EMC^2
where information lives®

EMC PERSPECTIVE

(Re)-Discovering the New Rules

When information comes together,
your world moves ahead.

Broad changes to the Federal Rules of Civil Procedure (FRCP) became effective December 1, 2006. The changes address issues related to the discovery of electronically stored information (ESI), including e-mail, instant messaging, and user-created documents such as word processing and spreadsheet files.

These new rules potentially affect every company transacting business in the United States, and serve as a guideline for many related state court rules. Despite this broad applicability, a survey at the time the new rules became effective revealed that 95 percent of companies were not fully prepared for the changes. As late as June 2007, 53 percent of respondents freely admitted they were still not ready, while almost one-third were still unaware of the amendments.

Much has already been written about the details of the amended FRCP. The goal of this paper is not to analyze the rules, but to provide practical guidance on assessing their impact and addressing the obligations they create.

Five Easy Pieces

1. Ready, Set: 12/1

A starting point, not a finish line

Unlike Y2K and the more recent Sarbanes-Oxley requirements, the December 1, 2006 date for the amended Federal Rules is not an all-or-nothing, pass-fail test. Nor is there really any way to be "in compliance" with the Rules—they are requirements for litigants in Federal Court, and each case presents its own specific challenges.

However, you could be subject to the new rules without further warning—maybe even with your company as the plaintiff. Obligations to provide information begin within the first 100 days after a lawsuit is filed, so get started right away by obtaining at least a basic familiarity of the electronic discovery process and the amended rules. Because the rules focus on your IT enterprise, find out whether you have existing work that you can leverage—perhaps a SOX or an IT security audit, a Daylight Savings change checklist or a data classification overview.

2. Legal, meet IT—IT, meet Legal

Cross functional communication is key

Contrary to conventional wisdom, IT teams at many companies are the drivers behind eDiscovery and policies for retention management. At some companies, legal is forging ahead alone, trying to establish policies and processes that may be extremely difficult (if not impossible) to implement in their IT infrastructure. Alone, both legal and IT departments are doomed to failure.

Successful eDiscovery planning and efficient processes require, as a starting point, both IT and legal to work together. Other groups, such as compliance, records management, and business unit leaders, are also critical to a successful process.

3. ESI is Everywhere

Know your sources and plan your litigation holds

Today's IT infrastructures have ESI in almost every nook and cranny. Certainly e-mail and file shares are front of mind, but have you considered instant messaging? What about Wikis, blogs, voice mail, pen drives—or those "tiny" 32 GB storage cards tucked away in cell phones? Has anyone walked around the IT staging area to determine whether there is a computer graveyard where old PCs and laptops go to die—but retain all of their data?

[1] Survey: Companies Not Prepared For New Federal Rules, 11/21/06, http://www.computerworld¬.com¬/action/article¬.do?command¬=view¬ArticleBasic¬¬&articleId=9005298&pageNumber=1

[2] LiveOffice Survey, 6/25/07, http://www.liveoffice.com/¬newsroom/PR/¬06-25-2007.asp

Consider developing a map of your IT data sources that can be used by the legal department in evaluating discovery requests and preparing for your early Rule 26 conferences. In addition, a practical, reasonable litigation hold process is invaluable.

4. Tiers Not Tears

Not all data is equal

One of the keys to meeting the new obligations is an actual understanding of your ESI—not just that it exists, but where, how, and on what media it is stored, how it is being used, backed up, etc. Data that is relevant and "reasonably accessible" will need to be part of the discovery process. However, data that is "not reasonably accessible" may not have to be provided at all—or the other party may be required to pay for all or part of the cost to collect that data.

Determining what is "not reasonably accessible" can depend upon a host of factors, including the cost of accessing the data, the importance of the data to the issues, whether the data is available from a less costly source, and how the company ordinarily uses that data. Keep in mind that backup tapes should not be used as archives—they should be for business continuity. And remember that even if you take the position that ESI as "not reasonably accessible," it needs to be preserved if relevant—the court could later require its production.

5. Keeping it Native and Preserving Metadata

Understand the issues

Once potentially relevant ESI has been identified, it will eventually need to be collected if the case proceeds. But be careful—the days of meeting your discovery obligations by printing out e-mail messages and files are (mostly) gone. At minimum, you should preserve your ESI in its "native" format, and certain cases may even test your ability to preserve "metadata."

Simply put, maintaining a file in its native format is as simple as keeping a word file as, well, a word file. Converting it to another format—say a PDF or TIFF—can make it more difficult for parties to store and search. Normally you will agree to a format with your opponent (sometimes with the help of the Court), which may be native or a "picture" format like PDF, but you will want to maintain the ESI in its native format until that point to preserve your options. And even in those rare cases where your opponent will inexplicably accept printouts, you may want to retain native data for your own use.

A related issue is metadata—sometimes defined as "data about data." While the amended rules do not directly address metadata, many litigants request metadata as a regular part of their discovery requests. But be careful to understand what their request really means. Metadata is typically defined to include at least two different types of data: file system data that is directly related to but stored separate from a file (date created, date last accessed, owner, etc.) and frequently maintained by an operating system; and other "hidden" data that is contained within a source document file but not always readily apparent to the user. This may include versioning data in a word processing document, formulas and hidden cells in spreadsheets, or even metadata that is specifically identified as metadata, such as the properties field of a word document. Sometimes the mere accessing or copying of a document can change its metadata, so understand the issues about metadata.

Action Plan

How you proceed will depend on many factors, but at a minimum you may want to consider the following:

- Establish a cross-functional committee, consisting of legal, IT, compliance, and records management, along with executive sponsorship, to look at your information management and records management policies.
- Understand your highest risk and pain points, and prioritize accordingly; implementing a real "E-mail Management" policy, with technology to enable and enforce the policy, is a common starting point.
- Evaluate your mountain of backup tapes and legacy data systems, both onsite and offsite; determine whether you have a business reason to save this ESI and whether you can responsibly destroy or reduce this data.
- Study your eDiscovery costs, risks, and processes, and make them more efficient and repeatable; consider leveraging technology as part of the process.

EMC²
where information lives®

EMC Corporation
Hopkinton
Massachusetts
01748-9103
1-508-435-1000
In North America 1-866-464-7381
www.EMC.com