

eDiscovery: A New Approach to Discovery in Federal and State Courts

Changes in technology have altered the way lawyers deal with preservation, collection, review, and production of evidence. The electronicdiscovery amendments to the Federal Rules of Civil Procedure, effective December 1, 2006, provide a framework for dealing with this new reality.

> By Scott A. Carlson and Ronald L. Lipinski



he Federal Rules of Civil Procedure have been amended to address issues arising from "electronic discovery" or "eDiscovery." So is this really going to change the way anyone approaches discovery?

The Federal Rules of Civil Procedure have been amended to address issues arising from "electronic discovery" or "eDiscovery." So is this really going to change the way anyone approaches discovery?

In its most basic form, the standard for discovery remains unchanged – the guiding principle is "relevance" (or that which would lead to relevant information). What has changed, however, is the "form" of the evidence we seek to discover. Instead of bankers boxes filled with paper, we face hard drives filled with electronically stored information. That seemingly simple shift from paper to electronic has forced judges and practitioners to rethink their approach to discovery and ultimately has led to the amendments to the Federal Rules of Civil Procedure.

The federal rule changes are, of course, on their face limited to federal civil cases. Their impact, however, will be felt beyond the federal courts. The federal rule changes embody a shift in discovery strategy that was taking hold in state and federal courts across the country, even absent the rule changes. (A Law Ed program on the new rules is coming to Chicago on April 30 – see sidebar on page 186.)

Many states have already adopted changes in their own procedural rules,

Scott A. Carlson <scarlson@seyfarth.com> is a partner at Seyfarth Shaw LLP in the litigation department, where he founded and co-chairs the firm's national eDiscovery practice, focusing on both litigation and consulting. Ronald L. Lipinski <rlipinski@seyfarth.com> is also a partner at Seyfarth Shaw LLP in the litigation department and a co-chair of the eDiscovery practice. and more are certain to follow. Even states that do not adopt rule changes must somehow accommodate the electronically stored information found in virtually every case filed. If any party cares about the issue, the court will need to address it – with or without guidance from their procedural rules.

Moving from paper to electronic: a bigger deal than you might imagine

There are some fundamental issues to face as the world moved from the "good old days of paper" to today's electronic age. Those issues include (1) an explosion of growth in the volume of discoverable information, (2) the reality that people often do not know where they keep their information, and (3) a new level of "fragility" of information.

Exploding volumes. In the good old days of paper, you went to Bob and asked for any information he had relevant to the case. He gave you a folder or sometimes a banker's box. On rare occasions, Bob told you about a warehouse in Topeka.

In the electronic age, things are different. Instead of a folder or a box, Bob is more likely to have gigabytes upon gigabytes of information that might be relevant to a case. His discussions at the water cooler are now memorialized in email and instant messaging.

His memo with it's handwritten notes are not just in his desk anymore; copies are littered about in his co-workers' email, on company servers, on a CD he took on his last trip out of town, on his home computer, and on back up tapes. The memo potentially comes complete with metadata describing the history of edits to the document, the contributing authors, how long they spent making the changes, when they printed it, who read it when it got emailed to them, and who deleted it without reading it.

If Bob is a typical corporate user, he has up to five gigabytes of electronically stored information. If two gigabytes is email, that represents 200,000 printed pages or over 60,000 messages. If he has another two gigabytes of word processing documents, that represents 65,000 pages. Another gigabyte of spreadsheets represents another 165,000 pages.

In other words, Bob has a lot more than a few folders or even a banker's box. He has his own private warehouse – and so does everyone Bob works with who might be relevant to the case. Suddenly, even the smallest case has the potential to be million-document cases. As for the big cases today, lawyers wish they only had a million documents.

Finding the documents is not so easy. Beyond the volume issue, if Bob is honest with you he doesn't really know where most of his records are. In the good old days of paper, he was the custodian. Now it's not so simple.

Bob may know he puts sales information into his computer, but he may not know that his information is stored on a server in Los Angeles or that he is just one of many who enter data that ultimately is tied to a complex database located in

New Jersey. A lot happens between the time Bob puts in his information and he gets back his sales projections and quotas the next week on the company intranet. Preserving and collecting his documents now requires a talk with him and the IT group.

Easily destroyed and easily created. In the good old days of paper, only Bob threw his documents away. Nobody "auto-cleaned" Bob's desk, throwing away

memos or phone messages he hadn't looked at for 60 days. But in the electronic age, things can be different. Bob's email may be set to delete messages that have not been touched in the last 60 days. Alternatively, Bob's documents may go away because the document management system deletes it after some preset period.

As easy as it is to destroy electronic documents without the custodian's knowledge, it is just as easy to create data without the knowledge of the custodian. Bob may not realize that every time he saves a word processing document, a new version is being kept for him by the document management system; that the drafts of his email are automatically being saved whether he sends them or not; that when he hits delete, a file may still be able to be recovered from an electronic "recycle bin" by the system administrator or may be found on a backup tape or be forensically recovered from a hard drive by an expert.

Understanding the new approach to discovery

As will be explained below in the context of the new rules, the changes in technology have altered the way practitioners have to deal with preservation, collection, review, and production of evidence in the electronic age. The changes to the federal rules are aimed at taking on some of these issues and attempt to provide a framework for dealing with them.

However, the amendments themselves do not represent a dramatic shift in the manner in which eDiscovery issues have developed over the last several years. Rather, the rules embrace much of the existing case law and practice regarding electronically stored information.

Some things have not changed. Writers and commentators in the popular

The electronic age has caused an explosion in the volume of discoverable information. And more often than in the past, people do not really know where they keep their information.

> press and legal publications warn of a radical change in the legal requirements placed upon litigants by the amended federal rules. Some have said in so many words that individuals and corporations now "must save and retain every e-mail drafted or sent" and produce it in litigation. Commentators speak of what lawyers must do to learn about computer systems and "data architecture."

> While the changes to the federal rules have sparked a new awareness about the obligations on lawyers and parties relating to the preservation and retrieval of electronic information, the basic litigation obligations have not changed. There has been no amendment to Rule 1 of the Federal Rules of Civil Procedure.

> Rule 1 provides that the federal rules govern procedure in the United States District Court in all suits of a civil nature. Rule 1 states very succinctly: "They shall be construed and administered to secure the just, speedy, and inexpensive determination of every action." The purpose of the rules is to provide a mechanism for parties to come to federal court and resolve disputes. They do not put the burden on individuals or companies to "keep everything."

The eDiscovery amendments seek to assist the parties before the court to define issues and resolve them. The new amendments do not require the creation of any pre-litigation record or document and impose no requirements about what information or data must be kept or preserved. They do not speak to what type of computer system is required.

No less than the U.S. Supreme Court has recognized that there are legitimate reasons for individuals and companies to dispose of documents and electronic information.¹ What the amendments do is remove all doubt that the duty resting upon lawyers and litigants to find and preserve evidence relevant to a dispute unequivocally includes electronically stored information.

A new category for "electronically stored information." In addition to "documents," the rules now specifically add a new category of discoverable information called "electronically stored information" (ESI).² This separate category is defined to make clear that ESI is on equal footing with, and is just as discoverable as, paper documents.

Gone for good are the days when parties can argue that electronic information is less discoverable than paper documents. ESI is not limited to the common items such as word processing documents and spreadsheets. ESI in a particular case could theoretically include databases, servers, voice mail systems, cell phones, memory chips in cars, instant messaging, digital cameras, portable GPS devices, handheld computing devices, etc. That is not to say any and every type of information stored electronically must be preserved and produced, just that it is in the potential scope of discoverable information under the rules.

Rule 26 Conferences: Discussing discovery early in the case

Perhaps the most significant change to the rules is the requirement that parties must discuss eDiscovery issues at the initial FRCP 26(f) conference. Issues to be discussed include the form of produc-

tion and preservation. Essentially, the rules envision an early, open, and frank discussion about (1) the information that may be in a party's possession, (2) the manner in which documents will be preserved and collected, (3) the scope of discovery contemplated, and (4) how that information will be produced in discovery.

This early, open, and frank discussion may not sit well with all parties and their counsel. Traditionally, some litigators have engaged in a game of "it's for me to know and you to find out" during the discovery process. Discovery was responded to more in the way of objections than through substantive answers. The discovery process sometimes became agonizingly slow as information dripped out of the par-

April 30: learn how to comply with the e-discovery law

A Law Ed program in Chicago late this month explains what electronic discovery is, how it works, and what the federal rule amendments mean to litigators and clients.

The half-day program, entitled "Electronic discovery: Important changes to the law, practical suggestions for complying, and issues for the profession," will be presented by the ISBA Committee on Legal Technology at the ISBA Chicago Regional Office on Monday, April 30.

The opening presentation looks at what electronic discovery is, why it's important, and what some of its costs and problems are. Another session describes the practical aspects of e-discovery – including how data is gathered and processed for review and production and how to use the meet-and-confer process to narrow e-discovery – while a third looks at the FRCP e-discovery amendments and how they affect your and your clients' duties. The program ends with a panel discussion on e-discovery's impact and implications.

For details and to register, visit the "Law Ed Calendar" link under CLE at isba. org or go straight to http://www.isba.org/lawed/Electronic4-07.html.

ties' hands to their opponents. In the eDiscovery context, such a practice can prove dangerous.

While it may seem daunting to address these issues so early in the case, doing so may protect your client from a motion for sanctions. Even before the rule changes, many practitioners were seeing the benefits of such discussions. Because of these discussions, and sometimes disagreements, parties were in court early in the case arguing about their preservation obligation rather than arguing years into the case about spoliation.

Perhaps the most significant change to the rules is the requirement that parties must discuss eDiscovery issues at the initial FRCP 26(f) conference.

> Identifying discoverable information and discussing preservation. Early discussions should take place to identify the location of discoverable information. This necessarily requires parties to arm their lawyers with information about their documents and IT systems, including how information is maintained and retrieved. While this is a shift from a traditional approach of guarding against disclosure of information, the benefits can translate to decreased litigation over discovery disputes.

> Parties must take this early step to identify relevant IT systems because each system will require its own methods of preservation and manner of production. Preserving a word-processing document may be easy, but preserving "all documents maintained by the sales force" may not be. Preserving a database may be nearly impossible without shutting it down, but a single report may be easy to export into a spreadsheet.

> One common example involving backup tapes illustrates the benefits of early discussion of these issues. Nearly every company backs up its computer systems on back up tapes to enable disaster recovery. Every night a copy of the system is dutifully copied to tape so that if the system goes down it can be re-

^{1.} Arthur Anderson, LLP v United States, 544 US 696 (2005).

^{2.} Fed R Civ P 16(b) and 26(a)(1)(B).

stored to look like it did the night before. Companies do not, however, keep those tapes forever. They routinely overwrite them. Some companies keep a few days worth of old tapes, while others keep months worth.

If a company is keeping months of backup tapes, they may contain the email Bob deleted 60 days ago, or the memo he deleted 30 days ago, or the draft of the policy he deleted 15 days ago – and it all might have some relevance to the recently filed case.

A requesting party may expect that the company will stop the recycling of backup because they may contain relevant information. The company, however, may face extraordinary costs to buy new tapes rather than overwrite old ones. Depending on the number of tapes involved and the time period, costs can quickly jump from tens to hundreds of thousands, even millions, of dollars just to keep buying blank tapes – not to mention the potential cost of restoration and attorney review time.

If we follow the traditional approach to discovery, we will wait until we get discovery requests and never address the issue with the other side. In so doing, the company will very likely continue to overwrite tapes in the ordinary course of business. The requesting party may a year or two later, perhaps after her allegations have lost support in the facts, find out the tapes have been overwritten. She will file the motion for sanctions, referring to the data that was "destroyed" and explaining how critical that information was to her case.

The company will respond, noting the costs (if they considered them before) and the limited evidence that could have existed on the tapes (if they know). Both parties will eagerly await the outcome of the motion for sanctions being heard by a judge who may or may not have ever heard of a backup tape before this case. And given the broad discretion of the court, the decision may range from no sanctions or a fine to an adverse inference or a default judgment.³

But there is another option: raising this issue early at the outset of the litigation. The parties may still disagree about whether the tapes can be recycled, but the argument in court will be about the extent of the parties' preservation obligations, not the extent of the sanction. The outcome of the court's decision may include requiring the saving of some of the tapes, or requiring the requesting party to bear the cost of saving tapes, or any other order that makes sense in the context of discovery. The outcome will *not*, however, be a sanction.

The list of items the parties can discuss is long and will depend upon the evidence that matters in a particular case. However, the list may include discussions about preserving metadata, whether forensic copies of hard drives are necessary or desired, how complex databases will be dealt with, how drafts of electronic documents will be addressed, whether voice mail and instant messaging will be preserved, how to deal with departing employees and whether Internet histories and Web site pages will be preserved. If dealt with appropriately, the list will be very specific.

More is not always better. Another topic of discussion is the scope of discovery. Given the explosive volumes of information involved, neither party can realistically and cost-effectively handle it all.

In the example earlier in the article, Bob and four of his co-workers may together have one million pages of email or over 300,000 email messages. A really fast reviewer, reviewing 600 messages per eight-hour day, could get through those five persons' email in a mere 500 days. Of course there are other ways to conduct a review and technology tools to help, but the message is the same – sometimes there's "too much stuff."

Accordingly, trying to limit the scope of what will be discoverable in the case can be in the interests of both parties. Efforts can be undertaken to identify key witnesses and agree to search terms rather than trying to have both parties do a document-by-document review. The options are many and are worth the open-minded discussions of both parties early in the case.

Determining the form of production. The form of production poses certain risks that are not apparent to most litigators and can be a trap for the unwary on both sides. The amendments provide that absent an agreement of the parties, the responding party is required to "produce the information in a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable."⁴ "Reasonably usable" is essentially defined as searchable.

This topic is worthy of discussion to save both parties time and money. Some electronically stored information cannot be "produced" in a traditional way. You can't take a complex database such as a company's general ledger system, burn it onto a CD, and turn it over to the other side. Instead, you illustrate through sample reports, exporting of particular data, or other means how you use that data and what is available so the requesting party understands how to access it.

While a vendor is certainly willing to charge by the gigabyte to "process" as much data as you want, you may find that the 10 gigabytes of digital camera photos is better produced "natively" by copying them to a few DVDs and giving them to your opponent rather than sending them through a vendor at \$1,000 per gigabyte. The photos may not have Bates numbers on them but you can always deal with that later.

On the other hand, turning over a DVD full of word-processing files in their "native" format may not make sense. Every time your opponent opens the document, that act now becomes part of the document. Your opponents can inadvertently (or sadly, sometimes on purpose) alter the document. When they print the document and hand it to a witness, you can't be sure it's the same document you produced.

Authenticity becomes a problem. For these types of files, using an eDiscovery vendor to process the data, emblaze Bates numbers, add protective order markings, and deliver the product in an unalterable and searchable form to you and your opponent may make perfect sense.

No shortage of challenges. While it's always difficult to negotiate limits on the form and manner of data production, the obligation to discuss eDiscovery issues early can work to the advantage of a well-prepared party. Parties and the court should seize the opportunity to clarify expectations, define the scope of preservation, and develop detailed discovery plans to avoid uncertainty. The parties should have early discussions to define what is and is not being done to preserve electronic data.

"Not reasonably accessible data"

The amendments provide a two-tiered

^{3.} Zubulake v UBS Warburg, LLC, 229 FRD 422 (SD NY 2004) (duty to preserve); Metropolitan Opera Association v Local 100, 212 FRD 178 (SD NY 2003) (duty to preserve); Wiginton v CB Richard Ellis, 2003 WL 22439865 (ND III) (costs); Zubulake v UBS Warburg LLC, 217 FRD 309 (SD NY 2003) (costs); Rowe Entertainment, Inc v William Morris Agency, Inc, 205 FRD 421 (SD NY 2002) (costs); Coleman (Parent) Holdings, Inc v Morgan Stanley & Co, Inc, 2005 WL 679071 (Fla Cir Ct) (sanctions). 4. Fed R Civ P 34(b) (ii).

approach to eDiscovery, presenting a significant opportunity to reduce the scope of eDiscovery for certain categories of data. Under the amended rules, a responding party may identify certain ESI as "not reasonably accessible," recognizing that relevant ESI may well exist in a particular location, but due to "undue burden or cost," the party does not intend to review or produce it.⁵ The requesting party may object and attempt to show "good cause" that the information should be produced notwithstanding the assertion of undue burden or cost.

This particular amendment is worthy of considerable attention. Many items that could be characterized as "not reasonably accessible" are those parties have struggled with preserving, reviewing, and producing. Examples of potentially notreasonably-accessible data include backup media, forensically recoverable data, and legacy systems. The rule is purposefully vague, however, and allows for flexibility as technology changes the "burden or cost." Restoring a backup tape today may be costly, but next year there may be a better and cheaper solution.

The Committee Note makes an im-

portant comment on the preservation of information that may be "not reasonably accessible," observing that whether such information must be preserved depends upon the circumstances of the particular case. Thus, even though you may take a position that you need not produce certain ESI, that does not mean you can always avoid its preservation.

Inadvertent disclosure: managing the attorneyclient privilege waiver

The revised rules also provide a procedure for dealing with the inadvertent disclosure of privileged documents or electronically stored information. The amended rule applies to both documents and electronically stored information. Specifically, if a party produces in discovery information subject to a claim of privilege and the other party is made aware of the claim, that party must return, sequester, or destroy the information and cannot use it until the claim of privilege is resolved.⁶

Note, however, that the rules do not address the substantive question of whether there has been a waiver of attorney-client privilege – only the disposition of the document during the duration of the dispute. The rules contemplate that the parties may enter into non-waiver agreements, but some commentators question the validity of such agreements.⁷

Conclusion

Dealing effectively with electronically stored information will require a new approach to discovery. Judges and practitioners must address eDiscovery early so when they bring the issue to court they are arguing about preservation, not spoliation. They must learn about the computer systems in the case at hand and understand how data is created and maintained if they hope to design appropriate preservation and collection strategies. Ultimately, however, the aim remains the same as in paper discovery – assembling the evidence and facts to resolve clients' disputes.

Reprinted from the *Illinois Bar Journal*, Vol. 95 #4, April 2007. Copyright by the Illinois State Bar Association. www.isba.org

^{5.} Fed R Civ P 26(b)(2)(B).

^{6.} Fed R Civ P 26(b)(5)(B).

^{7.} Hopson v Mayor and City Council of Baltimore, 232 FRD 228 (D MD 2005).