The New E-Discovery Amendments to the Federal Rules: Act Now To Manage Risks, Save Time, Reduce Costs and Avoid Embarrassment

December 7, 2006

THE AMENDMENTS

On December 1, 2006, e-discovery amendments to the Federal Rules of Civil Procedure became effective. The new amendments govern electronic discovery in cases filed in federal courts, including pending cases.[1]

The amendments recognize a new category of discoverable material called "Electronically Stored Information" – ESI.[2] They also address four broad topics:

1. The amendments require parties and the court to give attention to electronic discovery at the outset of a lawsuit. The parties must address e-discovery in their early "meet and confer" conferences and in their initial disclosures.[3] The court must address e-discovery in its scheduling order.[4]

2. The amendments provide for phased discovery. Initially, the amended rules require early production of relevant, non-privileged, and reasonably-accessible ESI. Subsequently, a court order is required for production of ESI that is "not reasonably accessible because of undue burden or cost".[5]

---

1 The amendments include changes and additions to Rules 16, 26, 33, 34, 37 and 45. They also include changes to Form 35 ("Report of Parties' Planning Meeting"). The amendments and related material are available on the Web site maintained by the Administrative Office of the U.S. Courts. *See* Administrative Office of the U.S. Courts, Amendments Approved by the Supreme Court – Submitted to Congress April 2006 (Effective December 1, 2006) <http://www.uscourts.gov/rules/congress0406.html>. The e-discovery amendments with Advisory Committee Notes are available at <http://www.uscourts.gov/rules/EDiscovery_w_Notes.pdf>.

2 *See* Fed. R. Civ. Pro. 34(b).

3 Fed. R. Civ. Pro. 26(a) & 26(f); Form 35.

4 Fed. R. Civ. Pro. 16.

5 *See* Fed. R. Civ. Pro. 26(b)(2).

3. The amendments formalize the recognition of so-called "claw back" arrangements whereby parties agree that if privileged material is produced inadvertently, the receiving party must return, sequester or destroy the data and cannot use or disclose it until resolution of the privilege claim.[6]

4. Finally, the amended rules recognize a so-called "safe harbor" to protect against sanctions for the inadvertent loss of data as a result of the routine, good-faith operation of an electronic information system.[7]

STEPS TO CONSIDER

There are steps that businesses may wish to take to improve risk management, to save time and to reduce litigation costs under the amended rules. A few are discussed below.

Create an ESI Source Map – Under the amended rules, counsel representing your business will be required to understand quickly your firm's computer network, the technologies and technological workflows that your firm has deployed, as well as the sources of ESI that could be relevant to the disputed matter. Your business should prepare to educate its counsel quickly and effectively.

One way to prepare is to develop an "ESI Source Map" that identifies all locations where ESI may be found. An example of such a map is the "Client Server Architecture Diagram" prepared by Microsoft Corporation as part of the comment process involving the rules amendments.[8] The diagram graphically depicts examples of potential ESI sources within a model corporation.

Such a map may be used to help counsel understand where ESI is located and what ESI is "not reasonably accessible". It might also be used to help counsel understand as quickly as possible automated technologies and workflows[9] that might lead to inadvertent loss of potentially relevant

---

6 *See* Fed. R. Civ. Pro. 26(b)(5).

7 *See* Fed. R. Civ. Pro. 37(f) ("Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.").

8 *See* Microsoft Corporation Comments on the E-Discovery Rules Change Proposals, E-Mail from Greg McCurdy to Peter McCabe, Aug. 25, 2004, p. 29 (unnumbered last page of a 29-page PDF document available at < http://www.uscourts.gov/rules/e-discovery/04-CV-001.pdf >).

9 An example of an automated technology that might lead to inadvertent data loss is the automatic deletion of e-mails that are more than 30 days old. Examples of "workflows" that might lead to inadvertent data loss include such activities as: (1) the routine replacement of an executive's failed computer hard drive and disposal of the original drive even though it might contain material that could be recovered forensically, if it became necessary; and (2) the cleansing of an executive's hard drive when the lease period for the executive's computer nears

data so that effective "litigation hold" preservation instructions can be issued expeditiously. This, in turn, may improve the company's chances of successful reliance on the new "safe harbor" in the event of later inadvertent data loss.

Providing counsel with a detailed Map of ESI Sources will save valuable time. Moreover, it will avoid "reinventing the wheel" in each lawsuit and the expense of having outside counsel conduct an investigation to locate sources of ESI.

Preparing a Map of ESI Sources also may reduce litigation risks. A business cannot protect itself effectively against spoliation claims if it cannot identify for its counsel where the ESI that must be preserved is located. Moreover, unless the business educates its counsel regarding its computer systems and data storage practices, it will be difficult for counsel to negotiate reasonable time frames for production of ESI and reasonable limits on the scope of such productions.

Assign Experienced ESI Stewards for Each Data Source – Most businesses have at least one knowledgeable individual with responsibility for each ESI source. For example, typically there are internal "experts" who deal with e-mail, backup systems, document management systems, legacy systems, desktop PCs, e-commerce servers, finance systems, human resource systems, *etc.* At least one experienced ESI "steward" should be assigned for each ESI source that may contain potentially relevant data in the event of a lawsuit. Current contact information for such individuals should be maintained on a single list or, if feasible, included on the Map of ESI Sources proposed above.

Designate such stewards for each location that contains active, inactive or archived data (including disaster recovery and backup systems). Ensure that such personnel are well trained regarding the organization's retention program, litigation hold process and the speed with which preservation issues must be handled. Consider educating such personnel regarding the new e-discovery amendments to the Federal Rules of Civil Procedure.

Conduct a Review of the Litigation Hold Process – Existing discovery rules require parties to impose a "litigation hold" on all potentially relevant documents once litigation is commenced or reasonably anticipated. Most large businesses already have developed a litigation hold process. It is critical, however, that once an ESI Source Map is created, the company should also review its litigation hold process in light of that map; the two must be in perfect harmony.

Conduct a Review of the Retention Policy – The business likewise should review its "document" retention policy to ensure that all data sources encompassed within the ESI Source Map are adequately addressed in the retention policy. Indeed, the creation of an ESI Source Map presents an opportunity to update the retention policy not only to ensure that all data sources are addressed but also to ensure that the company has appropriate procedures to dispose of electronic data once it no longer is needed.

---

expiration with the good-faith intent that the leased computer should be returned to the lessor free of confidential business data.

Consider Whether To Centralize In-House Legal Oversight of E-Discovery – It may be appropriate, in certain circumstances, to designate one or more in-house attorneys to oversee all e-discovery for the business. Experienced and knowledgeable oversight can improve the speed with which issues that arise under the newly-amended rules are handled.

For example, if the business is faced with multiple litigations involving discovery of ESI, it is possible that numerous litigation holds exist throughout the organization covering overlapping personnel, time periods, systems, *etc.* Ensuring that in-house counsel responsible for oversight of all such discovery are fully aware of the nature and scope of all such litigation holds can avoid problems that may arise when a previous litigation hold has resulted in preservation of data that becomes relevant to a later dispute. Centralized management by in-house counsel can avoid the problems that might otherwise arise if material preserved for one litigation is overlooked in connection with assessing ESI issues in a subsequent dispute. Moreover, the efficiencies and knowledge gained by repeated oversight of such matters cannot be underestimated, particularly now that electronic preservation and ESI issues must be addressed with such dispatch at the outset of a case.

Prepare Now for the Difficult Issues – Identify ESI sources likely to be the subject of negotiation and possible dispute in cases involving your business. Such an analysis should proceed together with the identification of ESI that might be deemed "not reasonably accessible" but should involve much more than merely "mapping" problematic ESI sources.

Consider, for example, so-called legacy systems, large relational databases, customized or proprietary main frame computer systems and short-lived data systems (*e.g.*, systems in which data turns over so frequently it is hard to reconstruct the past). The company should consider – in advance – the positions it is willing to take when faced with discovery demands that encompass data within such systems.

In this regard, the Advisory Committee Notes to the newly-amended rules state that when a responding party asserts that requested ESI is not reasonably accessible:

> "The requesting party may need discovery to test this assertion. Such discovery might take the form of requiring the responding party to conduct a sampling of information contained on the sources identified as not reasonably accessible; allowing some form of inspection of such sources; or taking depositions of witnesses knowledgeable about the responding party's information systems.
>
> Once it is shown that a source of electronically stored information is not reasonably accessible, the requesting party may still obtain discovery by showing good cause, considering the limitations of Rule 26(b)(2)(C) that balance the costs and potential benefits of discovery."[10]

[10] *See* Fed. R. Civ. Pro. 26(b)(2) (Committee Note by the Advisory Committee on Civil Rules).

Accordingly, the company may wish to identify such systems in advance and prepare for each such system a clear statement of the company's positions regarding technical issues, undue burden, undue cost and cost/benefits issues. Preparing thoroughly in such a fashion will reduce the time and expense associated with litigation counsel having to investigate and prepare such arguments once a discovery dispute arises.

CONCLUSION

Electronic discovery is burdensome and expensive. The newly-amended e-discovery rules will reduce neither burden nor expense. Following steps such as those outlined above, however, may help your business better manage both the legal risks and expenses associated with e-discovery under the newly-amended rules.

* * *

This memorandum is for general information purposes only and should not be regarded as legal advice. Please contact your relationship partner if we can be of assistance regarding these important developments. The names and office locations of all of our partners, as well as additional memoranda regarding recent legal developments, may be obtained from our Web site, *www.simpsonthacher.com*.