Decreased Risk* – By keeping less content, an organization decreases the risk of adverse evidence being found.
- *Higher Productivity* – By organizing content through a file plan, key information, such as regulatory filings, tax information, business licenses, invoices, and other content, can be more easily found.
- *Lower Discovery Costs* – With less information available for discovery, an organization will reduce the cost of restoration of content and the cost of legal review.
- *Increased Flexibility* – An organization will be prepared to present a catalog of discoverable content, which is a requirement of the FRCP “meet and confer” Rule 26.
- *Stronger Legal Action* – By “knowing hand,” or knowing the evidence

that an organization possesses, legal counsel can more quickly assess strategy and pursue a settlement, which can be a huge money savings.

- *Less Vulnerability* – Organizations that are unable to comply with electronic discovery requirements are beginning to see nuisance lawsuits. When an organization cannot comply with discovery requirements, it may set a cost threshold – stating, for instance, that any lawsuit under \$100,000 is not worth the discovery effort and should be settled. This exposes the organization to nuisance lawsuits that are brought at just under the threshold.

Results of the 2006 Amendments

With the introduction of the 2006 amendments to the FRCP, many people expected 2007 to be full of spectacularly failed discovery efforts, as well as judgments. However, there was only one case of note: *Columbia Pictures v. Brunell*, in

which defendants were to turn over ESI kept in computer memory. The effects of the amendments will emerge over the next few years, as most cases that involve large discovery efforts take years to work their way through to trial and decision.

Savvy records managers realize that if they have not already done so, now is

the time to develop ESI retention programs. Now is the time to create committees within their organizations and to bring their expertise together with legal counsel and IT to prepare for e-discovery and litigation. And, now is the time to focus on one of any organization's greatest assets, its information. ■

***Brian Dirking** is principal product director at Oracle. He has been in the electronic publishing industry for more than 15 years, as marketing manager for Barrington House Publishing, product manager for OWL International Inc., and director of marketing for InfoAccess Inc., and director of business development for Stellent Inc. He is active in local chapters of ARMA and AIIM, and he is on the AIIM Board of Directors. He may be contacted at brian.dirking@oracle.com.*

***Raghu R. Kodali** is consulting product manager and SOA evangelist for Oracle Application Server. Kodali held presales and technical marketing positions in Oracle Asia-Pacific, based in Singapore. Prior to joining Oracle, he worked as a software developer with National Computer Systems, Singapore. He holds a master's degree in computer science and is a frequent speaker at technology and user group conferences. He may be contacted at raghu.kodali@oracle.com.*

References

ARMA International. *Glossary of Records and Information Management Terms*. Lenexa, KS: ARMA International, 2007.