Your Company and the New Federal e-Discovery Rules

By Jack Molisani, *Associate Fellow,* and Johnette Hassell

When a lawsuit is brought against a company or individual in the United States, the U.S. legal system requires the defendant to produce information that the plaintiff believes might be relevant to the claims in the case. For example, there have been numerous high-profile cases in the media over the past year in which corporate executives were suspected of insider trading. In such cases, the plaintiffs subpoenaed copies of correspondence sent or received by the executives in the months prior to the event to determine whether they contained evidence that the executives did indeed have insider information and acted on it illegally.

The process by which plaintiffs request such information and defendants produce (or refuse to produce) it is called *discovery*. Each side is said to produce (that is, deliver) material in response to the other's discovery requests.

The U.S. legal system provides a set of rules that governs how the discovery process should be conducted. This article discusses revisions to the federal discovery rules that went into effect December 1, 2006, and how they provide technical communicators an unprecedented opportunity to expand their sphere of influence.

Please note: We are not legal professionals, nor are we qualified to give legal advice. While this article offers a lay interpretation of U.S. discovery rules and suggests actions you can take, you should check with your company's legal team and work with them to help ensure that your company is prepared.

The Old Discovery Rules

For hundreds—if not thousands—of years, "discoverable" information was pretty much limited to written records such as letters, memos, receipts, and so forth. The media on which information was recorded may have evolved from clay tablets to papyrus to office paper, but the content was still *written* (initially by hand, and later also printed).

The invention of computers, however, radically changed how information was stored and transmitted. Instead of interoffice memos, we send e-mails. Spreadsheets have replaced paper accounting ledgers. Customer and relationship management systems, enterprise-wide accounting and finance systems, and other complex data storage and retrieval systems have replaced shoeboxes stuffed with smudged and dog-eared index cards.

With the arrival of the information age, the old discovery rules needed to be updated.

The New Discovery Rules

Since 1938, the U.S. legal system has provided rules for the discovery process. These rules assumed information was produced (delivered) on paper. Several revisions were made over the years—the latest in 2000—yet the rules still contained inadequate provisions for the differences between paper-based and electronically stored information (ESI). In 2006, after a four-year process, the U.S. federal court system created and published new rules aimed specifically at managing the discovery of ESI.

The new discovery rules cover three main areas of interest to technical communicators:

- A new, proactive role attorneys must take in understanding a client's entire ESI
- How and in what form ESI should be produced
- What companies should do in the normal course of business (that is, *before* a legal action is initiated) to avoid the risk of fines or other legal sanctions

Types of ESI

The new discovery rules address many types of ESI, some of which spring immediately to mind:

- E-mail (and e-mail attachments)
- MS *Office* files
- Files published to PDF or HTML
- MS *Outlook* calendars
- Software source files
- Documentation source files
- Web site source files

Other types of ESI that might not immediately come to mind include the following:

- Digital audio files (music, personal and corporate voice mail, etc.)
- Digital photos
- Digital video
- Web site metadata (accessibility tags, search engine tags, etc.)
- Document metadata (revision histories, document properties and statistics, etc.)
- Internet browser files such as "favorite" URLs, search histories, and Web site cookies
- Instant message "buddy lists"
- Saved instant or text messages

- Online purchase histories
- Backup tapes, e-mail archives, etc.

While the examples of information stored in a personal or mainframe computer are clearly ESI, keep in mind that ESI is also found in devices such as cell phones, iPods™, Blackberries, and PDAs. It is interesting to note that while the new e-Discovery rules address how (that is, in what form) ESI should be produced, they do not define or identify what exactly should be retained.

What types of information are stored electronically at *your* company?

ESI Retention and Destruction

In many lawsuits, the plaintiff requests copies of ESI that it believes might contain information relevant to the claims in the case, but the defendant claims the ESI has been deleted or overwritten or is otherwise inaccessible. The old discovery rules contained no guidelines about when companies could destroy ESI (such as reusing backup tapes, deleting e-mail archives, and so on); as a result, defendants often would say, "Sorry, we deleted that," while plaintiffs asked for all the ESI that the defendant stored anywhere. This omission in the e-Discovery rules led to accusations of willful destruction of evidence by plaintiffs and complaints of "overly burdensome" ESI production requests by defendants.

While the new e-Discovery rules do not specifically say companies "should" or "must" do anything, they do provide sanctions if a company cannot demonstrate that ESI was destroyed or otherwise became inaccessible in the course of normal business practices (as opposed to being purposely destroyed because it was potentially incriminating).

We believe that if a lawsuit is filed against a company and the plaintiff requests copies of ESI that is no longer accessible, the only way the company can show that ESI was destroyed in the normal course of business is to have formal ESI retention policies that specify precisely what information is saved, the format in which it is saved, where it resides, how long it is maintained, and how and when it can be destroyed.

We also advise that in order to ensure compliance with their own ESI retention policies, companies should spot check or audit affected departments at regular intervals.

Note: While this article addresses ESI, companies can also have retention and destruction policies in place for paper-based documents. Check with your company's legal staff about how you might help ensure that your company is prepared.

ESI Production

Under the old rules, the plaintiff's attorney could, during the discovery process, ask what data the other side stored electronically, then wait to see what ESI (if any) the defendant would identify. This would often take months—and longer if the defendant was intentionally trying to draw out the process.

For example, we were involved in a hit-and-run personal injury case in which the plaintiff suspected that the defendant, a trucking company, had global positioning system (GPS) navigation data in its mainframe that would identify and place one of its trucks at the scene of the accident. Requests for the defendant to identify what GPS and vehicle data it tracked were refused; the defendant claimed that no such data were saved for more than a few days. This claim conflicted with testimony from witnesses who swore that they had seen GPS data that had been stored for months, if not years.

When the plaintiff asked the trucking company to produce a copy of its database, the defendant protested that the request to produce that much data was "unreasonable" and "overly burdensome," and that it wasn't about to allow the plaintiff to conduct a "fishing trip" through its data. A judge finally ordered the defendant's computer experts to meet with the plaintiff's experts and to answer the plaintiff's questions about how and where GPS data were stored. But it took months and many hours of the plaintiff's attorney's time just to get that far.

The new e-Discovery rules, which include provisions on how ESI should be produced, could have prevented such delaying tactics. Had these rules been in effect, the defendant's attorney would have been required to discuss what ESI was available at the start of the discovery process. The defendant might have been sanctioned for destroying evidence, and the jury (had the case gone to trial) given instructions to construe the missing data as evidence harmful to the defendant.

The new discovery rules also stipulate that ESI must be produced in the format in which it was originally created or in some other form that does not degrade the usefulness of the evidence to the requesting party. In one case in which we were involved, a party subpoenaed the other party's e-mails on the matter. The other party complied by *printing* every e-mail for each person in question, scanning each e-mail into a bitmap image, and then dropping the scanned images into individual PDF files (one per page!), an act that made the e-mails virtually impossible to search short of opening and *reading* each individual page (optical character recognition software proved ineffective). And the company produced *thousands* of such files.

Such obstructionist practices are prohibited under the new rules.

Is your company considering migrating legacy documents to a new authoring tool or environment? If so, be sure to keep copies of the files in their original formats as well as the tools that can process them; you may well be asked to produce the files in the original format.

Also remember to archive any "keys" or hardware devices required to run the authoring tools, the original hardware being used to create backup tapes (tapes are seldom readable by newer models), and so forth.

These federal rules are already in place. Is your company prepared?

What You Can Do

The new discovery rules contain other provisions—for example, rules dealing with unreasonable discovery requests and safeguarding a company's trade secrets—but the preceding information highlights the provisions most critical to businesses.

So what does all this mean to you, the technical communicator? Plenty!

First, you should be aware of the new e-Discovery rules so that you can comply with your company's document retention policies. Next, if your company is not aware of the new e-Discovery rules, you may need to write requisite policies or even spearhead your company's efforts to prepare.

The following are some steps you might take to capitalize on this opportunity to increase your value and sphere of influence. Check with your company's legal team to see which are applicable to your situation.

1. Familiarize yourself with the new e-Discovery rules (see Suggested Readings at the end of this article).
2. Take a copy of this article to your company's legal counsel and see if anyone is preparing your company to comply with the new rules.
3. Offer to spearhead the effort to prepare your company.
4. If counsel accepts your offer, explain the situation to your boss and get his or her approval as well.
5. Working with your company's attorney, put together a high-level presentation on the new e-Discovery rules. Brief your company's management, starting with your boss and working your way up the organizational chart as far as needed to get buy-in from stakeholders. The presentation should include a summary of the new e-Discovery rules and the liabilities that can result if your company is not prepared; the actions all companies need to take to prepare; a request for the resources needed to research what it will take to prepare *your* company; and a request to be formally appointed as the project manager for the project. Note: Do not fall into the trap of giving an estimate off the top of your head. Just as you should create a document plan for a complex documentation project prior to giving a firm estimate, you should research how much ESI your company has before estimating how long it will take to inventory and document it. If additional resources are needed from outside the company, contact a technical staffing company for temporary resources, or outsource the whole project to a company that provides e-Discovery support.
6. Create a plan for the project. (If you are new or expanding into project management, ask a more senior project manager to mentor you.)
7. Issue (or draft for someone else to issue) an announcement instructing everyone in the company to cease destroying ESI (as much as practical) until new ESI and document retention policies can be issued.
8. Organize an internal "SWAT team" to identify the areas of the company that contain ESI. The size of the team will depend on the size of your company. If you work for a small company, your team may not be much more than you and someone from IT, while larger companies may require representatives from various departments. In either case, be sure to include your company's legal counsel on the team. Keep the legal counsel in the loop as you proceed, and ask for clarification about the e-Discovery rules as needed.
9. Begin creating an inventory of all types of ESI at your company. (See Suggested Readings for links to sites containing sample retention policy and information-gathering forms.) If possible, record how the ESI was created and has been modified or destroyed, as well as any extant policies governing its destruction.
10. Compile the various sublists into a master inventory document and have the SWAT team review it for completeness.
11. For any type of identified ESI that does not have an extant retention and destruction policy, have someone in the department/division who "owns" the data determine what the retention and destruction policies for that ESI should be. Note: It is likely that many stakeholders will be involved at this point, each with a different opinion on which ESI should be retained and for how long. Consider this another opportunity to expand your sphere of influence and practice your conflict management and workplace negotiation skills!
12. Have your corporate attorney approve the format you will be using for the final ESI inventory and retention and destruction policies.
13. Also have your corporate attorney identify what other information you should be collecting. For example, the new e-Discovery rules state that the company may not have to produce ESI if doing so would be "too burdensome." However, you should be prepared to present a precompiled list of ESI "too burdensome to produce" at the scheduling conference (a preliminary conference for setting deadlines and discussion of legal and factual issues). Consult your company's attorney to determine what would be considered unreasonable for your company, what other information you *should* or *should not* record, and so on.
14. Keep accurate records of your contributions as you proceed through this effort. You'll want written records to show how your company became prepared, and you'll certainly want management to appreciate what a monumental task you've pulled off when it comes time for your annual review and pay raise!
15. If possible, enlist one or more additional technical communicators to draft or review the policy and procedures to ensure that they are well written, understandable, measurable, and maintainable.
16. Once you have completed a draft of the ESI inventory and corresponding retention and destruction policies and procedures (and policies for paper-based documents if your company needs those as well), gather as many members of your com-

pany's legal team as applicable (both internal and external counsel) and brief them on how you've prepared.

17. Once the ESI inventory and retention/destruction policies have been written, create a policy and procedure for auditing them on a regular basis. (Again, consult your company attorney for what would be considered "regular" for your situation.)
18. Get an appropriate (senior) company official to approve and sign the ESI inventory, retention/destruction, and audit policies and procedures.
19. Following approval, issue formal policies and procedures for each specific area of your company, as well as those that apply companywide (for example, the policy covering the archival and deletion of e-mails and voice mails).
20. Coordinate with your human resources department so that the policies and procedures are incorporated into new employee orientations and trainings.
21. Ensure that procedures are in place to maintain the ESI inventory documents and to audit them as required.
22. Conduct a postmortem on how the project went, turn over the maintenance phase to another member of the team (an assistant you've been mentoring for just that purpose?), and then look for another high-visibility project in the company with which to assist.
23. Oh, and remember to ask for a raise come annual review time!

Suggested Readings

The new e-Discovery rules are available at no cost at ***www.law.cornell.edu/rules/frcp***.

A copy of the book *The New E-Discovery Rules*, which includes excerpts from the September 2005 Report of the Committee on Rules and Practice & Procedure and the May 2005 Report of the Civil Rules Advisory Committee, can be obtained for $15 at ***www.legalpub.com***.

Molisani, Jack. "Hidden Information for All to See." *Intercom*, February 2005.

Visit ***www.ElectronicEvidenceRetrieval.com*** for additional articles and resources on the topics of the new rules and computer forensics, including several sample document retention policies.

---

*Jack Molisani has a degree in computer engineering from Tulane University in New Orleans and more than twenty years' experience in the computer and software industries. He provides e-Discovery training for Electronic Evidence Retrieval, LLC, when he is not running ProSpring Technical Staffing (**www.ProspringStaffing.com**). He also produces LavaCon, the annual conference for advanced technical communication professionals (**www.lavacon.org**).*

*Dr. Johnette Hassell is a recognized expert witness in the field of computer forensics with more than thirty-five years' experience in the computer and software industries. She is president of Electronic Evidence Retrieval, LLC, a computer forensics company headquartered in New Orleans, Louisiana (**www.ElectronicEvidenceRetrieval.com**). She is a national consultant and expert witness in case evaluation, preparation, deposition, and testimony. She has served on the faculty of Tulane University's School of Engineering for more than twenty-five years.*