04-CV- 225

MAYER BROWN ROWE & MAW

Mayer, Brown, Rowe & Maw LLP
190 South La Salle Street
Chicago, Illinois 60603-3441

Main Tel (312) 782-0600
Main Fax (312) 701-7711
www.mayerbrownrowe.com

Ashish S. Prasad
Direct Tel (312) 701-8438
Direct Fax (312) 706-8670
aprasad@mayerbrownrowe.com

February 14, 2005

BY OVERNIGHT DELIVERY AND EMAIL

Peter G. McCabe, Secretary
Committee on Rules of Practice and Procedure
Administrative Office of the U.S. Courts
One Columbus Circle NE
Washington, DC 20544
Email: Peter_McCabe@ao.uscourts.gov

Re: Proposed Amendments to the Federal Rules of Civil Procedure Governing Electronic Discovery

Dear Mr. McCabe:

I appreciate the opportunity to comment on the proposed amendments to the Federal Rules of Civil Procedure regarding the discovery of electronically stored information. This letter contains my comments, which I submit to the Civil Rules Advisory Committee for their review.

I base these comments on my experience representing corporate clients in civil litigation and as head of the Electronic Discovery and Records Management Group of Mayer, Brown, Rowe & Maw LLP. In the last several years my practice has focused largely on the challenges and opportunities presented by the increasing prominence of electronically stored information in civil discovery. I have served as electronic discovery counsel in product liability litigation for different clients, and have participated in the electronic discovery efforts of several organizations, including the Sedona Conference, Lawyers for Civil Justice, and DRI. Although my comments are based on my experience with clients and others deeply involved in electronic discovery, I must emphasize that these comments reflect my personal views, and not the views of any particular client or entity.

Initially, I must applaud the Committee for their efforts in drafting these proposed rules. The proposed Rules address a number of pressing electronic discovery issues in a thoughtful and balanced manner. Importantly, the proposed Rules by and large describe electronically stored information with sufficient generality to allow the Rules to adapt to new and changing technology. Each of the proposed rule changes has merit, and I strongly believe that bench, bar, and, most importantly, litigants will benefit from their adoption.

Nonetheless, there are a number of places in the proposed amendments where the Rule or Note could be clarified to better serve the objectives of the Committee and the interests of litigants. Further, the Committee has specifically requested comments on a number of issues addressed by

the proposed amendments. This letter responds to the Committee's request for comments, including comments on some of the issues expressly identified by the Committee.

Rule 26(b)(2)

The proposed changes to Rule 26(b)(2) provided a much-needed general framework addressing the discoverability of electronically stored information that is not reasonably accessible. I would suggest one balancing revision to the text of the Rule. It should clarify that the burden of establishing "good cause" falls on the requesting party, given that the Rule already provides that the burden of showing that the information is not reasonably accessible falls on the responding party. In other words, the rule itself should make clear that the burden of overcoming the presumptive limitation should shift to the requesting party once the responding party meets its burden of showing its applicability.

In the proposed Committee Note discussing the "good-cause analysis" under Rule 26(b)(2), the *Manual for Complex Litigation* (4th) § 11.446 is quoted for the proposition that the balancing factors in existing Rule 26(b)(2)(i)-(iii) should be applied so as to discourage unduly burdensome or speculative discovery or to defray the cost of more expensive forms of production. The concepts expressed in this passage are sound, but by citing them here, the Note could be read to imply that such considerations are relevant only to an analysis of "good cause." Of course, these concerns should animate a court's management of discovery of all types of information, not just inaccessible electronically stored information. The Note should clarify this point.

The Committee has requested comment on whether further explanation of the term "reasonably accessible" in the Note would be helpful. I believe it is imperative that the Note be revised to provide clearer, though not necessarily more detailed, explanation. The text of the Rule wisely avoids any attempt to define "reasonably accessible" with particularity, and the Note provides several useful examples of what may constitute information that is not reasonably accessible, such as "legacy" data or deleted data. The Note explains that whether information is "reasonably accessible" depends "on a variety of circumstances" and that "[o]ne referent would be whether the party itself routinely accesses or uses the information." (Proposed Amendments p. 12.) This statement may engender a misunderstanding of "reasonably accessible" in this context. In regard to discovery, "reasonably accessible" should mean "reasonably accessible for discovery in litigation" and *not* "reasonably accessible in the course of business operations." While these two meanings often coincide, the Note should make clear to lawyers and judges that they are distinct concepts.

This distinction exists because many types of electronically stored information are "routinely accessed" as "active data," yet would require an unreasonable and burdensome amount of time and expense in order to be identified, preserved, collected, reviewed and produced in litigation. Thus, even though the responding party may "routinely access" the information in the course of business, the information may *not* be "reasonably accessible" for litigation purposes to *either* party to the litigation. In such a case, the burden and expense of making the information usable by *either* party to the litigation renders it not "reasonably accessible."

This situation is particularly problematic when dynamic databases are involved. For example, a business's proprietary database may contain many categories of information, but only certain categories may be searchable, because the business created the database to perform specific functions. It may be very difficult to identify, collect, review and produce data if a document request seeks information based on categories for which the database was not designed to search. Standard reports generated through the user interface may be "routinely accessed," but, in this example, the underlying data would not be "reasonably accessible" in litigation with the meaning of Rule 26(b)(2).

Of course, the converse is also true: certain information may not be routinely accessed in the course of business, but may nonetheless be "reasonably accessible." A possible example of this is the email archives stored on optical disk described in *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309, 320 (S.D. N.Y. 2003). Information from such discs is "reasonably accessible," despite rarely being accessed, because the information can be searched for and produced to the plaintiff "cheaply and quickly." *Id.* In short, the touchstone of "reasonable accessibility" should be the time and expense attendant to producing the electronically stored information, if relevant, in the litigation.

Rules 26(b)(5) and 26(f)(4)

The proposed amendments to Rule 26(b)(5) and Rule 26(f)(4) very soundly steer clear of advocating any type of agreement regarding the inadvertent production of privileged documents or information. The neutrality of the Rule would be strengthened, however, if the Note emphasized that a party's failure to enter into a agreement regarding inadvertent production should have no effect on whether an inadvertent production of a privileged document constitutes a waiver of the privilege. This is an area of particular sensitivity for many litigants, and any amendments to the Rules should not further complicate the process of navigating the maze of rules governing waiver of privilege.

Rule 33

As it has long been the practice of litigants to respond to interrogatories by producing responsive documents rather than answering the interrogatories, it is sensible to clarify Rule 33 by making express the fact that this practice is proper for electronically stored information. As currently drafted, however, the Note to the proposed amendment may not provide the clarity hoped for by the Committee. By emphasizing that Rule 33 may "require . . . technical support" or "access to the pertinent computer system," the Note appears to suggest that allowing the requesting party direct access to the responding party's computer system may be routinely required, rather than continuing the practice of producing copies of the information to the requesting party. Direct access to a responding party's computer systems is often highly disruptive to the responding party, as it can compromise data integrity, system security, personnel privacy rights, and confidential or privileged information. The Note to the Rule should make absolutely clear that it does not mandate direct access as the alternative to answering an interrogatory, but that

production of copies of the electronically stored information, consistent with the provisions of Rule 34 governing form of production, is sufficient.

Rule 34(b)

The Committee should be commended for recognizing the importance of form of production in electronic discovery. The default rule for form of production in rule 34(b)(ii), however, is deeply flawed. The analogy to the alternative forms of production for hard-copy documents is an imprecise one and ultimately may confuse litigants and impair electronic discovery. Neither of the forms of production permitted for electronically stored information—"the form in which it is ordinarily maintained" or "an electronically searchable form"—lends itself to general application or efficient discovery and is not consistent with best practices I have observed.

First, "the form in which it is ordinarily maintained" has clear meaning for many types of electronically stored information, such as word processing files being produced in native format, but not for other types of electronically stored information, such as databases. For many types of databases, replication would require re-creating not only the individual data elements and tables of the database, but the underlying database environment and computer platform. Such an impractical result is entirely unwarranted.

Second, "an electronically searchable form" can be a meaningful option for some types of electronically stored information, such as electronic data that can be converted to text files, but may be meaningless for other types of data, such as pictures or graphics files, sound files, and other non-text objects which are not electronically searchable under current technology. For example, a graphics file (such as a bitmap) cannot be searched using text-searching tools—even words that appears as part of the graphical image are not represented in the file as text, but merely as a collection of individual colored pixels.

In keeping with the objective of the proposed amendments to provide a general framework that is not dependent on particular technology, the Rule and Note should utilize terminology that can better accommodate the immense variety of forms of electronically stored information that exist and that may be developed. For this reason, I agree with the recommendation in the December 16, 2004 comments of Microsoft Corporation (04-CV-001) that Rule 34(b)(ii) require that the responding party produce electronically stored information in a "reasonably useable format." This approach would require responding parties to act reasonably in choosing a production format, and would encourage requesting parties to be explicit if they have a preference about form of production. Further, the requirement of "reasonably useable format" does not presume that electronic format is necessarily superior to paper format. In many cases, especially those involving small amounts of electronic discovery, paper production may be preferable to both parties.

Rule 37

The Committee has stated that it is particularly interested in comment on whether the standard that makes a party ineligible for a safe harbor should be negligence or a greater level of culpability or fault in failing to prevent the loss of electronically stored information as a result of the routine operation of a computer system. As the Committee recognized in drafting this proposed Rule, the normal operation of virtually any business enterprise requires that data which is no longer needed for a business purpose be overwritten or deleted on a regular basis. Further, businesses are currently subject to stricter compliance requirements, and greater regulatory and public scrutiny, regarding their document retention policies and practices than ever before. There are severe regulatory and criminal penalties attached to the illegal destruction of documents and electronically stored information.

In light of these realities, then, it is unnecessary and counterproductive to subject responding parties to open-ended risk of liability based on a post-hoc judgment of the "reasonableness" of their decisions to allow their computer systems to continue to operate. Instead, I recommend that the "safe harbor" rule protect the *good faith* actions of parties who lose electronically stored information as a result of the routine operation of a computer system.

I recommend the use of a standard of "good faith" rather than the standard proposed in the footnote to the proposed amendment to Rule 37 (Proposed Amendments, pages 32-33), which relies on the concept of "intentional[ ] or reckless[ ]" conduct. Other commentators have observed that a party which recycles backup tapes or utilizes a spam filter does so "intentionally" yet has no intention to delete discoverable information. Accordingly, a reference to "good faith" or "bad faith" will express the same concept without the same possibility of ambiguity.

The Committee has also solicited comments on whether the proposed Rule and Note adequately and accurately describe the kind of automatic computer operations, such as recycling and overwriting, that should be covered by the safe harbor. Although the dialogue on routine deletion of electronically stored information has often focused on backup tapes used for disaster-recovery purposes, there are countless other examples of data being routinely overwritten during the course of normal business operations. Database records are updated, old emails are deleted by email management programs, "spam" email is deleted by automated systems, and so on. Indeed, the mere act of opening a word processing document to view it—let alone revise it—causes data to be overwritten. Thus, routine loss of information occurs in myriad ways on virtually all computer systems. It is unnecessary to attempt to describe them all in the Note, but the Note should make clear that the kinds of routine loss of electronic data that are covered by Rule 37(f) are not limited to the types of features described in the Note, but also include more subtle ways that data can be lost, such as through the overwriting of dynamic database records. For example, a party could act reasonably and in good faith by attempting to preserve a "snapshot" of a dynamic database, even if it does not preserve a "snapshot" of the database every time a single record is updated—a process that would be enormously expensive and virtually useless in any litigation.

It has been a privilege to share these comments with you. I thank the Committee for considering them.

Sincerely,

Ashish Prasad

Ashish S. Prasad