

## Legal Alert: E-discovery Amendments to the Federal Rules of Civil Procedure to Take Effect on December 1, 2006

September 14, 2006

On December 1, 2006, amendments to the Federal Rules of Civil Procedure relating to discovery of “electronically stored information” (ESI) take effect. These amendments codify on a national scale the access that litigants in federal court have to the vast array of ESI produced in the course of business. The Amendments do little to alter the kind of information subject to disclosure; “any matter, not privileged, and relevant” remains the familiar phrase outlining the scope of discovery. The Amendments instead target three sensitive e-discovery issues: volume of information, variability of form, and routine destruction of data. The emphasis is on faster, cheaper, and less-risky disclosures.

In short, the Amendments address the following:

- Initial disclosures relating to a party’s claims or defenses that involve ESI
- Early discussion of e-discovery and judicial recognition of party agreements
- Limiting discoverability of ESI that is not reasonably accessible
- Providing a procedure to recapture inadvertent disclosures in order to litigate privilege
- Allowing substitution of access in place of a response to an ESI-related interrogatory
- Amending the scope of a request for production to include ESI and establishing a procedure for determining form of production
- Shielding parties from sanctions for good-faith routine destruction of ESI in limited circumstances
- Updating subpoena practice to conform to the above.

Due to judicial developments in recent years, the discoverability of information found on servers, laptops, PDAs, or internal phone and fax logs is nothing new for most attorneys. Amendments to the Rules in 1970 entitled a party to documents “including . . . phonorecords and other data compilations” translated, if necessary, into reasonably usable form (usually a computer printout). Many courts also interpreted “documents” generally to include most forms of ESI, concluding that insistence on tangibility or “fixed expression on paper” would permit

improper evasion of discovery obligations simply because the language of the Rules failed to reflect the ever-evolving technological landscape.<sup>1</sup>

Nevertheless, the special issues raised by e-discovery, the risk of a patchwork of local rules frustrating the federal interest in uniformity,<sup>2</sup> and the increased difficulty of fitting the dynamic forms of ESI within the traditional concept of a “document” inspired the Advisory Committee (“the Committee”) that prepared the Amendments for Judicial Conference review to amend the Rules to explicitly recognize ESI, and place electronic evidence “on equal footing with the discovery of paper documents.”<sup>3</sup>

The 2006 Amendments also emphasize recent trends in case law and case planning to avoid the costs of resolving electronic discovery disputes late in the litigation, long after the Rule 26(f) scheduling conference, described below. Finally, the Amendments provide new protection against undue hardship and address sensitive interests such as privilege, which suffers increased vulnerability following a massive digital disclosure.

### **Changes in Focus: Rules 16, 26, 33, 34, 37, 45 and Form 35.**

#### *Definitional Amendments—Including ESI in Old Language.*

A few of the 2006 Amendments merely shoehorn ESI into the familiar laundry list of information subject to discovery.

Rule 26(a), for example, adds ESI to the list of sources of information subject to a party’s initial disclosure obligations.<sup>4</sup> Although describing the sources of information or system processes relating to discoverable information for purposes of making initial disclosures sounds burdensome, the Committee considered this simply a “conforming amendment” to prior practice;

---

<sup>1</sup> In the Rules, the replacement of “data compilations” with ESI eliminates an “archaic” description and makes the Rules “flexible enough to encompass future changes and developments.” Committee Note to Rule 34(a). See also Summary of the Report of the Judicial Conference Committee On Rules of Practice and Procedure, September 2005, at App. C-64, available at <http://www.uscourts.gov/rules/Reports/ST09-2005.pdf> [hereinafter “Rules Report”].

<sup>2</sup> Rules Report, at App. F-4.

<sup>3</sup> However, parties and courts should continue the prevailing judicial practice of interpreting requests for production of “documents” under Rule 34 to include ESI unless the circumstances clearly distinguish between the two. Rules Report, App. C-65. Still, the Committee hopes that the distinction will ultimately prevail and “documents” will not “continue to be stretched to accommodate the [important] differences.” Rules Report, at 28.

<sup>4</sup> See Rule 26(a)(1)(B) (“[a party must, without awaiting a discovery request, provide] a copy of, or description by category and location of, all documents, *electronically stored information*, and tangible things . . . in [the party’s] possession . . . and that the disclosing party may use to support its claims or defenses . . . .”) (emphasis added).

it did not even publish the amendment for public comment.<sup>5</sup> Noting concerns about the burden of requiring parties to locate and disclose ESI “too early” in the case, the Committee responded that “[t]he obligation does not force a premature search, but only requires disclosure, either initially or by way of supplementation, of information that the disclosing party has decided it may use to support its case,” whatever the form.<sup>6</sup>

The Amendments have also added ESI to the “substitution option” of Rule 33(d), which allows a party to substitute access to business records in place of the sought-after response to an interrogatory if the burden of ascertaining the answer from those records is “substantially the same for the party serving the interrogatory as for the party served.” Like the pre-existing form of Rule 33(d), the party served must provide a “reasonable opportunity” for the inquiring party to locate, identify, and derive the information requested in the interrogatory “as readily as can the party served.”<sup>7</sup>

Finally, Rule 34(a) adds ESI to the inclusive list of *sources* of information subject to a request to produce (while the *scope* of information proper for discovery remains governed by Rule 26, discussed below). Comparatively, Rule 45, concerning subpoena practice in discovery, has followed the same course, making clear that discovery of ESI is also available by subpoena and mimicking the special ESI protections relating to discovery between the parties to litigation, described below. The Committee recommends special emphasis on the protective provisions of Rule 45, in contrast to Rule 34, because of the particular interests in privacy and confidentiality of non-parties subject to a subpoena for ESI.<sup>8</sup>

*Form, Volume, and Routine: Recognition of the Unique Aspects of ESI Disclosure and Preparing Rule Practice to Deal with Problems at the Earliest Opportunity.*

More comprehensive amendments were necessary to address the special difficulties of formally including ESI within the traditional discovery process.

For instance, Rule 34(b) addresses the reality that production of ESI in forms different from how a party regularly maintains the information in the ordinary course of business may often be appropriate. The amended rule now allows the *requesting* party the opportunity to specify the form in which it wants ESI produced. If the requesting party fails to specify a particular form, or if the responding party objects to a certain form, the latter must propose an alternative form. While not necessarily the form in which the information was originally maintained, the alternate form must be at least “reasonably usable.”

---

<sup>5</sup> The 1970 insertion of “data complications” in the Rules where ESI now appears allowed the initial disclosure obligation to evolve so that no practical change was necessary. Rules Report, at 26.

<sup>6</sup> Rules Report, App. C-23.

<sup>7</sup> Committee Note to 33(d).

<sup>8</sup> Cf. Rule 45(c)-(d).

Responding to a request for production of (or access to) information compressed on backup drives is a far different exercise than emptying file cabinets. Rule 26(f) broadens the scope of the parties' mandatory discovery conference, requiring discussion of issues relating to discovery and disclosure of ESI, if any, "including the form or forms in which [the ESI] should be produced," an issue complicated by amended Rule 34.<sup>9</sup> Also continuing the theme of early planning and settlement of disputes, amended Rule 26(f)(4) pushes the parties to reach agreement on the handling of privileged matter, whether encountered before or even *after* disclosure (so-called "quick peek" protocols or clawbacks, described below). Finally, the Committee seized upon another prevailing theme by adding "discuss[ion] [of] issues relating to *preserving* discoverable information" to the general description of the conference's purpose in the introductory language of Rule 26(f). While the increased risk of destruction or spoliation of ESI inspired this slight change, issues of preservation in any medium are proper for discussion at the conference.<sup>10</sup>

Once the parties have mapped out their discovery plan in the 26(f) conference, amended Rule 16(b)(5) permits the court to expedite and enforce the special ESI obligations by adopting tailored provisions in its scheduling order. If the parties reached agreement with a "quick-peek" protocol or similar agreement, Rule 16(b)(6) allows the court to incorporate the agreement within the scheduling order as well. Similarly, the Amendments slightly alter part III of Form 35 to inform the court of the parties' ESI discovery plans and any special agreements.

### Inadvertent Disclosure and Undue Burden Issues.

Three major changes appear in the Rules to protect parties from over-exposure in meeting their e-discovery obligations.

First, Rule 26(b)(2)(B) addresses the vast expense that can accompany a request to produce or provide access to ESI by distinguishing between "reasonably accessible" and not reasonably accessible ESI. The party opposing the request has the initial burden to show that the information described is "not reasonably accessible" due to undue burden or cost."<sup>11</sup> This is an

---

<sup>9</sup> In addition to discussing the nature and extent of the contemplated discovery, as well as the burden and cost of retrieving the information, i.e., whether the information is "reasonably accessible" per amended Rule 26(b), "[i]t may be important for the parties to discuss [their] systems, and accordingly important for counsel to become familiar with those systems . . . . [and] individuals with special knowledge of a party's computer systems" before the conference. Committee Note to Rule 26(f).

<sup>10</sup> "The volume and dynamic nature of [ESI] may complicate preservation obligations. The ordinary operation of computers involves both the automatic creation and deletion or overwriting of certain information. Failure to address preservation issues early in the litigation increases uncertainty and raises the risk of disputes." Committee Note to Rule 26(f).

<sup>11</sup> The Committee did not provide strict guidance for determining accessibility. The following analysis might provide a helpful analogue to estimate the difference:

affirmative burden; parties may no longer simply omit information they consider burdensome from their disclosure, as the Committee observed in prior practice. Instead, parties must *identify* what they are not searching or producing and describe, to the extent possible, the burdens and costs associated with the process. Still, a party is not obligated to *produce* what it self-designates as “not reasonably accessible” until instructed by court order.<sup>12</sup>

“Not reasonably accessible” ESI is not placed wholly outside the bounds of discovery obligations, however. A party still may suffer the burden of production of such information if the requesting party can demonstrate good cause, i.e., that “the need for discovery outweighs the burdens and costs of locating, retrieving and producing the information” in addition to screening for privilege and relevance.<sup>13</sup> Also relevant to the good cause determination is a requesting party’s willingness to share in those costs. Interestingly, the Committee chose to limit what constitutes “good cause” primarily by the same fairness and proportionality factors that restrict the scope of discovery generally in each particular case, now appearing at amended Rule 26(b)(2)(C). Note that Rule 45(d) mirrors this inquiry as applied to subpoena practice, and the Committee emphasized special sensitivity to avoiding the undue burden and interference upon non-parties called to respond to a subpoena for discoverable information.

Second, in order to ameliorate the acute risks of inadvertent disclosure of privileged information in e-discovery (and to help parties avoid the massive costs and delay in prevention), amended Rule 26(b)(5)(B) creates an explicit right of a party to reclaim (or direct the receiving party to sequester or destroy) inadvertent disclosures after the fact. The rule establishes only a *procedure* for damage control, leaving the issue of privilege or work product protection, as well as waiver, to be litigated (according to the law of the controlling jurisdiction) after the parties seal the breach. Again, Rule 45 replicates this provision as applied to subpoena practice.<sup>14</sup>

In addition to aiding the producing party’s recovery of inadvertently disclosed information, the amended Rule concomitantly establishes a responsibility upon the recipient. Once notified of the privilege claim, the receiving party has a duty to preserve that information from further disclosure and take reasonable steps to retrieve the information if already disclosed to third parties. However, the rule also gives the receiving party the option of submitting the material to the court under seal.

---

[A]ccessible data is information that is stored in a format that does not require further manipulation. . . . Inaccessible data includes [information] that need[s] to be recovered or restored from damaged computers or servers, . . . erased or overwritten [files], backup tapes, and other backup media.

Jennifer A. Mahar and Bryant M. Farland, Introduction to Electronic Discovery, in DISCOVERY DESKBOOK FOR CONSTRUCTION DISPUTES 132–33 (Buckner Hinkle, Jr. et al. eds., 2006).

<sup>12</sup> Rules Report, App. C-44.

<sup>13</sup> Committee Note to Rule 26(b)(2)(B).

<sup>14</sup> Rule 45(d)(2)(B).

The Amendments welcome parties to go further, however, in handling discovery of privileged matter early:

The volume of such data, and the informality that attends use of e-mail and some other types of [ESI], may make privilege determinations more difficult, and privilege review correspondingly more expensive and time consuming. . . . [Moreover], production may be sought of information automatically included in electronic files but not apparent to the creator or to readers. Computer programs may retain draft language, editorial comments, and other deleted matter . . . . [or] [i]nformation describing the history, tracking, or management of an electronic file (sometimes called “metadata”) . . . usually not apparent to the reader viewing a hard copy or screen image.<sup>15</sup>

Parties may minimize these costs while protecting against the risk of waiver by adopting their own arrangements, such as “quick peek” and “clawback” agreements. A quick peek allows the requesting party to have more comprehensive access to requested materials for an initial examination while it designates the documents actually sought for production. This protocol helps the responding party to avoid expense and delay by screening for privilege only those documents identified for complete production out of the larger ESI or traditional document group. The fact that the very documents screened out were previously disclosed to the requesting party, according to the agreement, does not constitute waiver. Clawback agreements are similar; they provide that production without intent to waive privilege does not constitute waiver.<sup>16</sup>

The third change aimed at protecting parties from over-exposure in meeting ESI disclosure requirements is the Rule 37(f) “sanction shield,” which should reduce the anxiety parties have when faced with a disclosure obligation that may include information tucked away in sensitive areas of system processes or destroyed to keep those processes working effectively.

Traditional sources of information are “static”; they are not generally destroyed absent an “affirmative, conscious effort” by a human being. In contrast, computer information, the Committee recognized, is dynamic. While large organizations can fill off-site warehouses with their paper histories, the essential functions of almost any computer program inherently destroy (or overwrite) some kinds of information in order to keep operating. For example, “merely turning a computer on or off can change the information it stores,” metadata can change to

---

<sup>15</sup> Committee Note to Rule 26(f) (describing scheduling conference amendments).

<sup>16</sup> An article by the Fulton County Daily Report seems to suggest that Rule 26(b)(5)(B) is itself a “clawback” provision. Leigh Jones, Zero Hour on e-Discovery Change Looms, FULTON COUNTY DAILY REPORT, August 25, 2006. However, the amended Rules appear only to encourage agreement between the parties in forming their own arrangement. Rule 26(b)(5)(B) is only a procedure for protecting the ESI from further use or third-party disclosure after the responding party has timely asserted the claim of privilege.

reflect the most recent document editor, and some programs automatically recycle backup tapes that protect against short-term, system-wide disasters or dump unused files.<sup>17</sup>

Rule 37(f) recognizes that inevitably some ESI will include data vulnerable to “routine deletion or overwriting as part of the good faith operation of information systems.” The Committee acknowledged that these systems should not suffer costly (or prohibitively expensive) disruption with each round of discovery.<sup>18</sup> As such, Rule 37(f) shields from sanction, under the discovery rules, litigants who lose discoverable information on account of these routine processes, absent exceptional circumstances.

Of the amendments submitted for public review, Rule 37(f) elicited extensive commentary. Just how far the “limited” shield extends is apt to remain a mystery until the courts have their say. However, the weight of the Committee’s response and insight suggests that human-oriented document retention policies would not qualify as the kind of inevitable “routine operations” that enjoy the good faith culpability standard under the rules, unless such “policies” are written in binary code, i.e., the policy is expressed in the system’s programming or design itself, and does not involve an operator’s decision or input. Indeed, Committee reports have described the Rule’s coverage as those “automatic” and “essential” alterations often occurring “without the operator’s specific direction or awareness.”<sup>19</sup>

---

<sup>17</sup> Rules Report, p. 32 & App. C-83.

<sup>18</sup> “Many steps essential to computer operation may alter or destroy information, for reasons that have nothing to do with how that information might relate to litigation. . . . [T]he ordinary operation of computer systems creates a risk that a party may lose potentially discoverable information without culpable conduct on its part.” Committee Note to Rule 37(f). Even when litigation is anticipated, the Committee noted,

it can be very difficult to interrupt or suspend the routine operation of computer systems to isolate and preserve discrete parts of the information they overwrite, delete or update *on an ongoing basis*, without creating problems for the larger system. Routine cessation or suspension . . . is also undesirable; the result would be even greater accumulation of duplicative and irrelevant data that must be reviewed, making discovery more expensive and time-consuming.

Rules Report, 32–33.

<sup>19</sup> The Rule does not unequivocally limit itself to such processes. Objections to the Rule included the concern that a party could set up a *policy* “that systematically destroys relevant information harmful to its interests.” Instead of suggesting the Rule does not apply to “policies,” the Committee responded that the good faith standard was the compromise to that objection.

Still, under the good faith standard, most “policies” would not likely qualify for protection in the event of such a loss. In that less often case where an operator *is* involved with the routine deletion or overwriting process, setting the time frame of an e-mail purge, e.g., the good-faith standard will scrutinize the party’s ability to impose a litigation hold in time to prevent the loss, i.e., directing the operator to amend or halt the variable purging schedule.

Contrast one of the heartland examples of “routine operation”: the periodic recycling of backup “disaster” tapes. From the filing of the complaint to the deadline for an answer, a system’s two-week backup tapes may have been wiped clean and used again, by necessity and design, three or four times (and hundreds of times since the cause of action arose). Isolating information relevant to the claim in time would be near impossible, if not inordinately expensive (and this is before a discovery request has even been served).

This does not mean, however, that all design function overwriting is protected by the Rule. Although the Committee made clear that the good-faith standard does *not* create or affect preservation obligations, good faith *may* require, in some circumstances, intervention into the routine processes. Whether this is the case will likely include a cost-benefit analysis not uncommon to many discovery questions: What is (or was) the risk of injury to the system from intervention, the likelihood the requested information will be (or would have been) found, and the burden of isolating the information or imposing a litigation hold?<sup>20</sup> Anticipation of litigation or the pre-existence of a preservation obligation are also factors in assessing whether good faith required efforts to stop the process from overwriting or destroying information. Of course, a party may not exploit the fact of routine deletion, or the ability to design such a system, for the purpose of destroying discoverable information.

The shield does not deprive the court of the power to equitably respond to an inadvertent loss. The court may still alter the discovery relationship by allowing the aggrieved party more witnesses to depose or more interrogatories. Ethical or statutory sanctions existing outside the discovery context remain unaffected, as well.

### **CONCLUSION**

The 2006 Amendments update the rules of discovery to address the dynamic nature of ESI disclosure while stressing the importance of early conciliation of e-discovery disputes. Technological evolution is not likely to render these changes obsolete because they target the perennial costs and risks of electronic information storage and production: volume, form, and routine. As the capacity of storage devices increases, the Rules will provide parties with new avenues to ameliorate the cost of preventing and redressing inadvertent disclosures of privileged material. As ESI continues to take diverse forms for different purposes, the Rules will help balance cost with accessibility to identify the ultimate form of production. Finally, as systems continue to create and destroy data in unique ways, the shield against sanctions for essential routine deletions will reduce the anxiety and danger of interrupting sensitive operations.

---

<sup>20</sup> Rules Report, 84–85. Note, however, that there is no necessary relationship between what is “not reasonably accessible” per Rule 26(b)(2) and what is a good faith routine operation per Rule 37(f). In certain cases good faith may require preservation of information found on sources a party identifies as not reasonably accessible.

n n n

*We hope you find the foregoing information useful. Please do not hesitate to contact us at the numbers below should you have any questions.*

Thomas M. Byrne	404.853.8026	<a href="mailto:tom.byrne@sablaw.com">tom.byrne@sablaw.com</a>
Jennifer W. Fletcher	404.853.8145	<a href="mailto:jennifer.fletcher@sablaw.com">jennifer.fletcher@sablaw.com</a>
Ann G. Fort	404.853.8493	<a href="mailto:ann.fort@sablaw.com">ann.fort@sablaw.com</a>
J. Dean Marshall, Jr.	404.853.8153	<a href="mailto:dean.marshall@sablaw.com">dean.marshall@sablaw.com</a>
Brian L. Rubin	202.383.0124	<a href="mailto:brian.rubin@sablaw.com">brian.rubin@sablaw.com</a>
William R. Wildman	404.853.8406	<a href="mailto:bill.wildman@sablaw.com">bill.wildman@sablaw.com</a>
Andrew S. Hiller	404.853.8148	<a href="mailto:andrew.hiller@sablaw.com">andrew.hiller@sablaw.com</a>