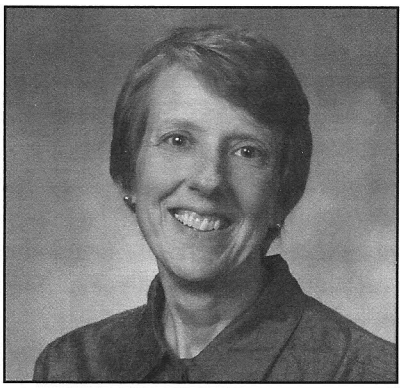
Here Comes The Judge: The New Federal Rules On E-discovery

Helen L. Marsh

Planning the scope, form, and timing of electronic discovery is now more important than ever.



Helen L. Marsh
is an attorney with Heller Ehrman LLP, in San Francisco. Her practice emphasizes mass torts and she has special experience in handling document-intensive complex litigation. She can be reached at helen.marsh@hellerehrman.com.

THE UNITED STATES SUPREME COURT recently approved amendments to the Federal Rules of Civil Procedure that are designed to address the unique issues presented by the proliferation and importance of electronically stored records in litigation. The amendments took effect on December 1, 2006 and apply to cases filed on or after that date but also to pending cases "insofar as just and practicable." 2006 U.S. Order 20, April 12, 2006. Thus, cases already on file are likely to be affected by these amendments.

The vast majority of documents maintained by businesses today do not exist in paper format. They are maintained on a long-term basis only in electronic format. Furthermore, it has been estimated that billions of emails are sent in the United States every day. When litigation ensues, vast quantities of electronic information must be preserved so that it can be evaluated for relevance to that litigation. To the extent electronic data is responsive to discovery requests, it must be produced.

The courts and litigants have been struggling to manage e-discovery for the past decade. Although electronically stored data has been expressly deemed discoverable since the 1970 amendment to Fed. R. Civ. P. 34(a), which includes "data compilation" within the definition of what

constitutes a document, there is no other guidance in the current rules that helps the courts or parties to navigate the shoals of e-discovery. Some courts, as well as individual judges, have attempted to address the problem with local rules or case management orders, and parties have attempted to negotiate agreements regarding e-discovery, resorting to motion practice as needed. State courts are beginning to address these electronic discovery issues as well.

For the past five years, the Judicial Conference's Advisory Committee for the Federal Rules of Civil Procedure ("Advisory Committee") has been studying proposed changes to the Rules to take into account the unique problems posed by discovery in the electronic age. The process involved publication of proposed rules, written testimony and public hearings, and revisions. This sustained effort has culminated in the adoption of the amendments to the Federal Rules of Civil Procedure discussed in this article.

THE NEW RULE • Rule 26(a)(1)(B) identifies a new category of materials—"electronically stored information"—that is subject to production, in addition to the standard "documents" and "things." (The older phrase from the 1970 amendments—"data compilation"—is being eliminated.) Electronic information is no longer considered a kind of document, but rather a unique category of discoverable material.

The new Rules address several important issues specific to the discovery obligations regarding "electronically stored information:"

- The need for early planning on the scope, timing, form, and management of e-discovery;
- The form of production;
- The increased possibility of inadvertent production of privileged or work product materials involved when massive quantities of data must be produced on a short time schedule;
- The duty to search media that is not easily accessible, such as backup tapes, for relevant material;
- A recognition that electronic materials may be lost due to automatic operation of computer controlled processes and thus not available for production (the "safe harbor" provision); and
- The production of electronic materials in response to third-party subpoenas.

PLANNING FOR ELECTRONIC DISCOVERY • The Rules require early attention to electronic discovery issues. The parties must discuss document retention as it relates to electronically stored information in the Rule 26(f) conference:

"(f) Conference of Parties; Planning for Discovery. ....[a]s soon as practicable and in any event at least 21 days before a scheduling conference is held or a scheduling order is due under Rule 16(b), confer to consider the nature and basis of their claims and defenses and the possibilities for a prompt settlement or resolution of the case, to make and arrange for the disclosures required by Rule 26(a)(1), *to discuss any issues relating to preserving discoverable information*, and to develop a proposed discovery plan that indicates the parties' views and proposals concerning:

"(3) *any issues relating to the disclosure or discovery of electronically stored information, including the form or forms in which it should be produced*...."

(Emphasis added.)

Preservation And Native Format

Thus, there are two issues that are raised by Rule 26(f):

- First, the parties must discuss preservation of relevant documents, and although this new section is not limited to electronic materials, it will no doubt have its greatest effect in this area;

- Second, the parties must discuss the production of electronically stored information specifically. Because the parties must also address the form of the production, it will be necessary for each party to come to the Rule 26(f) conference with an understanding of the form in which the electronically stored information exists (its "native format") and the data management systems in place to organize, identify, and retrieve the electronic materials.

In fact, the Advisory Committee recognizes that "it may be important" for the parties to discuss each party's information management system at the Rule 26(f) conference. This could include, presumably, email systems, storage protocols and media, relevant databases, document management systems, and other information regarding the electronic environment in which a particular party operates. The Advisory Committee references the *Manual for Complex Litigation (Fourth)* §40.25(2) with respect to the matters to be addressed in the meet-and-confer session. Now, with Rules specifically addressing electronically stored information, discussion of these matters will include discussion relating to the production of electronic materials. If the parties agree on a list of relevant topics, for example, the parties will need to discuss the preservation and production of electronically stored information relevant to those issues. For example, in a simple products liability case, a defendant should be prepared to identify the computerized complaint database, the software used, and the general scope of information in the database.

With the new emphasis on substantive discussions about electronically stored information, courts are likely to have higher expectations, particularly in larger cases.

Estimates Of Volume And Cost

In limiting what might otherwise be unduly burdensome discovery, a party may wish to come to a Rule 26(f) conference with estimates of the volumes of material that exist for particular data systems or particular periods of time, and the costs associated with processing, reviewing, and producing that material. It may be possible to narrow the scope, or at least lay the groundwork for later arguing for a narrow scope, by demonstrating the absence of a need to produce certain electronic materials from specified time periods or that are otherwise marginally relevant. Similarly, in cases in which all parties have large caches of electronically stored materials, there will be an incentive to be reasonable. For example, at the Rule 26(f) conference, it may be possible to agree not to seek production from Personal Digital Assistants ("PDAs") or from digital voice mail systems.

Preserve Now, Produce Later?

Alternatively, the parties may agree to preserve certain material but postpone production until such time that it appears that it will be necessary and fruitful to go further in the discovery process. For example, the parties may agree only to produce information from certain databases for specified date ranges. The idea here is to focus on the "low-hanging fruit"—the documents that both parties agree are relevant and producible, and agree to delve further into additional records as the need develops, based on the review of the earliest materials exchanged by the parties and developments in the litigation.

Rule 26 Conference Likely To Be More Important

In the past, Rule 26(f) conferences have often been perfunctory. With the new emphasis on substantive discussions about electronically stored information, courts are likely to have higher expecta-

tions, particularly in larger cases. Thus, the work of preparing for the meet-and-confer will begin immediately upon retention by a client for a federal case. In addition to investigation the factual basis for the action, lawyers will need to simultaneously focus on the identification and preservation of electronic data, so that a reasoned and cost-effective proposal for approaching electronic discovery can be made at the Rule 26(f) conference. The two checklists attached to this article suggest some questions to raise with clients and their information technology personnel at the earliest possible stage of an engagement.

Delay And Destruction

One should anticipate the potential problems associated with the lack of a promptly held meet-and-confer under Rule 26(f). The Rule does not require such a conference until 21 days before the scheduling conference, but depending on the court and the judge, this might be many months after the complaint is filed. Clearly, the motivation for adopting new rules that require early attention to the preservation of electronic materials and the exchange of information about the potentially relevant electronic materials is to prevent inadvertent destruction or alteration of those materials.

This destruction or alteration may fall short of any usual definition of spoliation because of the ephemeral nature of electronic materials. Databases, for example, are often dynamic rather than static, and data will be overwritten as part of the normal operation of the software. If discussion of preservation is delayed, there may be disputes about whether essential data has been lost that could have been retained, in this example, by "ghosting" the database, or taking a snapshot of it at an early point in the litigation. (Note that preservation obligations must be examined not only in the context of the initial suit, in which the parties may agree to limit the scope of a production, but also in the context of potential follow-on or related litigation.)

Rule 16(b)(5) requires the parties to make provisions for the disclosure and discovery of "electronically stored information." Form 35 has also been amended so that the agreements (or disputes) between the parties on these issues can be included in the litigants' report to the court.

Focusing Initial Discovery On Computer And Records Management

The Committee also acknowledges what has already become the practice in many large cases: the need to focus initial discovery on computer and records management systems. Thus, the first deponents may be the Chief Records Officers and Chief Technology Officers, rather than percipient witnesses, as have generally been the case in the past. The Advisory Committee suggests this possibility: "In appropriate cases identification of, and early discovery from, individuals with special knowledge of a party's computer systems may be helpful." A large corporate client may have one individual responsible for email systems and another responsible for financial databases. It may be wise in such instances to exchange organization charts so that the correct individual is named, or in the alternative, to rely on carefully worded deposition notices under Rule 30(b)(6).

For clients who are often involved in litigation, it may be prudent to identify and educate a suitable person for in-house and outside counsel to work with on all e-discovery issues. Moreover, it is important to prepare all company witnesses for examination on topics relating to records retention and production.

THE FORM OR FORMS OF PRODUCTION

• Rule 34(a) and (b) allows the requesting party to specify the form or forms of production. As the Advisory Committee recognizes, the requesting party may not know the best form of production without having information regarding the systems used by the producing party. By discussing this issue early in

the course of litigation, it will be possible to identify instances in which the producing party cannot easily meet the requesting party's demand, and less burdensome alternatives can be explored that may be mutually agreeable.

"Reasonably Useable"

In all cases, under Rule 34(b), electronically stored materials must be produced in a form that is "reasonably useable." If the material cannot be produced in the format requested, it should be produced in the format in which it is kept in the ordinary course of business. In some cases, however, this will not be sufficient because the requesting party may require expensive, proprietary software in order to use it. These situations will need to be addressed by IT professionals. It is safe to expect that the courts will support requesting parties that want production of documents in native format, and in other formats that can be electronically searched.

Who Specifies The Form?

Even if the requesting party does not specify a form or forms of production, Rule 34 requires that the responding party identify the form in which it intends to produce electronic documents in its written response to document requests. If a party makes a unilateral decision to produce documents in a certain form, and that decision is challenged, the court may require that the production be redone to fit the needs of the requesting party. For example, in the past, it has been common to take electronically searchable materials such as email, identify responsive documents, and then convert them before production to a format that is not searchable. In addition, this format typically omits metadata that may be quite relevant to the issues in the case. (Metadata is "data about data." It can show such things as when emails were opened and printed.) This is not likely to be acceptable under the "reasonably useable" language of Rule 34, because such language is clearly designed to allow the requesting party to be able to conduct full text searches of electronic materials.

Native Format Requests

Requesting parties may also request that documents be produced in native format. For example, programs such as Microsoft Excel can have data or notations that do not appear when those documents are printed. This embedded material can include formulas, "sticky" notes, and other commentary. Other programs also have similar features. Metadata will also be included in native file productions, and many litigants believe that metadata will contain the key information. Parties that request the production of electronically stored information in native format are likely to be able to get it. Because these native documents can be altered, both parties will need to consider how authentication will be addressed. This issue is not addressed by the new Rules and could result in substantial controversy as they are implemented. These problems will be more troublesome when dealing with counsel (and courts) unsophisticated in cases involving electronic discovery.

There are also benefits to producing documents in non-native format:

- First and foremost, one avoids the potential for alteration (inadvertent or intentional) of a document;
- Second, it is easier to use software for the initial review of those materials.

One can also assign a unique identifying number to each page, as well as confidentiality footers as appropriate. Thus, the parties should explore various options in this regard. They may agree to produce certain types of documents in native format, such as databases and spreadsheets, but produce other documents, such as email and word processing documents, in non-native format such

as TIFF or PDF formats. The parties might agree to produce the bulk of the electronic materials in non-native format, with the understanding that the requesting party can later ask for selected, important documents to be produced in native format.

Testing And Sampling

Rule 34(a)(1) allows parties the opportunity to test or sample material before inspection, copying, or production. This could benefit both the requesting party as well as the producing party, because it may result in decisions to forgo requests for certain electronically stored materials or to narrow the scope of the requests. Both parties can benefit from efficiencies and cost savings, and the producing party can avoid needless involvement of the court in resolving disputes.

POSSIBLE WAIVERS OF PRIVILEGE AND WORK PRODUCT PROTECTIONS • Rule 26(b)(5) addresses the real risks of inadvertent production of privileged materials when processing and producing millions of gigabytes of data. The Committee recognizes that the challenges of review for attorney-client privilege and attorney work product increase substantially in the electronic environment. Although electronic documents can be searched electronically for the names of lawyers or words such as "legal" or "lawsuit," this approach will not identify every privileged document. For example, a lawyer may have a common name or be referred to in some documents by first name only. In addition, many companies use a standard non-waiver legend containing the words "privileged and confidential" on every email sent by the company. So automated privilege reviews, although useful, do not obviate the need to review every responsive document to determine if it is privileged or attorney work product.

Return Of Potentially Privileged Documents

In recognition of this fact, and in recognition of both the costs and the delays associated with requiring such an exacting examination of every producible document, the new Rule 26(b)(5)(B) allows for a producing party to request the return of a potentially privileged document until the status of the document can be resolved by the court (or, presumably, agreed upon by the parties). In the past, this provision has appeared by agreement in case management orders, or voluntarily in discovery orders, and is often referred to as a "clawback" provision. The receiving party may still claim waiver, but the new Rule provides a mechanism for maintaining the confidentiality of a document while the dispute is being resolved.

Court-Sanctioned Mechanism For Addressing Inadvertent Disclosure

When read in conjunction with Rule 26(f), which includes a discussion of privilege in the issues to be discussed in preparation of a discovery plan, Rule 26(b)(5)(B) will provide a court-sanctioned way to address inadvertent waiver in the e-discovery environment. However, the parties are free to agree upon other methods to address this issue, and can seek court approval for any method they have agreed to. For example, in some instances, parties will produce large volumes of material for inspection in order to allow the receiving party to determine which materials it would like to copy. Generally referred to as the "quick peek," this method allows the producing party to perform a privilege review only on those documents the receiving party has requested. Rule 16(b)(6) also makes it clear that the parties can propose alternatives for addressing privilege issues to the court in the context of pretrial management.

However, there is a significant risk to proceeding without a full privilege review as sanctioned by this Rule because it is procedural and not substan-

tive. The Rule and any agreement of the parties under it, even if approved by the court, does not affect the substantive law of waiver that might be applied in future cases. Other adverse parties seeking the same documents might argue that there was an intentional waiver of any privilege or work product protections.

INACCESSIBLE MEDIA • Rule 26(b)(2) provides that media that is "not reasonably accessible" will not ordinarily be discoverable unless there is a showing of "good cause." If good cause is established by the requesting party, a court may order cost sharing or cost shifting for recovery of backup tapes, legacy materials (electronic data that is dependent on antiquated software or hardware), or similar difficult-to-recover media. In this area and elsewhere, the Advisory Committee seems to have been influenced in substantial part by the multiple opinions of Judge Shira Scheindlin in *Zubulake v. UBS Warburg*, 217 F.R.D. 309 (S.D.N.Y. 2003) ("*Zubulake I*"); 230 F.R.D. 290 (S.D.N.Y. 2003) ("*Zubulake II*"); 216 F.R.D. 280 (S.D.N.Y 2003) ("*Zubulake III*"); 220 F.R.D. 212 (S.D.N.Y. 2003) ("*Zubulake IV*"); 229 F.R.D. 422 (S.D.N.Y. 2004) ("*Zubulake V*").

In addition, although the Rule recognizes two levels of data—accessible and non-accessible—many will view this as not technically accurate, and certainly subject to change as technology evolves. In *Zubulake I*, the court identified five categories of data, based on expert testimony, and determined whether each type was reasonably accessible:

- Active, online data;
- Near-line data, stored but available with only a short delay;
- Offline storage/archives;
- Backup tapes intended for disaster recovery; and
- Erased, fragmented, or damaged data that can only be recovered by a forensic expert.

217 F.R.D. at 318-9. According to Judge Scheindlin, the first three categories are reasonably accessible and the last two are not. *Zubulake* does not address the question of legacy data, which is material stored on obsolete software or hardware. Presumably, because the retrieval of this data generally requires forensic expertise, it would fall in the fifth category of the least accessible material.

The general rule in litigation requires a producing party to bear the costs of its production. In the e-discovery arena, if a requesting party asks for materials that are not reasonably accessible, the *Zubulake* series of cases and subsequent opinions by other courts provide various tests for determining if cost shifting to the requesting party is appropriate. Judge Scheindlin arrived at a seven-part test, in general order of importance:

- The extent to which the request is specifically tailored to discover relevant information;
- The availability of such information from other sources;
- The total cost of production, compared with the amount in controversy;
- The total cost of the production, compared with the resources available to each party;
- The relative ability of each party to control costs and its incentive to do so;
- The importance of the issues at stake in the litigation; and
- The relative benefits to the parties of obtaining the information.

Zubulake III, supra, 216 F.R.D. at 284. Before making a final determination, the court ordered the defendant to restore and produce a small sample of the inaccessible material. The first two factors are the most significant, but the sixth can dominate in some cases.

Falling Costs

One additional point: costs in the area of forensic data recovery are generally falling. What is inaccessible or burdensome today due to cost may not be as expensive a year from now. For example, in the past, backup tapes consisted solely of unindexed data identified only by the date on which the tape was made, and perhaps, the server from which the data was obtained. Now, many vendors are capable of producing indices for backup tapes inexpensively, allowing a producing party to home in on potentially relevant material, as well as to ignore obviously irrelevant material. Thus, the characterization of backup tapes as inaccessible may change.

Stick To The High Road

Finally, lest any party be tempted by the threat of litigation to accelerate the conversion of active or accessible electronic materials to inaccessible formats, it will do so at its own peril. The Committee notes that a party cannot escape its discovery obligations by making accessible material inaccessible. Thus, for example, if a party continued to delete emails after litigation ensued, making the backup tapes the only place where such emails could be found, a court is not likely to look with favor on the conduct.

SAFE HARBOR • Rule 37(f) provides limited protection from sanctions when data is unavailable because of normal computerized processes. The Rule states:

"(f) Electronically stored information. 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."

There was a great deal of controversy about this so-called safe harbor provision during the adoption process, and there is likely to be a great deal of debate about what it means. It may cover, for example, databases that contain information that is automatically updated and overwritten as an inherent part of the database software design. On the other hand, it is not likely to cover a failure to modify a procedure automatically deleting email after some time period.

"Good Faith" Standard

State of mind is key, however, and "good faith" must be shown to avoid sanctions. The Advisory Committee agreed on this "intermediate" test of a party's state of mind, viewing the "good faith" requirement as being more lenient than "intentional" but more demanding than "negligent." Note also that, even in instances in which good faith can be proven, sanctions can still be imposed in "exceptional circumstances." This is another area of ambiguity in the new Rule 37(f) that is likely to generate litigation. Moreover, Rule 37(f) relates to sanctions that can be imposed under the Federal Rules of Civil Procedure, but not to other possible sources of authority to impose sanctions, including, for example, ethical obligations, statutes requiring records retention, or the inherent powers of the court.

Duty To Prevent Destruction

One thing is clear: A party must, when possible, intervene to prevent destruction of relevant electronic materials if such intervention can be accomplished readily. The Advisory Committee states: "The good faith requirement of Rule 37(f) means that a party is not permitted to exploit the routine operation of an information system to thwart discovery obligations by allowing that operation to continue in order to destroy specific stored information that it is required to preserve." For example, if a party has an email system that automatically

deletes emails after a certain period of time, that party will be required to disable that feature for custodians with potentially relevant emails. The requirement to preserve relevant documents and to avoid spoliation is not affected by the safe harbor provisions.

Thus, in the database situation described earlier, it may be necessary to make a static copy of the database at the time litigation began or became foreseeable. For data stored on hard drives, "ghosting" or imaging those hard drives may be a feasible way of preserving data and easing the obligation on the part of a party's employees to affirmatively understand, implement, and adhere to a litigation hold over the course of a long period of time.

Similarly, it is likely that the failure to craft and implement a litigation hold in a timely fashion will threaten a party's ability to claim good faith. Thus, early procedures to prevent destruction of all pertinent materials, including electronic records, is critical and should be considered as soon as litigation is contemplated or foreseeable. Promptly issued litigation holds, along with early meet-and-confers on the preservation and production of electronic materials, will be the key to avoiding sanctions under Rule 37(f) or any other statute, rule, regulation, or ethical standard.

RULE 45 • Finally, Rule 45 makes it clear that subpoenas for records of non-parties also relate to relevant electronically stored information. The subpoena can stipulate the form or forms in which those materials should be produced. It is safe to anticipate efforts to obtain reimbursement of costs associated with responses to particularly broad subpoenas.

CONCLUSION • The new Rules will require immediate and careful planning with regard to the preservation and production of electronic documents. It is more critical than ever that attorneys act quickly in partnership with clients to institute thoughtful and comprehensive litigation holds. Moreover, it will be essential to gain a thorough understanding of a client's information technology at the earliest possible opportunity.

PRACTICE CHECKLISTS FOR
Hear Comes The Judge: The New Federal Rules On E-discovery

Client Interview Checklist

- Review litigation hold in detail and re-emphasize importance of steps necessary for compliance.
- Identify divisions or departments potentially involved in litigation.
- Identify employees with knowledge of relevant facts, including their assistants.
- Identify information technology ("IT") personnel including chief information officer, IT manager, and persons responsible for email, networks, desktops, servers, security, databases, help desk, records management, and voice mail.
- Identify third parties with potentially relevant materials.
- Determine practices regarding communications with the legal department, such as use of attorney-client footers or other clear designation indicating potentially privileged nature of communications.
- Inquire regarding previous litigation holds affecting electronically stored information.
- Inquire regarding previous productions of electronically stored information.

Client IT Personnel Interview

- Identify basic IT functions and hardware that are supported internally.
- Identify IT functions and hardware that are supported externally (outsourced).
- Identify the email system used and how it is supported. Do employees use other email systems?
- Identify auto-delete or auto-archive policies, employee compliance with those policies, and determine modification, if necessary, to meet requirements of litigation hold.
- Identify desktop applications commonly in use.
- Identify core administrative applications, such as financial services, marketing, human resources, work product management, records, and research.
- Identify relevant databases and regularly run reports.
- Obtain information regarding archived material (material retained for archive purposes rather than disaster recovery).
- Obtain information regarding backup policies and practices.
- Obtain information regarding inventories of hardware, re-deployment of computers assigned to departing employees, and disposal practices for computers that are being replaced.
- Identify retention and backup policies, and practices regarding use of PDAs, home computers, and laptops.
- Identify any significant systems upgrades (hardware or software) during the relevant time period.
- Determine if there have been any system failures during the relevant time period that may have affected potentially relevant data.