

**THE DECEMBER 2006 FEDERAL RULES AMENDMENTS
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 proposed Federal Rule of Evidence 502, along with some personal comments and observations.

The rule amendments address five related areas: (1) giving early attention to electronic discovery issues; (2) discovery of electronically stored information 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

^{1/} Prior versions of this paper appeared in Labor and Employment Law, Vol. 33, No. 4 (Summer 2005), and in the Program Material for the ABA Employment Rights & Responsibilities March 2006 Meeting. All opinions expressed herein are my own and may change when the issues are presented in a more specific factual context in litigation before my court.

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 thereafter as further issues arise).

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. 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 objections should be narrowly tailored. Ex parte preservation orders should issue only in exceptional circumstances.

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. Counsel also can discuss at the

Rule 26(f) conference whose electronic files should be searched and what search terms or protocols to use.

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.

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. It even may be useful to have someone from the IT staff at the Rule 26(f) and/or Rule 16 conference (and 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.

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."^{2/}

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

^{2/} 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."

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 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 cost, as opposed to the restoration and search cost, ordinarily cannot be shifted to the requesting party).

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. 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." Proposed Evidence Rule 502, discussed below, would allow the court to enter a non-waiver order without the parties' agreement.

The language of Rules 16 and 26 as adopted deleted the draft's reference to the court's order "protecting the right to assert privilege after production of privileged information," since the Rules have no substantive effect outside of the specific litigation. While the parties' agreement is binding in that litigation, whether it is sufficient to preserve the privilege in subsequent litigation with a different adversary will be decided by the substantive privilege waiver case-law. Counsel, particularly corporate counsel, should consider carefully this problem, and the risks for future litigation, when making decisions about how much expense to devote to pre-production privilege review of electronic data. See Hopson v. Baltimore, 232 F.R.D. 228 (D. Md. 2005).

As a result of this issue, the Advisory Committee on Evidence Rules has proposed Federal Rule of Evidence 502 to deal with several privilege waiver issues, including the ability to enforce so-ordered "clawback" agreements in subsequent federal or state litigation. Proposed Rule 502 is on a separate track, and even if approved, would not take effect before December 2008 (and to have effect in state court litigation, must be statutorily enacted by Congress, beyond the normal rules enactment procedures). Proposed Evidence Rule 502 states in relevant part:

(d) Controlling effect of 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. The order binds all persons and entities in all federal or state proceedings, whether or not they were parties to the litigation.

(e) Controlling effect of party agreement. – An agreement on the effect of disclosure is binding on the parties to the agreement, but not on other parties unless it is incorporated into a court order.

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.

A practice point: counsel sending "privileged" emails can reduce the review cost by including the word "Privileged" in the "re" line of the email. Companies also may want to use a separate server for the in-house legal department.

On the related subject of inadvertent production, Rule 26(b)(5)(B) provides a procedural mechanism, without changing the substantive law, 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. The issue of whether such inadvertent production waives the privilege is not addressed by the Rule, and is left to the case law. Proposed Federal Rule of Evidence 502(b)-(c), holds that there is no waiver for inadvertent disclosure if the holder of the privilege "took reasonable steps to prevent disclosure" and "promptly took reasonable steps to rectify the error."

ESI, and particularly email "chains," create some 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 privilege log email chains, see Muro v. Target Corp., No. 04 C 6267, --- F.R.D. ---, 2007 WL 1630407 (N.D. Ill. June 7, 2007).

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, and for the 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).

If the requesting party wants "metadata," it should so state in its request. Whether metadata should or should not be ordered produced is an unsettled issue. See 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. Claback agreements as to the metadata may be a solution.

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.

Rule 37: Sanctions and A "Safe Harbor"

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

(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.

The Advisory Committee Note gives some guidance about "good faith"^{3/} and the need for a "litigation hold":

Rule 37(f) 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(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. 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(f) does not address when the duty to preserve first arises. For example, in my opinion, the duty clearly arises on receipt of a document 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 probably 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? 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

^{3/} The Rule 37(f) "good faith" safe harbor is an "intermediate" standard from the two alternative proposals originally considered: negligence and intentional failure to preserve.

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 work product privilege at a particular point prior to litigation, the duty to preserve similarly should apply at that point.

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. Counsel should speak directly to the key players and their support staff, as well as the IT department, and remind them again as time goes on. However, 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.

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, 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 like this one). Counsel should utilize them and 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 personnel and senior management (to advocate the system within the company) should be established.

In most of the reported spoliation sanction cases (e.g., Zubulake, Metropolitan Opera, Morgan Stanley, and my decision, In re NTL, Inc. Sec. Litig., No. 02 Civ. 3013 & 7377, 2007 WL 241344 (S.D.N.Y. Jan. 30, 2007) (Peck, M.J.)), sanctions occurred because counsel ignored their e-discovery obligations, used only a memo without any follow-up, and/or were not candid with opposing counsel and the court. 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.

Conclusion

The new Rules provide only the broadest guidance; the detailed e-discovery rules largely will flow from judicial decisions, 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. The new Rules, however, really just take good (paper) document production practices that we all have used for years and "translate" them over to electronic information.

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. Where e-discovery issues are brought before the court, counsel needs to educate the judge and show that counsel and client acted reasonably.

Most importantly, it is no longer acceptable for counsel to inform the court that they do not understand their client's electronic data systems. Attorneys, young and old, must become sufficiently electronically "literate."

The next issue that we all will face is admissability of ESI at trial. Magistrate Judge Paul Grimm recently (May 2007) issued a detailed opinion on that subject, which should be required reading. Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534 (D. Md. 2007).

A. J. P.

8/10/07