

## Federal Judges Association Newsletter November 29, 2006

### FAQ's of E-Discovery

by Judge Shira A. Scheindlin, S.D. N.Y.

#### The Ten Most FAQ's in the Post-December 1, 2006 World of E-Discovery

Every reader of this article knows that on December 1, 2006, the Federal Rules of Civil Procedure will embrace the 21st Century world, where 95% of records are electronically created and stored and all discovery is now e-discovery. It is no longer necessary to summarize these Rules, which have been discussed at uncountable conferences and in innumerable articles for more than five years. In deference to that reality, I will, instead, attempt to write pithy and hopefully helpful answers to what I believe will be the FAQ's of the first five years of the new era that will forever be known as the "2006 Amendments."

#### 1. When is the duty to preserve triggered?

The short answer is when litigation is reasonably anticipated (at the earliest) and when litigation is begun (at the latest). How does one conclude that litigation is reasonably anticipated? Obviously courts will answer this question with hindsight if they are asked to impose a sanction because a party failed to take steps to preserve data. Some of the questions a court might ask would include: Did an organization create a process for evaluating the threat of litigation? Was a response team created to assess the threat and report to a responsible decision-maker? Did the decision-maker evaluate the threat in light of prior experience with similar facts and circumstances? In evaluating the credibility of the threat, other questions might be asked: Was the threat made by a known or unknown person or entity? Did the threat arise from a regulatory action or criminal proceedings? Did the threat arise from a respected attorney sending a notice to preserve? Did the threat arise from an event such as a plane crash or plant explosion? Did responsible media coverage alert the company of similar actions involving similar products or issues?

The list could be longer, but these questions should provide some guidance to decision-makers who must develop criteria to assess whether information they obtain would persuade a reasonable person to anticipate that litigation is likely to occur.

2. Does an entity have to suspend its routine document retention system when it reasonably anticipates litigation?

The short answer is yes. Rule 37(f) protects a party from sanctions if information is lost as a "result of the routine, good faith operation of an electronic information system." This Rule simply means that a court will not punish a party for the routine good faith deletion of information through recycling and overwriting. But once litigation is brought or reasonably anticipated, a party cannot put its head in the sand and continue the routine operation of its electronic information system, because then it would not be acting in good faith. It must do something to preserve relevant information. In short, it must suspend some part of the routine operation of the system to take account of its preservation obligation.

3. What is a litigation hold?

A litigation hold involves three components: (1) Identify and preserve relevant information when litigation is reasonably anticipated, or, at the latest, when it is commenced. In deciding what to preserve, a party must consider the nature of the issues raised; the experience of the company in similar circumstances; and the amount in controversy; (2) issue a written notice of the hold, clearly defining what information is to be preserved and how the information is to be maintained, to those employees most likely to have the relevant information; and (3) monitor compliance.

4. Does a party have to preserve inaccessible data that it does not have to search or produce under Rule 26(b)(2)(B)?

This must be the most frequently asked of the top FAQ's. The answer provided by the Advisory Committee in its Note on Rule 26(b)(2)(B) is that this will have to be left to the good judgment, and risk tolerance, of the decision-maker at the company. The Committee Note states that "[o]ne factor [that bears on the preservation obligation with respect to inaccessible data] is whether the [responding] party reasonably believes that the information on such sources is likely to be discoverable and not available from reasonably accessible sources." See, e.g., *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309 ("If unique, relevant information exists on backup tapes, a party may be obligated to preserve and review such tapes."). The inverse must then be true. If the information on such sources is not likely to be discoverable, most likely because it is not relevant, then there is no need to preserve the source. Similarly, if the information on the inaccessible source is likely to be available from an accessible source, then there is no obligation to preserve the inaccessible source. Finally, a company is entitled to conduct a cost benefit analysis under newly numbered Rule 26(b)(2)(C). If the burden of preservation is extraordinarily high and the potential benefit is low, there should be no need to preserve.

But if the cost of preservation is low to nil, which will often be the case, considering that the inaccessible source has been located and identified, and the risk of losing potentially relevant data is high, then preservation may be a wise decision. Common sense and good judgment, together with a review for reasonableness, will likely become the standard for judging such decisions.

5. What exactly are inaccessible sources and when should production from such sources be permitted?

Back-up tapes are the first source that comes to mind. These are considered inaccessible because they often have no organizational structure, are not indexed in any way, and are difficult to search. See *The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production*, Comment 5.b (July 2005) ("Absent specific circumstances, preservation obligations should not extend to disaster recovery backup tapes created in the ordinary course of business. . . . [E]mploying proper preservation procedures with respect to the active system should render preservation of backup tapes on a going-forward basis redundant."). Other sources might include "legacy" or "orphaned" data, both of which are found in sources that are no longer in use and are not supported by current technology. Retrieving data from such sources would require expensive restoration efforts, including rebuilding of platforms and operating systems needed to access the data. The Rules define inaccessible sources as those that cannot be accessed without undue burden or expense. While the Rules give no other definition, I can add that the term should be defined functionally rather than generically, because a source that is inaccessible today might well be accessible tomorrow given changing and improving technology. Functionally speaking, then, an inaccessible source is one where a party would have to acquire or create software to retrieve potentially responsive information or would otherwise be required to render inaccessible information accessible (e.g. restore/translate), which is always an expensive proposition.

6. If a court incorporates the agreement of the parties with respect to privilege waiver in its Rule 16 Order, will the parties be protected if a third party (non-party) asserts that the privilege has been waived by production?

Most likely not. Two recent cases are required reading on this topic. In *Hopson v. Mayor & City Council of Baltimore*, 232 F.R.D. 228 (D. Md. 2005), Judge Paul Grimm concluded that only if the production of privileged material was compelled by the court could a party successfully defend against a claim of waiver by a non-party. He did not think that the mere agreement of the parties would be effective when a non-party claimed that the production of privileged material in one forum resulted in a waiver. Even more recently, in *In re Qwest Comm. Int'l, Inc.*, 450 F.3d 1179 (10th Cir. 2006), the Court held that production of computerized information to a government agency, pursuant to a confidentiality agreement, resulted in a waiver of privilege as to third parties.

7. When should a court permit a party to conduct an on-site inspection of an adversary's computer system or obtain a mirror image of a computer hard drive?

Rule 34 contemplates that a responding party will search for and produce relevant data; it does not generally give the requesting party the right to conduct the actual search. Yet, courts have permitted mirror imaging in two distinct circumstances: (1) When the computer itself was allegedly used to commit the offense that is the subject of the suit (i.e. downloading an employer's files for use by a competitor) (see, e.g., *Balboa Threadworks, Inc. v. Stucky*, 2006 WL 763668 (D. Kan. Mar. 24, 2006)); or (2) when there is evidence that computer files that should have been produced were improperly deleted or destroyed (i.e. where email produced by other parties showed that defendant had not produced all responsive documents) (see, e.g., *Leviton Mfg. Co., Inc. v. Nicor, Inc.*, 2006 WL 1305036 (D. N.M. Jan. 6, 2006)).

8. And what is metadata anyway and must it always be produced?

"It's the electronic equivalent of DNA, ballistics and fingerprint evidence, with a comparable power to exonerate and incriminate. Metadata sheds light on the context, authenticity, reliability and dissemination of electronic evidence, as well as providing clues to human behavior. All sorts of metadata can be found in many locations. Some is crucial evidence; some is digital clutter. But because every active file stored on a computer has some associated metadata, it's never a question of whether there's metadata, but what kinds of metadata exist, where it resides and whether its potential relevance demands preservation and production." See Craig Ball, "I Never Metadata I Didn't Like" (January 2006) (unpublished manuscript, on file with author). See also *Williams v. Sprint*, 230 F.R.D. 640 (D. Kan. 2005) (sanctioning a party for "scrubbing" the metadata in a document production, finding that the producing party should have known that the metadata in that particular case was relevant). And now, the answer to the question is it depends. It need not always be produced, but it depends on the circumstances. Sometimes it is highly relevant and other times it is not. This is something the parties should discuss early on, and, if a dispute arises, the court will have to decide. But scrubbing without asking is a bad idea.

9. To shift costs or not, that is the question.

Rule 26(b)(2)(B) has created a two-tiered approach to discovery of electronic data. Accessible data must be produced in the first instance, subject to the proportionality factors set forth in newly numbered Rule 26(b)(2)(C). Thus, cost-shifting is a possibility under those factors but is not particularly likely given our usual rule that the producing party bears its own costs. However, with respect to inaccessible sources, the new Rule requires that if the producing party establishes that a source is truly inaccessible, then the burden shifts to the requesting party to show that there is good cause for nonetheless requiring production from such sources. If the requesting party is successful, then the court may order production from the inaccessible sources but is encouraged to consider cost-shifting or at least cost-sharing. So I expect that cost-sharing will be commonly applied to discovery from inaccessible sources.

10. Fooled you. Nine is more than enough.