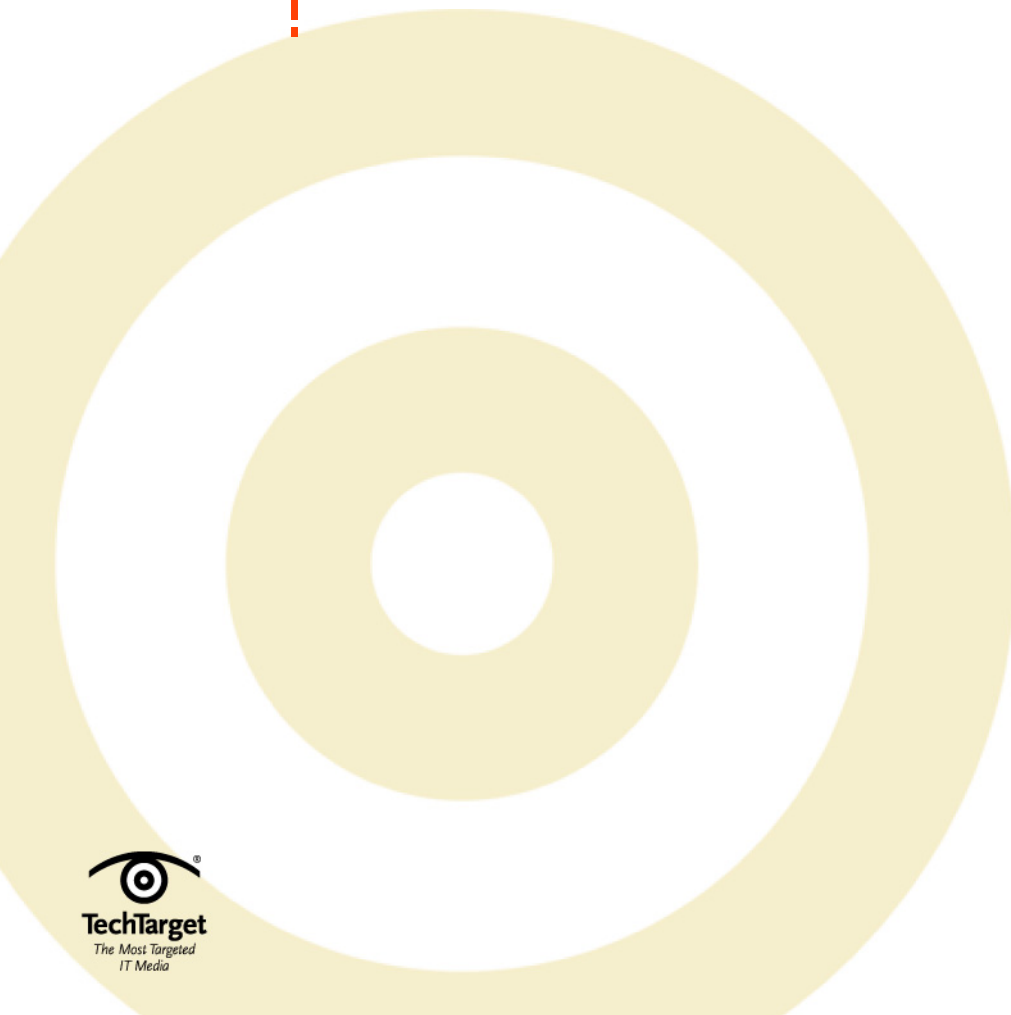


An IT Briefing produced by



Taking Control of Information: Managing Discovery



Sponsored By:



Taking Control of Information: Managing Discovery

By Mark Diamond and Pete Pepiton

© 2007 TechTarget

BIOS

Mark Diamond is President and CEO of Contoural Inc.

Pete Pepiton is Discovery Product Manager with CA.

This *IT Briefing* is based on a CA/TechTarget Webcast, “Taking Control of Information: Managing Discovery.”

This TechTarget *IT Briefing* covers the following topics:

- Introduction 1
- Legal Issues That Impact IT 1
- Changes in Legal Landscape 1
- Retention Policies 1
 - Litigation Hold Processes 2
 - Litigation Readiness 3
- What Do the New FRCP Rules Mean? 3
- Electronic Discovery Reference Model (EDRM) 4
- IT and Legal Disconnect 4
- Connecting Legal and IT 5

Copyright © 2007 CA. All Rights Reserved. Reproduction, adaptation, or translation without prior written permission is prohibited, except as allowed under the copyright laws.

About TechTarget *IT Briefings*

TechTarget *IT Briefings* provide the pertinent information that senior-level IT executives and managers need to make educated purchasing decisions. Originating from our industry-leading Vendor Connection and Expert Webcasts, TechTarget-produced *IT Briefings* turn Webcasts into easy-to-follow technical briefs, similar to white papers.

Design Copyright © 2004–2007 TechTarget. All Rights Reserved.

For inquiries and additional information, contact:

Dennis Shiao

Director of Product Management Webcasts, TechTarget

dshiao@techtarg.com

Taking Control of Information: Managing Discovery

Introduction

Years ago it was rare that the IT organization would have much interaction with Legal. However, today it is likely that IT will have an interaction with Legal weekly, if not daily. Legal frequently needs information from IT, sometimes as part of e-discovery and sometimes as part of compliance. This document discusses what Legal generally wants from IT and what IT can do to position itself to meet the needs of Legal.

Disclaimer: This document discusses legal information; this is not the same as legal advice. For actual legal advice, companies should refer to their own counsel.

Legal Issues That Impact IT

An important point to remember is that Legal does not usually think of the world in IT terms: they do not think about storage or file systems, for instance. Legal generally thinks in terms of nearly everything as a document: paper, electronic, or unstructured. Most of their requests involve:

- Finding documents
- Retrieving these documents
- Saving or preserving documents for a specific type of litigation

IT organizations need to be aware that Legal may think in terms of all this information being in as simple a format as paper. In fact, on average, 96% of documents in most organizations are electronic.

One of the areas most impacted within IT is e-discovery and litigation. Within e-discovery and litigation, e-mail is the most commonly requested document. When Legal makes requests, the location of requested electronic documents is irrelevant—whether they are on the main file server, in backup files, on laptops or desktops, or on home systems, they must be produced. In general, the cost of locating information is borne by the record holders, and being unable to locate the documents can bring on severe consequences.

Changes in Legal Landscape

On December 1, 2006, an amendment was made to the Federal Rules of Civil Procedure (FRCP). The FRCP is a set of rules that define how the federal courts operate, and many state courts follow the same rules. This amendment addressed e-discovery. Figure 1 summarizes the key points of this amendment.

The rules that call for full and accurate disclosure mean that anything electronically stored is potentially discoverable. There was some hope before this amendment came out that the courts would consider e-mail a transitory record that is not discoverable, but the courts have actually broadened potential discovery. These rules require a conference within 100 days of facing litigation, where both sides must have a “meet and confer” session. During this “meet and confer” session, both sides have to declare which documents they are going to use to support their side of the case. While the sides do not have to have the documents for 100 days, they have to define the names, types, dates, and locations of these documents. If a company cannot present the documents within 100 days, they run the risk of locating those documents later, only to have them ruled inadmissible.

Another important part of this amendment is that, under these new rules, the other side can request the document in native format. Generally, this is because they want the metadata associated with it.

The courts have also said that, during an initial search, companies need to look at reasonably accessible information in terms of discovery. In general, this means anything on an active disk or on recent backup media. If the other side forces a company to go beyond what is “reasonably accessible,” the company can potentially ask them to pay for the search.

Retention Policies

Companies need a clear retention policy for electronically stored information. Courts immediately look at whether a company involved in litigation has such a policy, and whether they have been following it.

New FRCP Amendments as of Dec 1st, 2006

- **Full and accurate disclosure (Rule 26, 34)**
 - Defines “Electronically Stored Information”
 - Requires early conference between parties in E-Discovery process
- **Establishes standards around “legal holds” (Rule 37)**
 - Prevent loss of information involved in litigation
 - Begins “when a party is under a duty to preserve information because of a pending or reasonably anticipated litigation.”
- **Specifies production formats (Rule 34)**
 - Requesting party specifies form of production
 - Default production format is “native” files
- **Limits fishing expeditions (Rule 26)**
 - Due to “due to undue burden or cost”

Page 5

CONFIDENTIAL Copyright © 2007. May not be distributed or reproduced outside of Confidential without written authorization.

Figure 1

Courts prefer that companies have automated policies with an audit trail.

What a company needs to be able to show is:

- There is a policy.
- The policy has been followed consistently across the entire organization.
- Since litigation began, appropriate documents have been saved.
- Older documents are unavailable because they have been deleted per policy.

The FRCP safe harbor analysis allows routine operations, but requires a legal hold on materials that may be subject to discovery. A company wanting to demonstrate good faith in such an analysis must suspend the operation of systems that destroy electronically stored information.

Many companies put in place e-mail deletion policies, and many try to use a 30-day deletion policy. However, personnel will often archive their e-mail in an “underground” fashion in the face of too-aggressive

deletion policies, which will cause the policy to backfire.

Litigation Hold Processes

Developing effective litigation hold processes requires close cooperation between Legal and IT. Effective litigation hold processes need to take into account:

- Saving required documents
- Notifying personnel that the required documents are being saved
- Ensuring that discovery can be done within days or weeks
- Certifying that the discovery process is finding everything needed

The companies that get into the most trouble are those that do not have effective litigation hold processes and attempt to put them together in real time.

A data map shows where all a company’s records are located and what information they contain. An up-to-date data map must be presented as part of the “meet and confer” session. It is necessary that this map

show everything possible to avoid appearing to hide any information. Creating and maintaining an effective data map is another synchronization of IT and Legal processes.

Because of the requirement for a fast discovery process, some companies will outsource to an e-discovery firm, but there is a high cost associated with this outsourcing. The cost is high enough in some cases that the expenditure could have funded an entire archival strategy that would enable a company to do the discovery process themselves. Much of the discovery process can be done internally, and internal discovery can go faster, more inexpensively, and, in some cases, more in compliance with regulations.

Currently, litigators are most concerned about the defensibility of the discovery process. Companies often worry about the cost of discovery. However, if a company makes a weak initial discovery pass, the other side will make them repeat the search. It is better when there is a process in place with the correct tools and technology to make an effective pass; this makes the process far more defensible and also results in the lowest-cost discovery.

In terms of improving defensibility, many courts are requiring an IT staff member to be conversant with the information, where it is, how it is managed, and how it was searched. These staff members may be required to testify as well.

Litigation Readiness

Figure 2 summarizes the key necessities for a company to be effectively ready for litigation.

What Do the New FRCP Rules Mean?

One key point regarding the meaning of the FRCP amendment is that every case is now an e-discovery case. In the past, many cases would settle or would otherwise be disposed of before discovery became necessary. Now, companies need to move quickly to determine early in the case what information may be pertinent to the case.

Also, the two-tier discovery process has been formalized by Rule 26(b)(2)(B), which requires the identification of sources too burdensome to search. That identification, made by the producing party, can be

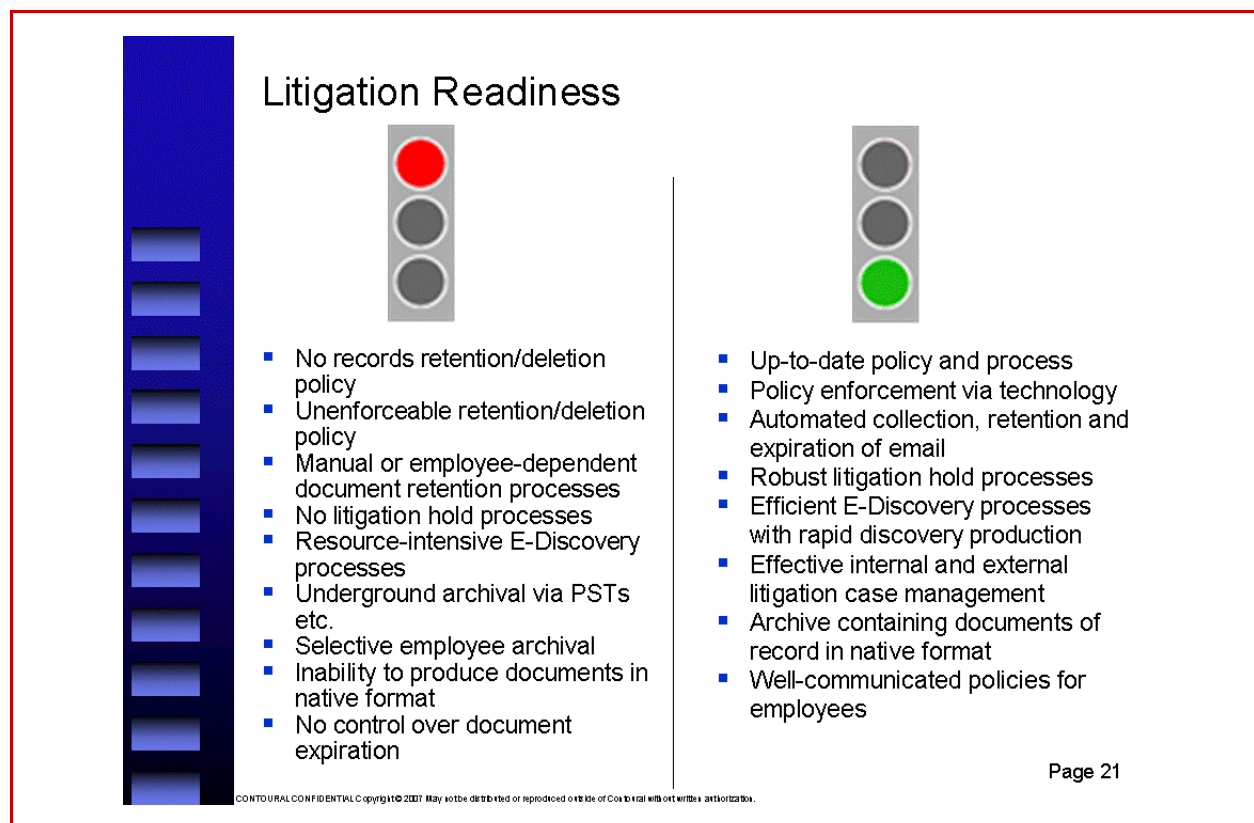


Figure 2

challenged, but opponents will generally focus on information on accessible sources.

Rule 34 mandates the production of materials in a requested format, negotiated format, the format in which the information is ordinarily maintained, or in another reasonably usable format. This means that an organization must understand what it has and exhibit a high degree of control over its enterprise data.

The FRCP does not:

- Change the substance of retention obligation
- Require companies to retain everything forever
- Require a designated IT representative to liaise with the court (though some states, such as Delaware, may require it)

Electronic Discovery Reference Model (EDRM)

An industry group called the Electronic Discovery Reference Module (EDRM) group has created a graphic of the e-discovery flow, shown in Figure 3.

Before the triggering event, an organization is in information governance mode: that is, maintaining records management and the policies and procedures around retention, deletion, storage, and backup.

Once a triggering event occurs, the company knows of or reasonably anticipates litigation. The company will be asked to preserve information that is potentially relevant. Therefore, the first thing the company needs to do is identify that information. One major focus is e-mail.

CA has created a tool that enables a company to archive e-mail, search it, and create a hold on relevant e-mails. This reduces the collection and processing phases shown in Figure 3. CA aims to reduce or remove the processing phases from e-discovery because they will have been performed in the ordinary course of business.

IT and Legal Disconnect

There is currently a large disconnect between IT and Legal. Current e-discovery is a services-based reactive set of processes that is managed by an outside law firm. Very little technology is able to help perform

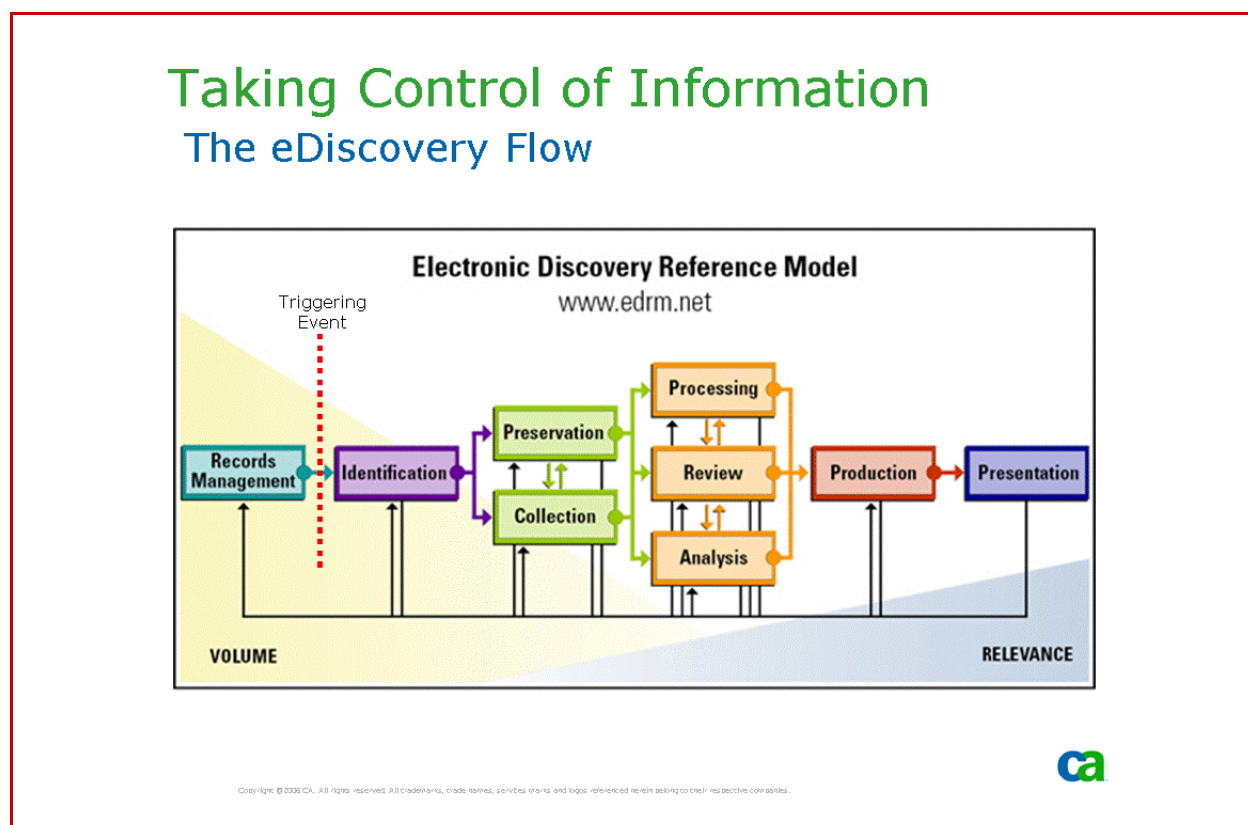


Figure 3

some of the tasks in e-discovery; this sort of work is generally billed by volume and results in a high cost. The control of the process is in the hands of a company outside the organization, resulting in a high business risk. The ultimate goal of CA and its tools is to help reduce this risk by returning control of the process to the organization.

Elements of the disconnect include:

- IT owns the data; Legal owns the discovery process.
- Legal responds on behalf of the organization to mandate the discovery process.
- IT must accomplish whatever Legal asks with scarce IT resources.
- IT may have to stop recycling backup media to meet the preservation obligation, which creates additional burdens on the organization.
- Legal is primarily responsible, but must rely on IT for critical tasks.

IT and Legal each have their needs in terms of the e-discovery process. For instance, IT wants:

- Manageable data stores
- Server performance
- Reasonable time for backup
- Ability to recycle backup media

Ideally, IT would like to hand the discovery process over to Legal. Legal wants:

- Defensible preservation and collection methodology
- Minimized disruption to the business

- Searchable electronic document universe
- Management of e-mail when necessary
- Discovery as a business process and investment

With an investment in the discovery process, the company can realize lower costs in the future. A key side benefit to automation is the ability to take the end users out of the preservation part of discovery.

Connecting Legal and IT

CA has created a technology platform that helps connect Legal and IT. One major feature is the ability to institute and administer multiple legal holds. There is no limit to how many holds can be applied or created, and any one given e-mail message or document can be subject to as many holds as there are. The e-mail is collected at the time of the hold creation, and is transparent. The collection does not generate a notice to the end user, which is helpful during internal investigations where investigators do not want to notify users that their e-mail is being collected. These messages are then indexed so that they are searchable. This makes it possible for discovery to be done without involving a third-party service company.

CA's technology reduces e-discovery costs, eliminates backups except for disaster recovery, and makes the e-discovery process predictable, understandable, and a repeatable business process. It improves the defensibility of the process and increases compliance. The single-instance storage means reduced storage costs, and the retention management means that if a record reaches the end of its lifetime and is not subject to a hold, it can be deleted. Finally, it clarifies the discovery process so it can be used to guide litigation strategy.



About TechTarget

We deliver the information IT pros need to be successful.

TechTarget publishes targeted media that address your need for information and resources. Our network of technology-specific Web sites gives enterprise IT professionals access to experts and peers, original content, and links to relevant information from across the Internet. Our conferences give you access to vendor-neutral, expert commentary and advice on the issues and challenges you face daily. Our magazines—*CIO Decisions*, *Information Security*, and *Storage*—give you in-depth analysis and guidance on the critical IT decisions you face. Practical technical advice and expert insights are distributed via more than 80 specialized e-Newsletters, and our Webcasts allow IT pros to ask questions of technical experts.

What makes TechTarget unique?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals. We leverage the immediacy of the Web, the networking and face-to-face opportunities of conferences, the expert interaction of Webcasts, the laser-targeting of e-Newsletters and the richness and depth of our print media to create compelling and actionable information for enterprise IT professionals. For more information, visit www.techtarget.com.

CA_09_2007_0020