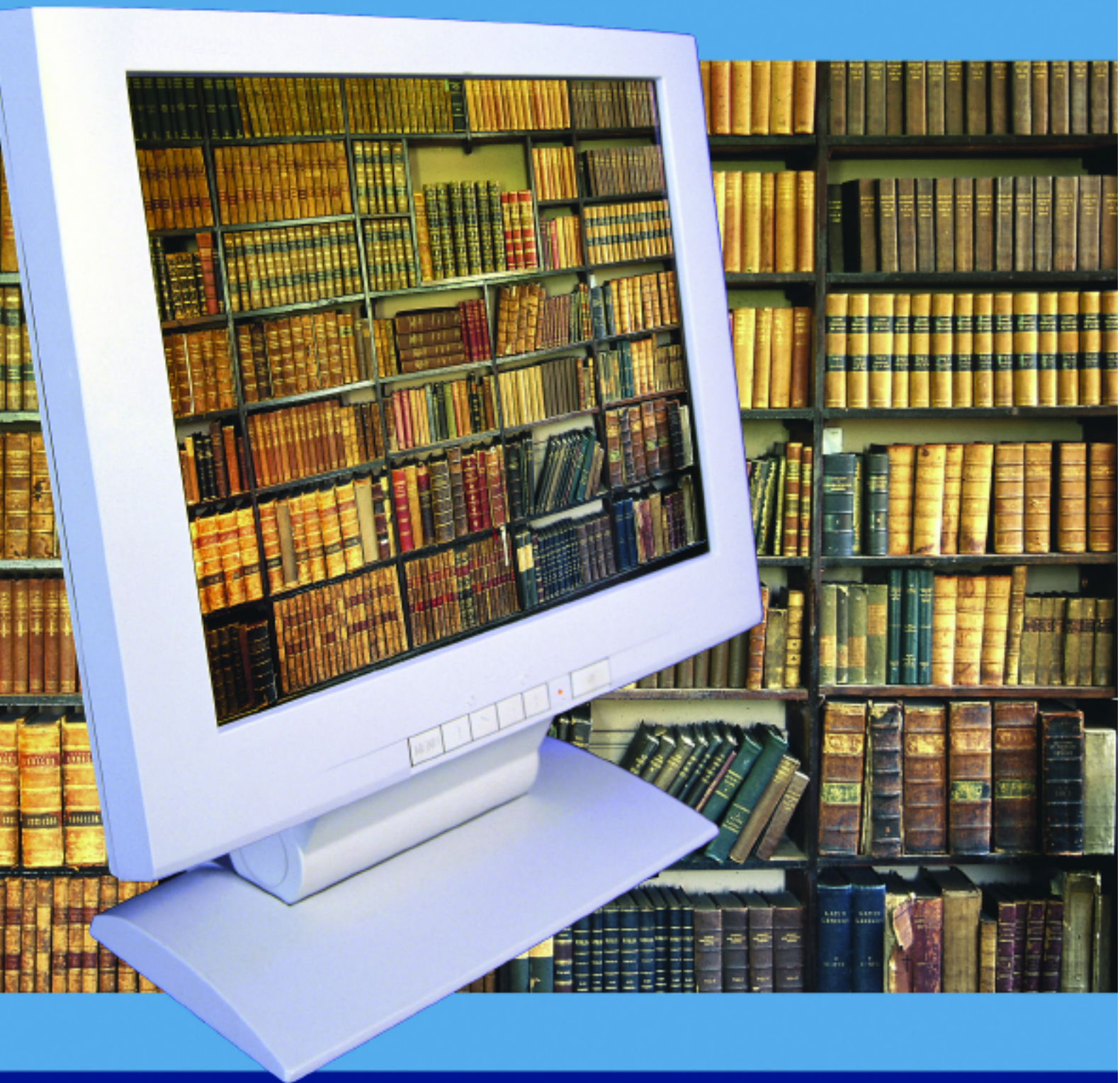
BY DAWN M. BERGIN

NEW FEDERAL RULES ON E-Discovery

Help or Hindrance?

Electronic information is changing the litigation landscape. It is increasing the cost of litigation, consuming increasing amounts of client resources, and creating a new industry of electronic systems consultants. It will require that judges learn new concepts of electronic information and understand "system architecture."

What about lawyers? Will we be held to a new standard? All indications point to the answer "Yes."



Dawn Bergin is a commercial litigation partner, member of the electronic discovery group and Chair of the Litigation Department at Lewis and Roca LLP in Phoenix. The author acknowledges the contributions to this article by Joseph Roth, a third-year law student at Columbia Law School.

The emerging case law sets forth specific and rigorous obligations for lawyers to locate, preserve and produce electronic data. As technology and the case law rapidly develop, the court system is trying to keep up.

On December 1, 2006, new amendments to the Federal Rules of Civil Procedure on electronic discovery will become effective. The rules will address multiple aspects of electronic discovery, including the form of data production, privilege issues, the "accessibility" of data, and the importance of early conferencing between the parties on electronic discovery issues.[1]

In an area where the case law is emerging and courts appear to be imposing new obligations on lawyers, the amended rules will no doubt provide some useful guidance in navigating the myriad issues that arise with electronic discovery. At the same time, their adoption signals the undeniable arrival of a new required course for litigators—location, preservation and production of electronic information.

The Emerging Standards

In the last couple of years, courts have increasingly addressed a lawyer's duty to locate, preserve and produce electronic data. Though these duties have always existed in the paper document world, the electronic age presents complexities and challenges for lawyers that have not been seen in the profession before.

For example, a lawyer could miss a collection source for paper documents—maybe some boxes, maybe a file cabinet or two. But it's pretty unlikely that she would miss a warehouse.

Not true in the electronic world. Missing the equivalent of a warehouse of documents could result from simply failing to ask about every part of every server or failing to obtain each personal laptop with potentially relevant information.

The same holds true for the destruction or loss of paper documents. You may lose some paper documents, but you are not likely to lose a warehouse full of documents. In contrast, electronic data can be deleted or copied over within minutes. And many companies' computer systems have automatic mechanisms for deletion and recycling of backup tapes. The following cases demonstrate exactly these points.

Zubulake V: The Duties To Preserve and Produce Electronic Data

Zubulake V[2] is probably the most-often cited case in the electronic discovery arena, particularly with respect to the duties of lawyers. Interestingly, *Zubulake* did not involve a complex commercial transaction between two sophisticated parties. Instead, it was a gender discrimination claim by Laura Zubulake against her employer, UBS.

UBS' in-house lawyers gave oral instructions to employees not to delete or destroy any potentially relevant material, including electronic data. Outside counsel reiterated the instructions and put them in writing after Zubulake filed her suit. Although neither lawyer specifically requested backup tapes at the outset, outside counsel instructed UBS employees to stop recycling backup tapes once the plaintiff requested them.

During the restoration of the backup tapes, it became apparent that e-mails were missing from the tapes. During depositions of key UBS employees, Zubulake discovered that even more e-mails were deleted, and some e-mails residing in UBS's active files were never produced.

In evaluating Zubulake's request for sanctions for the missing e-mails, the court provided a detailed analysis of a lawyer's obligations to ensure preservation and production of electronic data, starting with the dictate that implementation of a litigation-hold is "only the beginning."[3] The lawyer must learn the client's document retention policy and its "data retention architecture," interview information technology personnel, interview "key players" (defined as those persons identified in the parties' disclosure statements), and to the extent it is not feasible to speak with every key player, "be more creative" (by, for example, conducting systemwide keyword searches). The lawyer must also reissue the litigation-hold periodically, advise key players about their preservation duty and periodically remind them of it, and instruct all employees to produce electronic copies of their relevant active files and ensure that backup media are identified and safely stored.[4]

The court acknowledged that both inside and outside counsel had issued a litigation-hold and had repeated the instructions to UBS employees, some of whom destroyed or deleted data anyway. Judge Shira Scheindlin also acknowledged that outside counsel spoke to most of the key players, took steps to preserve backup tapes when the plaintiff raised the issue, and instructed employees to produce copies of their active computer files.

The court nonetheless criticized counsel's efforts, labeling counsel "not entirely blameless."[5] Specifically, she criticized their failure to: (1) adequately communicate with one of the key players about how she stored data, making no effort to understand what she meant when she referred to her "archive"; (2) request that that employee produce her files; (3) communicate the litigation-hold instructions to a senior human resources employee actively involved in Zubulake's case; and (4) protect relevant backup tapes.[6]

Ultimately, the court sanctioned UBS, not its lawyers, noting that the lawyers' efforts were reasonable, if not completely satisfactory. Judge Scheindlin clearly used the opinion, however, to lay out the court's expectations of lawyers in preserving and producing electronic data. And those expectations are exacting, as demonstrated in another recent opinion from the Southern District of New York.

E-Discovery in Arizona

The State Bar Civil Practice & Procedure Committee is examining the possibility of amending the discovery rules to address e-discovery. It has formed a subcommittee that will make recommendations. Among other information, the subcommittee may well review the "Guidelines for State Trial Courts Regarding Discovery of Electronically-Stored Information," distributed by the Conference of Chief Justices in August 2006. The report is available online at

www.ncsconline.org/WC/Publications/CS_ElDiscCCJGuidelines.pdf

Phoenix Four: The Duties To Locate Electronic Data

In *Phoenix Four v. Strategic Resources Corporation*,[7] the plaintiff sued its investment adviser, Security Resources Corporation ("SRC") and its individual principals for various business torts. Shortly after the suit, SRC shut down and moved materials from its offices, including two computer servers, at least two computer workstations and documents related to the plaintiff.[8]

Both before and after plaintiff's first document request, defendants' lawyers, Mound Cotton, instructed them to gather relevant documents and electronic files.[9] The defendants searched their computers and found no relevant electronic files and so advised Mound Cotton. Defendants did not search the servers, however, because they were unaware of any pertinent material on them.[10]

Later, a service technician, who was hired to address a system problem totally unrelated to the lawsuit, discovered a large amount of electronic data stored on a dormant, partitioned part of one of the servers defendants had taken from their previous location. Because of the drive mapping, defendants had no access to this part of the server from their computers and they were not aware it existed. Once defendants learned of the data's existence, they advised Mound Cotton, who instructed them to download the data and deliver it to them.[11] Plaintiff ultimately agreed to accept the new information in hard copy, but by the time they received the documents, the depositions of the key defendants had already occurred.[12] Plaintiff requested an adverse inference instruction based in part on defendants' late production of documents from the server.

Although the court did not grant the request for an adverse jury instruction, it imposed monetary sanctions against defendants and Mound Cotton for the plaintiff's costs and fees and $10,000 each for a new round of depositions of defendants, finding Mound Cotton's failure to discover the existence of the server to constitute gross negligence.[13] The court cited to the proposed amendment to Rule 26(a), which explicitly requires a party to disclose a "description by category and location of … electronically stored information." The court also noted that the proposed amendment to Rule 26(b)(2), which allows a party to decline to produce data from a source that is not reasonably accessible, reinforced the concept that the party must at least identify the sources of such data. Mound Cotton failed to do this.[14]

The court also found that Mound Cotton did not meet *Zubulake V*'s mandate regarding lawyers' obligations to thoroughly educate themselves on a client's electronic systems.[15] The court suggested that had Mound Cotton asked defendants what happened to the computers from their former offices, they would have learned of the existence of the server, which in turn should have triggered questioning about the contents of the server, and if necessary, the hiring of a technician to determine the contents.[16]

Williams v. Sprint: The Duty To Produce Metadata

Another case that addresses a lawyer's specific duties in the electronic discovery realm is *Williams v. Sprint/United Management Company*.[17] There, the lawyers for Sprint scrubbed the metadata[18] from Sprint's electronic spreadsheets before producing them to plaintiffs.[19] Sprint argued that the emerging standards of electronic discovery provide for a presumption against the production of metadata because it is not considered part of a document unless it is both specifically requested and relevant.[20] Magistrate Judge David Waxse disagreed.

Acknowledging that metadata presents unique challenges in the production of electronic data, Judge Waxse held that:

> [W]hen a party is ordered to produce electronic documents as they are maintained in the ordinary course of business, the producing party should produce the electronic documents with their metadata intact, unless that party timely objects to production of metadata, the parties agree that the metadata should not be produced, or the producing party requests a protective order.[21]

Other courts will undoubtedly rely on Judge Waxse's opinion and adopt the same standard for production of metadata.

Zubulake V, *Phoenix Four* and *Sprint* make clear that the days of doing no more than asking your client to gather relevant documents and e-mails are over. Lawyers must question their clients sufficiently to determine whether there is "partitioned data" that may be relevant and subject to production. Lawyers must make sure they understand what words like "archive" mean when used by a key player during her interview. They must, in short, make every reasonable effort to locate, preserve and produce relevant electronic data, including metadata.

The Federal Rules Amendments

What about the amended rules? Will they help lawyers meet their new obligations and avoid sanctions for overlooking a server in the search for relevant electronic data?

They should. Though the amendments and comments contain directives to lawyers that could give rise to standards of care, they also provide much-needed structure for the process and some protections for lawyers and parties who proceed in good faith.

The key amendments to the rules that will assist in guiding the parties through electronic discovery are Rule 26(f), Rule 26(b)(5)(B), Rule 34(b) and Rule 37, FED. R. CIV. P.

Rule 26(f): Early Meet-and-Confer

The amendment to Rule 26(f) requires the parties "to develop a discovery plan that addresses … any issues regarding discovery of electronically stored information and the forms in which it should be produced."[22] The comments to the amended rule strongly suggest that the parties should familiarize themselves with their clients' systems prior to the Rule 26(f) conference.

This rule and comment are consistent with *Zubulake's* directive for lawyers to learn about their clients' electronic data systems. It also imposes order on the process because it forces the lawyers to determine early on who the key players are, interview them, meet with the information system personnel, and learn about the architecture of the system and deletion and backup policies, and so forth. A lawyer may very well have to hire a technical expert to assist with these tasks and to ensure that existing information is backed up or that an automatic deletion mechanism is changed or deleted.

Judges, like lawyers, will have to learn about things such as system "architecture," metadata and backup systems. Resolving disputes about electronic discovery issues will be as challenging for them as it is for lawyers, and they will rely on the parties to make substantial progress before seeking court assistance. Indeed, Judge Scheindlin noted in *Zubulake V* that working out the electronic discovery issues had been "tedious" and that she "hoped that counsel w[ould] heed the guidance provided by these resources and … work to ensure that preservation, production and spoliation issues are limited, if not eliminated."[23] Other courts are likely to echo that sentiment.

Rule 26(f): E-Documents Containing Privileged Information

Recognizing that the sheer volume of electronic data that will be at issue in many lawsuits presents a major challenge to lawyers and parties to ensure that privileged documents do not get produced, the amendments to the Rules provide some guidance.

Rule 26(f) requires the parties to address at the Rule 26(f) conference any issues related to assertions of privilege or work-product protection, including whether the parties should request the court to include the agreement in an order.

The comments to Rule 26(f) explain the types of agreements counsel can enter into to avoid the inadvertent waiver of privilege and suggest that they obtain court endorsement of any such agreement.

Under an inadvertent disclosure or "clawback" agreement, if a party inadvertently produces a privileged document, the production will not constitute a waiver, provided that the producing party identifies the documents mistakenly produced. Under these circumstances, the receiving party should return the document and cannot argue that the production resulted in a waiver.

> The sheer volume of electronic data that will be at issue in many lawsuits presents a major challenge to lawyers and parties.

Another type of agreement suggested in the comments is the "quick peek" agreement, under which the parties agree that the responding party will provide certain requested materials without waiving any privilege.

Clawback and quick peek agreements not only reduce the risk of inadvertent waiver, but, as noted in the comments to the rule, they "can facilitate prompt and economical discovery by reducing delay before the discovering party obtains access to documents, and by reducing the cost and burden of review by the producing party."[24]

The *Williams v. Sprint* case discussed previously demonstrates how a party can benefit from an early conference with the opposing party and a quick peek agreement.

In *Williams*, Sprint argued that the metadata it scrubbed from its files was protected by the attorney–client privilege.[25] The court

held that because Sprint failed to object to production of the metadata (and instead simply scrubbed the files), did not provide a privilege log identifying the electronic documents that it claimed included privileged metadata, and failed to provide the court with even a general description of the documents, it waived the attorney–client privilege with respect to the metadata.[26]

The new rules could have helped Sprint avoid the waiver. First, had counsel for Sprint conferred with plaintiff's counsel early on, the issue of metadata could have been addressed. Second, had the parties entered into a quick peek agreement, Sprint could have produced the metadata without waiving the privilege.

Rule 26(b)(5)(B): The New Retrieval Procedure

Rule 26 also provides a procedure for "retrieving" inadvertently produced privileged information until a court rules on whether the privilege was waived. Specifically, a party who produces privileged material may notify the recipient of its claim, which triggers obligations by the recipient to "promptly return, sequester, or destroy the specified information and any copies it has" and not to "use or disclose the information until the claim is resolved." The rule even requires the recipient of the privileged information to take reasonable steps to retrieve any information that was disclosed prior to the notice from the producing party.

Again, it is clear from this procedural safeguard, as well as from the proposed clawback and quick peek agreements, that the rule-makers understood the challenges presented by the daunting volume of electronically stored privileged information.

Rule 34(b): Form of Data

Another issue that presents challenges for parties and lawyers is identifying the form in which the data should be produced. Again, the new rules and comments provide some guidance.

Rule 26(f)(3) requires the parties to discuss the form in which electronic data should be produced, again, forcing the parties to address the issue at the outset. Second, Rule 34(b) allows a party to produce electronic data in a particular form, but if the responding party objects to the requested form, it must produce the data in the form in which it is ordinarily maintained or in a form that is reasonably usable. This rule assists lawyers by providing flexibility and a standard of reasonableness.

Rule 37: "Safe Harbor"

The rules provide other protections and structure as well. Rule 37(f), referred to as the "safe harbor" provision, precludes a court (absent exceptional circumstances) from imposing sanctions for "failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system."

For example, if a company's computer system has an automatic deletion mechanism that the party is not aware of, the safe harbor provision should apply.

Conclusion

There is a new developing standard of care for lawyers in the electronic age. Cases like *Zubulake V, Phoenix Four* and *Sprint* have set the stage. The amendments to the Federal Rules of Civil Procedure provide tools to deal with the myriad issues that arise with electronic data. The standards and obligations will become more solidified as the amendments to the rules are applied and interpreted.

What every lawyer needs to do right now, though, is recognize that we have landed in a new world with new rules and new obligations. Learn what they are, keep up with the case law and make your clients understand that complying with the new regime is not optional.

endnotes

1. For a comprehensive discussion of the amendments to the Federal Rules of Civil Procedure, *see* George L. Paul & Bruce Nearon, The Discovery Revolution: E-Discovery Amendments to the Federal Rules of Civil Procedure (2nd ed. 2006).
2. *Zubulake v. UBS Warburg, LLC*, 229 F.R.D. 422 (S.D.N.Y. July 2004).
3. *Id.* at 432.
4. *Id.* at 432-34.
5. *Id.* at 435.
6. *Id.*
7. 2006 WL 1409413 (S.D.N.Y. May 23, 2006).
8. *Id.* at *1-2.
9. *Id.* at *2.
10. *Id.*
11. *Id.*
12. *Id.* at *3.
13. *Id.* at *6, *9.
14. *Id.* at *6.
15. *Id.*
16. *Id.* at *5-6.
17. 230 F.R.D. 640 (D. Kan. 2005).
18. Metadata is data about data (*e.g.*, file names, access dates).
19. 230 F.R.D. at 644.
20. *Id.*
21. *Id.* at 652.
22. Rule 26(f)(3).
23. 229 F.R.D. at 440-41.
24. These agreements, however, are not necessarily foolproof. In *Hopson v. The Mayor and City Council of Baltimore*, 232 F.R.D. 228 (D. Md. 2005), Magistrate Judge Paul Grimm identified certain inherent risks associated with such agreements, including that waiver of the privilege is a substantive area of law that can vary from jurisdiction to jurisdiction, and that an inadvertent disclosure agreement might not protect against a waiver as to third parties. The comments to Rule 26(f) suggest that the parties obtain court endorsement of any such agreement, which, in addition to being a sound practice, should minimize the most significant risks.
25. 230 F.R.D. at 653.
26. *Id.* at 655.