



August 2004 Proposed Civil Rule Amendments—E-Discovery and Archiving Impact

By Greg Buckles

Sr. Product Manager, E-Discovery

Please Note: This paper is provided for general informational purposes only and is not legal advice. If you require legal advice for your specific circumstances, please consult with a competent attorney licensed to practice in your jurisdiction.

What is E-Discovery?

E-Discovery is a generic term used to encompass how the legal world of litigation, regulation, and criminal investigation searches, collects, processes, and produces electronic files. The scope of these activities can range from an expensive forensic reconstruction of file fragments on a laptop hard drive to corporation-wide searches and retrievals. Finding and collecting any relevant files are just the first step. In civil cases, the collection must be reviewed to find files protected under legal privilege or needing special treatment to preserve confidential business information. Most of the time, the responsive “native” electronic files are converted to numbered paper or images for production, a costly and imperfect process. A good overview of E-Discovery can be found at the Electronic Discovery Reference Model at www.edrm.net.

How does E-Discovery affect IT?

The IT department procures and maintains the servers, storage, and systems where these files reside. Enterprise-wide document management and archiving systems are increasingly the target of ever-expanding discovery requests. The scope of what is required versus what is reasonable changes with every major ruling. This has created confusion and contention in those charged with responding to legal requests. Consultants, law firms, and legal vendors have reaped enormous profit from this lack of firm guidance in the law. New federal rules of civil procedure have been proposed that will have a great impact on corporations and the systems they choose to manage their files, new and old.

How did we get here?

The U.S. civil courts have been relatively slow in adapting to the shift from paper documentation to electronic communications and records. It is an accepted fact that the majority of “business records” are never even physically printed any more. In 2004, Judge Shira A. Scheindlin made some of the first strong decisions regarding discovery and production of electronic records, specifically email, in the *Zubulake v. UBS Warburg* case.¹ Responding to these and other court decisions, the Sedona Conference Working Groups issued general guidelines for electronic discovery in January 2004.²

¹ *Zubulake v. UBS Warburg LLC, et al.*, S.D.N.Y. 02 CV 1234 (SAS) 7/20/04; 2004 U.S. Dist. LEXIS (S.D.N.Y. July 20, 2004).

² www.thesedonaconference.org

Addressing these issues on a case-by-case basis generated an overwhelming demand for better rules dealing with electronic evidence. A series of amendments to the Federal Rules of Civil Procedure were drafted in August 2004. These proposals were posted for public comment, and public hearings/meetings were held in various locations within the United States over several months. While the bulk of the comments were made by plaintiffs' attorneys arguing for better access to corporate data, there was also a lengthy comment by Microsoft. At present, these rules have passed the comment stage with little revision and may come into effect as early as December 31, 2006.

The purpose of this white paper is to quickly familiarize you with the changes in the Rules of Civil Procedure and their potential impact on corporate customers. It is important to keep in mind that these rules have not been interpreted nor argued before the courts yet, and so their final application is yet to be known.

Rule 16, Rule 26(f), and Rule 35—Early discovery conference and discovery plan

These rule changes mandate a pre-discovery meeting between the parties to discuss issues regarding the protection, discovery, and production of relevant electronic data. Any potential agreements for waivers of inadvertent production of privileged material should be discussed at this meeting. The important point here is that corporate defendants will have to disclose all sources of potential data and means of search/retrieval, and theoretically negotiate potential discovery parameters, e.g., search criteria.

This is a dramatic change to long-standing procedures and effectively requires the parties to “put their cards on the table” instead of participating in the normal rounds of interrogatories and answers. The courts expect the parties to come to a reasonable agreement and submit a discovery plan. This expectation of reasonableness will have to be rigorously enforced by the courts if it is to succeed. In extreme cases, the threat of sanctions or judicial instructions may be required to define the limits of reasonableness.

This means that IT departments should immediately begin to prepare a detailed inventory of data assets, systems, retention policies, backup strategies, employee termination protocols, and everything else that might impact discovery. An integrated message management system will ease this burden and abate the risk of court sanctions for failure to disclose requested email.

Rule 26(b)(2)—Exemption of “inaccessible” electronic information excepting court order for good cause

This change potentially exempts offline or tape backups from the normal course of discovery, though their existence must be declared in the initial discovery conference. This exemption was harshly criticized by plaintiff attorneys and academics as giving the big corporations a way to hide or protect data. The definition of “reasonably accessible” becomes critical, though the dividing line seems to be drawn between spinning and non-spinning media. The burden is on the responding party to demonstrate that information is not “reasonably accessible.”

There is a provision that allows sampling to verify the likelihood of relevant information and relative burden. Plaintiffs’ attorneys may argue that all corporate data should be considered reasonably accessible in light of new governance and accountability standards such as the Sarbanes-Oxley Act of 2002. The corporate archiving system must integrate with tiered storage systems to avoid costly tape restorations by vendors.

Most discovery happens within a 30- to 90-day period, forcing corporations to use outside resources when they must reach back to “inaccessible” data without the appropriate system capabilities.

Rule 26(b)(5)(B)—Procedure for asserting privilege after production—Claw-back and Quick Peek provisions

“Quick peek” provisions are used to allow an opposing side a brief inspection of large volumes of paper records in order to cut down on the number of unrelated documents that have to be reviewed prior to being produced. A “claw-back” agreement potentially allows the retrieval of documents inadvertently produced. At first, this new procedure seemed to offer an excellent opportunity to simply turn over everything to the requesting party without the expensive privilege review process. Unfortunately, recent U.S. and international decisions have seriously undermined confidence in any kind of “after-the-fact” retraction of privileged or otherwise protected materials.³

Until the accuracy of search and categorization technologies exceeds that of manual review by counsel, corporations are unlikely to utilize this procedure. The time period to identify and retract documents is just too short to be feasible in large-scale productions. However, the filters and policy management tools being integrated into the Symantec Enterprise Vault™ platform can substantially reduce the time and risk of review or even online preview. The same systems used in intelligent archiving will help by categorizing files and email well before the review.

³ *Atronic International GmbH v. SAI Semispecialists of America, Inc.*, 2005 WL 2738914 (E.D.N.Y. Oct. 18, 2005); Assertion of 30-day notice, *Burlington N. & Santa Fe Ry. Co. v. United States Dist. Court for Dist. of Mont.*, 2005 WL 730193 (9th Cir. 2005); *Steadfast Ins. Co. v. Purdue Frederick Co.*, 2005 WL 3511085 (Conn. Super. Ct. Nov. 30, 2005)

Rule 33(d)—Allows responding party to answer by providing access to information so long as the burden of deriving information is same for both parties (i.e., access to in-house search technology)

This procedure differs from Rule 26(b)(5)(B) in that the requesting parties are allowed access to the data on the responding party's system. They can use the same search tools to find and designate documents that they want, but the responding party then reviews this much smaller set for privilege before production. The rule requires a reasonable time to inspect (search) and review the requested files.

This rule holds great potential for the use of a tool such as Enterprise Vault Discovery Accelerator through an onsite workstation or secured Web page. There are several technological hurdles to overcome to make this process strategically attractive beyond the obvious cost savings, but Enterprise Vault is well positioned to take advantage of this avenue.

Rule 34(b)—Authorizes the requesting party to specify the form of electronic production; requires specific requests; production in native or “electronically searchable form”

Until very recently, all email and native electronic files were literally printed to paper or images and numbered by page for production to the requesting party. This allowed for easy authentication and use as exhibits in court. However, a 1-megabyte Excel worksheet might become 5,000 pages when converted to printed format. Many email attachments, such as voice mail messages and video clips, are just not suitable for printing.

The modified rule allows the requesting party to specify their preferred format for the production and allows the responding party to object for reasons of undue burden, expense, or feasibility. If the parties cannot agree, the rule defaults to production of the files as “kept in the normal course of business,” i.e., in their native electronic format. There is no perfect solution to this complex issue as yet, but be aware that Enterprise Vault can produce email in a variety of formats along with reports to ease tracking and authentication issues. A corporate archiving system should ease the burden of requests and be able to restore defensibly authentic copies of the original native file or email.

Rule 37(f)—“Safe Harbor” for loss of information due to routine system operations

This rule acknowledges the fact that network environments are dynamic, constantly altering files and data without human intervention. It provides for limited protection from the harsh sanctions and even criminal charges mandated in many of the new laws such as the Sarbanes-Oxley Act. However, this exemption of data lost to routine electronic systems only applies when the responding party has made a documented good faith effort to preserve the data. The implementation of a “litigation hold” is required as soon the party reasonably anticipates legal action. So corporate clients must have a plan of action and be able to defend it. Taking every potentially relevant backup tape in a corporate system out of circulation can cost hundreds of hours of labor and hundreds of thousands of dollars. Many legal cases can go for years before actually being resolved.

The new litigation hold capability of Discovery Accelerator allows customers to dynamically manage holds on email and files already held within their Enterprise Vault system in a single instance environment rather than holding hundreds of copies of the same files on monthly tapes.

Rule 45—Subpoena

Rule 45 brings the language covering the issuance of subpoenas into step with the other rule changes.

Conclusion

Corporations have a lot of work ahead of them to prepare for these changes. Many legal and IT departments have not contemplated the ramifications of disclosing every potential repository of electronic data relevant to every piece of civil litigation filed against them. Most corporations, whether plaintiff or defendant, will have a hard time even defining all the locations, types of data, means of search, and means of retrieval, much less have the resources to do this without bringing in expensive consultants and vendors. Once the requesting parties (plaintiffs) understand how this expands the potential scope and scale of productions, they will happily leverage this dramatic increase in overhead to force corporate defendants to settle, even when their cases have little or no merit.

Corporations must have access to all potentially responsive data to minimize the cost and manage the impact on IT and legal departments. Some corporations may try to push everything to tape to make data “inaccessible,” but it will take only one big case to force them to restore, to counter a hundred cases where they win the “inaccessible” argument.

Besides preparing for these new legal procedures, effectively owning and managing all aspects of the user knowledge base creates a vast array of business positives. Sarbanes-Oxley got a bad reputation for creating burdensomely complex tracking systems and bogging down infrastructure support. Preparing for these changes actually creates the opportunity for corporations to take control of important business knowledge scattered across their network in hidden shares, buried on encrypted laptops and in password-protected .PST files.

Enterprise message and file management systems allow security, legal, ethics, and audit departments to readily assess potential risk and liability for all kinds of matters. These rule changes expose the inner workings of the corporate infrastructure to hostile view. A corporation that cannot rapidly and defensibly find relevant electronic files will face escalating legal costs and unnecessary disclosure of vital corporate documents.

Symantec Enterprise Vault Discovery Accelerator 6.0

Symantec Enterprise Vault Discovery Accelerator 6.0 extends the basic search functionality of the Symantec Enterprise Vault message and file archiving software to help customers address amendments Federal Rules of Civil Procedure, scheduled to take effect December 1, 2006. These amendments set firm guidelines for the E-Discovery process, what records an organization should be prepared to produce and in what format.

Discovery Accelerator 6.0 enables the creation of automated legal holds, ensuring all e-mails, instant messages, files and other content relevant to a specific case or cases are not deleted as part of an organization's records retention and deletion schedule. Discovery Accelerator 6.0 also features a flexible search capability, which provides ad-hoc preview searches in addition to formal discovery searches. This allows an organization to respond to a discovery request to quickly determine the scope of a particular discovery request. Finally, Discovery Accelerator 6.0 can export archived files to their native format and directory structure, enabling responding parties to produce these files more quickly while skipping the expensive image conversion process.

More information can be found at www.symantec.com/enterprise_vault.

About Symantec

Symantec is the world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information.

Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries.

More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com

Copyright © 2006 Symantec Corporation. All rights reserved. Symantec, the Symantec logo, and Enterprise Vault are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners. Printed in the U.S.A.
08/06 10757481