

THE FEDERAL RULES GOVERNING ELECTRONIC DISCOVERY^{1/}

**By Magistrate Judge Andrew J. Peck
United States District Court
Southern District of New York**

This article summarizes the December 2006 amendments to the Federal Rules of Civil Procedure dealing with discovery of electronically stored information ("ESI") ("e-discovery"), and the September 2008 enactment of Federal Rule of Evidence 502, along with some personal comments and observations.

These rules address five areas: (1) giving early attention to electronic discovery issues; (2) discovery of ESI that is not "reasonably accessible"; (3) privilege issues; (4) application of Rules 33 and 34 to ESI; and (5) a Rule 37 "safe harbor."

Early Attention to Electronic Discovery

Rules 16(b)(5)-(6) and 26(f)(3)-(4) require early discussion of e-discovery issues.

Rule 26(f) requires the parties to discuss at their initial planning conference:

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

(4) any issues relating to claims of privilege or of protection as trial-preparation material, including – if the parties agree on a procedure to assert such claims after production – whether to ask the court to include their agreement in an order; . . .

Rule 26(f)(3)-(4). Similar changes to Rule 16 require that these issues be discussed at the initial pretrial conference with the court. While some judges' Rule 16 conference discussion of these issues will be cursory absent disputes or issues raised by the parties, it is safe to say that the judiciary expects counsel to have thoroughly discussed these subjects at the Rule 26(f) conference (and

^{1/} All opinions expressed herein are my own and may change when the issues are presented in a more specific factual context in litigation before me.

thereafter as further issues arise). Counsel should discuss at the Rule 26(f) conference whose electronic files should be searched and what search terms or protocols to use.

Rule 26(f) also requires counsel "to discuss any issues relating to preserving discoverable information." This is the only reference to preservation (as opposed to production) in the Rules.^{2/} The Advisory Committee Note stresses the reasons for and importance of the direction to counsel to discuss preservation issues:

Rule 26(f) is also amended to direct the parties to discuss any issues regarding preservation of discoverable information during their conference as they develop a discovery plan. This provision applies to all sorts of discoverable information, but can be particularly important with regard to electronically stored information. The volume and dynamic nature of electronically stored information may complicate preservation obligations. The ordinary operation of computers involves both the automatic creation and the automatic deletion or overwriting of certain information. Failure to address preservation issues early in the litigation increases uncertainty and raises a risk of disputes.

The parties' discussion should pay particular attention to the balance between the competing needs to preserve relevant evidence and to continue routine operations critical to ongoing activities. Complete or broad cessation of a party's routine computer operations could paralyze the party's activities. . . . The parties should take account of these considerations in their discussions, with the goal of agreeing on reasonable preservation steps.

The requirement that the parties discuss preservation does not imply that courts should routinely enter preservation orders. A preservation order entered over

^{2/} The preservation obligation almost always will begin before litigation commences. The Federal Rules of Civil Procedure, however, only address obligations once litigation has commenced. Many large companies are implementing email archiving and indexing systems, and ESI retention practices, as a general matter, separate and apart from any specific litigation. That preparation should bring down the cost of discovery of ESI when litigation arises.

objections should be narrowly tailored. Ex parte preservation orders should issue only in exceptional circumstances.^{3/}

Where the litigation involves not just historical information but ongoing ESI and preservation might bring the client's business to a standstill, counsel may be able to discuss and agree at the Rule 26(f) conference that the client need not preserve certain ongoing ESI.

Rule 26(a)(1)(B) requires production, as part of mandatory initial disclosure, of a copy or description of not only "documents" but now also "electronically stored information." The Advisory Committee Note states: "Rule 26(a)(1)(B) is amended to parallel Rule 34(a) by recognizing that a party must disclose electronically stored information as well as documents that it may use to support its claims or defenses." If counsel is unable to identify all ESI at the time of the original Rule 26(a)(1) disclosure, supplementation is required thereafter (and should occur as soon as possible).

The Advisory Committee Note to Rule 26(f) emphasizes the importance of counsel becoming familiar with the client's information technology systems:

It may be important for the parties to discuss those systems, and accordingly important for counsel to become familiar with those systems before the conference. With that information, the parties can develop a discovery plan that takes into account the capabilities of their computer systems. In appropriate cases identification of, and early discovery from, individuals with special knowledge of a party's computer systems may be helpful.

^{3/} For a discussion of the standard for issuance of a preservation order, see Treppel v. Biovail Corp., 233 F.R.D. 363 (S.D.N.Y. 2006) (Francis, M.J.).

In my opinion, it is important for outside counsel to talk directly with the client's information technology ("IT") staff, in addition to inside counsel or other client contacts.^{4/} It is a good idea to have IT personnel at the Rule 26(f) and/or Rule 16 conference (and definitely at any subsequent discovery conferences with the court). Also, since counsel is required to identify "good" electronic data in its Rule 26(a)(1) mandatory initial disclosures, it is important to quickly become familiar with the client's computer system and contents. Moreover, to avoid spoliation problems (discussed below), counsel must get involved with preservation of ESI as early as possible (including before a lawsuit is brought) and must be hands on and give detailed directions to the client. In short, lawyers can no longer afford to be computer-illiterate.

The best practice for counsel to follow is cooperation with opposing counsel and transparency as to the steps taken to preserve and produce ESI. Indeed, I support The Sedona Conference's "Cooperation Proclamation," available at www.TheSedonaConference.Org. The "Cooperation Proclamation" states in no uncertain terms that "Cooperation in Discovery is Consistent With Zealous Advocacy." The "Cooperation Proclamation" further states that "[t]he effort to change the culture of discovery from adversarial conduct to cooperation is not utopian. It is, instead, an exercise in economy and logic." It is the failure to cooperate that increases suspicion, increases the costs of litigation, and is one of the common themes in the sanction cases. Cooperation does not mean that the parties will never have disagreements that require court decision. It will, however, allow the court to decide the issue at the earliest possible time (whether at the Rule 16

^{4/} Counsel should talk to at least three IT people: (1) the department head as to the company's policies, (2) a person running the system, to see what is actually done, and (3) the longest serving IT person, who is likely to know about legacy systems and the closet full of backup tapes that everyone else has forgotten.

conference or thereafter) with a helpful record – rather than at the end of discovery (or even, as in Qualcomm, during trial), when the only remedy is preclusion, an adverse inference instruction or monetary or other sanctions.

While Rule 26(f) refers to a single conference, cooperation among counsel will require frequent meetings or discussions between opposing counsel during the e-discovery process. It is unlikely that all issues will have been resolved in the initial Rule 26(f) conference. E-discovery is an iterative process.

One form of cooperation that can work well is to have the in-house IT personnel from both sides informally talk to each other (since to some extent they speak a different language than the rest of us).

Rule 26(b)(2)(B) and "Inaccessible" Data

Rule 26(b)(2)(B) sets up a distinction between "accessible" electronically stored information that can be discovered without court intervention, and "not reasonably accessible" ESI that requires good cause and court order:

A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

Rule 26(b)(2)(B) has been described as a "two-tier system," i.e., one where lawyers first sort through the electronically stored information that can be provided from easily accessed sources and then determine whether it is necessary to search the difficult-to-access sources.

The Advisory Committee Note makes clear that while the responding party determines what is not reasonably accessible, it must do so openly, that is, the "responding party must also identify, by category or type, the sources containing potentially responsive information that it is neither searching nor producing."^{5/}

An earlier version of the Advisory Committee Note provided further guidance as to what was "inaccessible" (but those comments were deleted from the final Committee Note): If the producing party routinely uses the data, or if the producing party accessed otherwise inaccessible data for its own benefit in the lawsuit, it is considered accessible. In my opinion, that approach is likely to continue. In my opinion, not reasonably accessible data presumably includes disaster recovery data, "legacy" data from obsolete systems, and "deleted" data (i.e., data a person believes was deleted but which remains, unindexed, on the computer); however, with advances in technology (and reductions in restoration and/or search costs), that may well change. Accessibility really comes down to a cost-benefit analysis.

The Advisory Committee Note provides extensive guidance on the requesting and responding parties' respective burdens, and the likely need for discovery to satisfy the burden. It is worth quoting the Note at length:

If the parties cannot agree whether, or on what terms, sources identified as not reasonably accessible should be searched and discoverable information produced, the issue may be raised either by a motion to compel discovery or by a motion for a protective order. The parties must confer before bringing either motion. If the parties do not resolve the issue and the court must decide, the responding party must show that the identified sources of information are not reasonably accessible because

^{5/} The Advisory Committee Note also makes clear that identifying a source "as not reasonably accessible does not relieve the party of its common-law or statutory duties to preserve evidence."

of undue burden or cost. The requesting party may need discovery to test this assertion. Such discovery might take the form of requiring the responding party to conduct a sampling of information contained on the sources identified as not reasonably accessible; allowing some form of inspection of such sources; or taking depositions of witnesses knowledgeable about the responding party's information systems.

Once it is shown that a source of electronically stored information is not reasonably accessible, the requesting party may still obtain discovery by showing good cause, considering the limitations of Rule 26(b)(2)(C) that balance the costs and potential benefits of discovery. The decision whether to require a responding party to search for and produce information that is not reasonably accessible depends not only on the burdens and costs of doing so, but also on whether those burdens and costs can be justified in the circumstances of the case. Appropriate considerations may include: (1) the specificity of the discovery request; (2) the quantity of information available from other and more easily accessed sources; (3) the failure to produce relevant information that seems likely to have existed but is no longer available on more easily accessed sources; (4) the likelihood of finding relevant, responsive information that cannot be obtained from other, more easily accessed sources; (5) predictions as to the importance and usefulness of the further information; (6) the importance of the issues at stake in the litigation; and (7) the parties' resources.

The responding party has the burden as to one aspect of the inquiry – whether the identified sources are not reasonably accessible in light of the burdens and costs required to search for, retrieve, and produce whatever responsive information may be found. The requesting party has the burden of showing that its need for the discovery outweighs the burdens and costs of locating, retrieving, and producing the information. In some cases, the court will be able to determine whether the identified sources are not reasonably accessible and whether the requesting party has shown good cause for some or all of the discovery, consistent with the limitations of Rule 26(b)(2)(C), through a single proceeding or presentation. The good-cause determination, however, may be complicated because the court and parties may know little about what information the sources identified as not reasonably accessible might contain, whether it is relevant, or how valuable it may be to the litigation. In such cases, the parties may need some focused discovery, which may include sampling of the sources, to learn more about what burdens and costs are involved in accessing the information, what the information consists of, and how valuable it is for the litigation in light of information that can be obtained by exhausting other opportunities for discovery.

The good-cause inquiry and consideration of the Rule 26(b)(2)(C) limitations are coupled with the authority to set conditions for discovery. The conditions may take the form of limits on the amount, type, or sources of information required to be accessed and produced. The conditions may also include payment by the requesting party of part or all of the reasonable costs of obtaining information from sources that are not reasonably accessible. A requesting party's willingness to share or bear the access costs may be weighed by the court in determining whether there is good cause. But the producing party's burdens in reviewing the information for relevance and privilege may weigh against permitting the requested discovery.

The limitations of Rule 26(b)(2)(C) continue to apply to all discovery of electronically stored information, including that stored on reasonably accessible electronic sources.

The test simplifies to a balancing test of the requesting party's need compared to the burden (and expense) on the producing party; in short, a cost-benefit analysis. The Advisory Committee Note also indicates that in performing this balance, the producing party's burden in reviewing ESI for relevance and privilege is a factor that the court can consider (but that review cost, as opposed to the restoration and search cost, ordinarily cannot be shifted to the requesting party).^{6/}

Privilege "Claw-Back" and Inadvertent Production of Privileged Material

Rules 16 and 26(f), discussed above, require the parties to discuss whether they will agree to allow production of ESI without a careful privilege review and without waiver of the privilege, referred to in the literature as "claw-back" or "sneak-peek" agreements.^{7/}

^{6/} Another source of "inaccessibility," not discussed by the Advisory Committee Notes, is where the ESI is located abroad and may be covered by that country's privacy, bank secrecy or other blocking statutes. See Societe Nationale Industrielle Aerospatiale v. United States Dist. Ct. for S. Dist. of Iowa, 482 U.S. 522, 107 S. Ct. 2542 (1987).

^{7/} Implicit in Rules 16(b)(6) and 26(f)(4) is that the court can order such a provision only if the parties agree to it. The Advisory Committee Note to Rule 16(b) states that "[t]he rule does not provide the court with authority to enter such a case-management or other order without party agreement, or limit the court's authority to act on motion." Recently adopted Federal
(continued...)

The Advisory Committee on Evidence Rules proposed Federal Rule of Evidence 502 (introduced in Congress as S. 2450) to deal with several privilege waiver issues, including the ability to enforce "clawback" agreements in subsequent federal or state litigation. Rule 502 was enacted by Congress and signed by the President, effective as of September 19, 2008.

Federal Rule of Evidence 502 has several key provisions. First, it makes uniform for all federal courts the rule for determining whether production of privileged information (documents or ESI) in litigation constitutes a waiver. It adopts what was the majority rule, that disclosure is not a waiver if (i) it was inadvertent, (ii) the holder of the privilege took reasonable steps to prevent disclosure, and (iii) the holder took prompt steps to rectify the error. Fed. R. Evid. 502(b).

It is always embarrassing to counsel to have to litigate whether production went beyond inadvertent to sufficiently careless to have waived the privilege. To avoid that problem Rule 502 allows, and protects, the "clawback" agreements. Rule 502(d) and (e) provide:

(d) Controlling Effect of a Court Order. – A Federal court may order that the privilege or protection is not waived by disclosure connected with the litigation pending before the court – in which event the disclosure is also not a waiver in any other Federal or State proceeding.^{8/}

^{7/} (...continued)

Rule of Evidence 502, however, allows the court to enter a non-waiver order without the parties' agreement.

^{8/} The Advisory Committee Note to Rule 502(d) states:

Under the rule, a confidentiality order is enforceable whether or not it memorializes an agreement among the parties to the litigation. Party agreement should not be a condition of enforceability of a federal court's order.

This appears to conflict with Fed. R. Civ. P. 16 and 26's implicit limitation on entry of non-waiver orders to where the parties have agreed.

(e) Controlling Effect of a Party Agreement. – An agreement on the effect of disclosure in a Federal proceeding is binding only on the parties to the agreement, unless it is incorporated into a court order.

I suggest that in every case where you are producing approximately the same or more ESI than your adversary, you seek a court-ordered clawback agreement. With the huge quantity of ESI to review, an arguably privileged document is sure to slip through, no matter how careful you try to be. The clawback agreement allows you to avoid litigating how it slipped through the cracks.

On the related subject of inadvertent production, Fed. R. Civ. P. 26(b)(5)(B) provides a procedural mechanism for dealing with claims of inadvertent production of privileged material, applicable both to paper documents and ESI. The Rule allows a party that inadvertently produced privileged material to request it back; the receiving party must return it or sequester it, or can "promptly present it to the Court under seal for a ruling." The Advisory Committee Note makes clear that "[t]he proposed amendment does not address the substantive question whether privilege or work product protection has been waived or forfeited. Instead, the amendment sets up a procedure to allow the responding party to assert a claim of privilege or work-product protection after production." In my opinion, the Rule merely codifies current procedural practice.

ESI, and particularly email "chains," create complications for the party preparing "privilege logs," as required by Fed. R. Civ. P. 26(b)(5) and many courts' local rules. (See, e.g., SDNY/EDNY Local Civil Rule 26.2, specifying the information to be included in the privilege log.) For a good discussion of the correct way to prepare the privilege log for email chains, see Muro v. Target Corp., 243 F.R.D. 301 (N.D. Ill. 2007). On the other hand, in situations where there are too

many privileged emails to log one by one, some courts have liberalized the requirements of privilege logging to reduce the burden.

Another privilege related issue is whether "litigation hold" memos and similar instructions from counsel to the client as to preservation and production are privileged. Some decisions find the litigation hold memo to be privileged but not what was done. E.g., In re Ebay Seller Antitrust Litig., No. C 07-01882, 2007 WL 2852364 at *2-3 (N.D. Cal. Oct. 2, 2007); see also Paul D. Grimm, et al., "Discovery About Discovery: Does the Attorney-Client Privilege Protect All Attorney-Client Communications Relating to the Preservation of Potentially Relevant Information?," 37 U. Balt. L.Rev. 413 (2008). In any event, transparency and cooperation should prevent this from becoming an issue, but if it does become an issue, you need a witness or witnesses who can testify as to the reasonableness of the client's preservation and production processes.^{2/}

Changes to Rules 33 and 34: ESI and Form of Production

Rule 34(a) separates paper "documents" from "electronically stored information." Nevertheless, the Advisory Committee Note makes clear that "a Rule 34 request for production of 'documents' should be understood to encompass, and the response should include, electronically stored information unless discovery in the action has clearly distinguished between electronically stored information and 'documents.'" In my opinion, however, requests should specifically and separately request electronically stored information so there can be no question. This also has the

^{2/} Another "is it privileged issue" relates to draft expert reports. Proposed amendments to Fed. R. Civ. P. 26(b)(3), if enacted, would protect experts' oral and written drafts. See Gregory P. Joseph, "Federal Practice: Expert Witness Rules," National L.J. 9/8/08 at 13.

additional benefit of focusing the responding party on its e-discovery obligations (at least until it becomes more second-nature for counsel and their clients).

Consistent with the possibility of sampling to determine whether electronic sources are accessible, Rule 34(a)(1) makes clear that parties may request an opportunity to test or sample materials sought, whether electronic or hard copy material.

Rule 34(b) provides that the requesting party may specify the form or forms in which electronically stored information is to be produced. The requesting party can specify different forms for different types of ESI (e.g., one form for email, a separate form for word-processing documents). Each type of ESI need only be produced in one form. If the requesting party does not specify a form, the responding party can produce ESI in a form "in which it is ordinarily maintained or in a form or forms that are reasonably usable." Where the requesting party has specified the form it wants, the responding party may object to the form specified by the requesting party.

While in the absence of agreement the responding party can choose the form of production, it cannot convert the data to a form that is more burdensome or less searchable. The Advisory Committee Note provides that "the option to produce in a reasonably usable form does not mean that a responding party is free to convert electronically stored information from the form in which it is ordinarily maintained to a different form that makes it more difficult or burdensome for the requesting party to use the information effectively in the litigation. If the responding party ordinarily maintains the information it is producing in a way that makes it searchable by electronic means, the information should not be produced in a form that removes or significantly degrades this feature."

"Under some circumstances, the responding party may need to provide some reasonable amount of technical support, information on application software, or other reasonable assistance to enable the requesting party to use the information." Neither the Rule nor the Advisory Committee Note addresses the issue of copyrighted or proprietary software that may be needed to utilize the electronic information (particularly where e-data is sought from the opposing party's expert witness). In cases involving huge databases, it may be necessary for the producing party to run reports as requested by the requesting party.

If the requesting party wants "metadata," it should so state in its request. Cases go both ways as to whether metadata needs to be produced. See, e.g., Williams v. Sprint, 230 F.R.D. 640 (D. Kan. 2005). Technology now has reduced the technological cost of producing metadata (indeed, it apparently is more expensive to eliminate the metadata), but there is usually a large cost in lawyer time to review the metadata for production. Clawback agreements as to the metadata may be a solution. Moreover, metadata is a term loosely used to cover different things, from "track changes" in a word-processing document, to the identification of senders and recipients of email, to much more "complicated" computer-generated information.

A practice point: the parties should consider whether at the Rule 26(f) conference to agree that despite the "one form" of production rule, a party can ask for an additional form of production for specified and limited ESI (e.g., if there was no request for metadata in general, agreement that the party can later request it for a few "key" ESI documents).

Parallel changes are made to Rule 45 for e-discovery from non-parties. Courts, however, are more likely to shift costs where e-discovery requests are made to a true non-party. See

The Sedona Conference "Commentary on Non-Party Production & Rule 45 Subpoenas" (April 2008), available at www.TheSedonaConference.Org.

While not strictly a "form of production" issue, it is important for counsel to be transparent about the search procedures it will use, both in terms of which custodians will be searched and what search method will be used. Counsel should be aware of recent decisions criticizing (and imposing sanctions with respect to) key word searches designed by counsel without adequate explanation of why those terms were used or what "quality control" was employed to determine whether those key words worked. See, e.g., Victor Stanley, Inc. v. Creative Pipe, Inc., No. MSG-06-2662, 2008 WL 2221841 at *3 (D. Md. May 29, 2008) (Grimm, M.J.); In Re Seroquel Prod. Liability Litig., 244 F.R.D. 650 (M.D. Fla. 2007) (Baker, M.J.). This problem can be largely avoided where counsel discuss and agree upon the search protocols. Beside key word searches, other search methods include Boolean searching, proximity searching, concept-based searching, clustering and Bayesian search methods. Whatever method you want to use, the "best practice" is to discuss it in advance with opposing counsel.

Rule 37: Sanctions and A "Safe Harbor"

Rule 37(e), originally enacted as 37(f), provides a so-called "safe harbor," as follows:

(e) 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.

The Advisory Committee Note gives some guidance about "good faith"^{10/} and the need for a "litigation hold":

Rule 37[(e)] applies to information lost due to the routine operation of an information system only if the operation was in good faith. Good faith in the routine operation of an information system may involve a party's intervention to modify or suspend certain features of that routine operation to prevent the loss of information, if that information is subject to a preservation obligation. A preservation obligation may arise from many sources, including common law, statutes, regulations, or a court order in the case. The good faith requirement of Rule 37[(e)] 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. When a party is under a duty to preserve information because of pending or reasonably anticipated litigation, intervention in the routine operation of an information system is one aspect of what is often called a "litigation hold." Among the factors that bear on a party's good faith in the routine operation of an information system are the steps the party took to comply with a court order in the case or party agreement requiring preservation of specific electronically stored information.

Rule 37(e) does not address when the duty to preserve first arises. For example, the duty to preserve clearly arises on receipt of a Rule 34 request; it arises even earlier, as soon as the defendant is served with the complaint, at least for material that is clearly discovery-relevant to the case; and it almost definitely arises when an employee files an EEOC complaint. Does it arise when an employee complains internally to Human Resources, or when a company is considering a reduction-in-force ("RIF") that may lead to litigation? The party's prior experience in these situations may help determine if a duty to preserve arises. And whenever the duty to preserve arises, how broad is the scope of the material to be preserved? Only time, and case law, will answer these questions definitively. For now, it is enough to note that whether litigation is "reasonably anticipated" is not a new concept; that is the test for the work product privilege. If a party claims

^{10/} The Rule 37(e) "good faith" safe harbor is an "intermediate" standard from the two alternative proposals originally considered: negligence and intentional failure to preserve.

work product privilege at a particular point prior to litigation, it should have taken steps to preserve ESI at or before that point.^{11/}

In my opinion, for preservation steps to be reasonable, an email or memo to the client's employees to preserve data is not, by itself, enough. After the hold memo is issued, counsel should speak directly to the key players and their support staff, as well as the IT department. These steps should be repeated as time goes on. However, in employment discrimination cases, employers have to be wary of creating information that could lead to an assertion of retaliation against a plaintiff still employed by the company; an IT department-based hold might be preferable in that situation. Counsel should document all steps taken to preserve and later to produce ESI.

In my opinion, counsel's litigation hold and later search and production efforts must be "transparent." While it might be argued that counsel's efforts are work product (see above), if there is a spoliation claim it is impossible to show "reasonableness" and good faith to the court without telling the court what you did. Counsel needs to have someone on the team (other than lead trial counsel) in a position to testify about what was done, why it was done, and why that is reasonable.

There are many "check lists" available in the literature (and presented at conferences). One such article is The Sedona Conference "'Jumpstart Outline': Questions to Ask Your Client and Your Adversary to Prepare for Preservation, Rule 26 Obligations, Court Conferences and Requests for Production (Public Comment Draft)" (May 2008), available at www.TheSedonaConference.Org.

^{11/} For an interesting discussion of how to deal with preservation decisions before litigation has been commenced where there is no opposing counsel with whom to have a dialog, see The Sedona Conference "Commentary on Preservation, Management and Identification of Sources of Information That Are Not Reasonably Accessible" (July 2008), available at www.TheSedonaConference.Org.

Counsel should prepare customized checklists and other procedures for use in their cases, so counsel does not have to start from scratch when litigation arises (because any delay can lead to unintentional loss of ESI). In-house counsel especially should establish an ESI retention system (and educate all company employees as to the system) and litigation hold procedures that can be rapidly implemented when litigation occurs or is reasonably anticipated. A response team of counsel, IT and records management personnel and senior management (to advocate the system within the company) should be established. Counsel needs to inquire as to the company's policy, and practice, as to use of home computers and home email accounts, and be sure to inquire about all sources of ESI including laptops, Blackberries and other PDAs, instant messaging, voice messages and, in regulated industries, recorded telephone calls, etc.

In most of the reported spoliation sanction cases (e.g., Zubulake, Metropolitan Opera, Morgan Stanley, Qualcomm, and my decision, In re NTL, Inc. Sec. Litig., 244 F.R.D. 179 (S.D.N.Y. 2007) (Peck, M.J.)), sanctions occurred because counsel ignored their e-discovery obligations, or, most importantly, were not candid with opposing counsel and the court.^{12/} There is now a great deal of instruction in the case law and literature as to what counsel must do to be "reasonable" in preserving and later searching for and producing ESI.

^{12/} These cases, particularly Qualcomm, raise issues as to the duties of and potential practical conflict between in-house and outside counsel. An important way to avoid problems, however, is to be sure to be completely open and honest with opposing counsel and especially the court. Where in-house counsel has a hands-on role in the preservation and/or production of ESI, that in-house counsel may need to attend discovery conferences with the court to insure that what the court is told is accurate.

Conclusion

The December 2006 amendments to the Federal Rules of Civil Procedure provide only the broadest guidance; the detailed e-discovery rules largely will flow from judicial decisions (often by Magistrate Judges), many of which may be announced from the bench or contained in unpublished orders or opinions, and few of which will be subject to effective appellate review. (Indeed, already one can find cases with apparently contradictory results.) The new Rules, however, really just take good (paper) document production practices have been used for years and "translate" them over to ESI.

The early discussion requirement of Rules 16 and 26 should significantly reduce those e-discovery problems that come from counsels' different understandings (or lack of understanding) and failure to focus on and understand electronic discovery. Counsel must cooperate with each other to cost-effectively preserve and produce ESI. The steps taken to produce ESI should be transparent (i.e., discuss with the other side which key players will be searched, what search terms or techniques will be used, etc., rather than making a unilateral choice and having a fight as to its sufficiency after the fact). I certainly hope that counsel will take the Sedona Conference "Cooperation Proclamation" to heart. Where e-discovery issues are brought before the court, counsel needs to educate the judge and show that counsel and the client acted reasonably (and it is a "best practice" to have an IT person and/or in-house counsel at all such conferences, as discussed above). Cooperation also should significantly reduce the cost of discovery of ESI.

Discovery of ESI is only the beginning. The next issue that we all will face is admissibility of ESI at trial. Magistrate Judge Paul Grimm recently issued a detailed and extensive opinion on that subject (including authentication and hearsay issues), which should be required reading for all counsel. Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534 (D. Md. 2007).

A. J. P.

Rev. 10/8/08