American Petroleum Institute

1220 L Street, Northwest
Washington, DC 20005-4070
Tel 202-682-8248
Fax 202-682-8033
E-mail ng@api.org

Harry M. Ng
General Counsel

04-CV-178

February 15, 2005

Peter G. McCabe, Secretary
Committee on Rules of Practice and Procedure
Judicial Conference of the United States
Thurgood Marshall Federal Judiciary Building
Washington, D.C. 20544

Re: **Proposed E-Discovery Amendments to Federal Rules of Civil Procedure**

Dear Mr. McCabe:

Please accept the attached comments of the American Petroleum Institute in response to the Committee's proposed amendments of the Federal Rules of Civil Procedure governing discovery of electronically stored information.

Please feel free to contact me or Ralph Colleli of my staff (202-682-8252) if you have any questions or need any additional information regarding these comments.

Sincerely,

Harry M Ng

Comments of the American Petroleum Institute
On Proposed Amendments to the Federal Rules of Civil Procedure
Regarding Discovery of Electronically Stored Information

February 15, 2005

The American Petroleum Institute (API) welcomes this opportunity to comment on the proposed amendments to the Federal Rules of Civil Procedure regarding discovery of electronically stored information ("ESI"). API congratulates the Committee on Rules of Practice and Procedure and the Civil Rules Advisory Committee for their thoughtful and timely effort to address a burgeoning problem of concern to API and its member companies.

API is a nationwide, not-for-profit trade association representing over 400 member companies engaged in all aspects of the oil & gas industry, including exploration and production, transportation, refining, distribution and marketing. API represents its members in many regulatory, administrative and litigation matters of concern to the industry before many federal and some state *fora*, including the federal court system.

Many of API's member companies do business on a nationwide or international scale, and many of those companies have facilities in dozens or even hundreds of locations. Virtually all of those facilities (as do the facilities operated by smaller API member companies) have extensive computerized records, using a wide variety of formats and systems, which are often decentralized. Moreover, many of those same companies are or have the potential to be involved in hundreds or thousands of lawsuits at any given time, many of which would be subject to the Federal Rules governing discovery of ESI.

API's members – like many other members of the business community – are concerned that the current rules and case law governing discovery of ESI impose or can impose unnecessarily costly, complex and burdensome requirements for preserving and producing ESI that ultimately results in little or no benefit to the litigants or the court. API and its members are encouraged that the Rules Committee recognizes the need for revisions to the Federal Rules to mitigate the excessive burdens and potential abuse of discovery procedures for ESI and to reduce the possibility of unwarranted sanctions against parties acting in good faith.

API understands that several of its member companies have testified at the regional hearings on the proposal and have submitted written comments to the Rules Committee. In light of that fact, API itself will not attempt to comment on all of the proposed revisions. Instead, API will address two of the major, and most important, reforms proposed by the Committee – the "two-tier" approach to discovery of ESI that is (or is not) "reasonably accessible;" and the related "safe harbor" from sanctions for routine deletion of ESI by normal computer operations in the absence of an agreement or court order.

A. API Supports Adoption of a Reasonable "Two-tier" System for ESI

The proposed amendment to Rule 26(b)(2) would clarify that "a party need not provide discovery of electronically stored information that the party identifies as not reasonably accessible." If the requesting party moves for discovery of such information (the second tier), the responding party must show that the information is not reasonably accessible. However, even if that showing is made, the court may still order discovery, provided that the requesting party shows good cause, subject to appropriate terms and conditions.

API believes that this proposal has the potential to reduce the unwarranted costs and burdens required to preserve or disclose ESI that can be preserved and retrieved only by extraordinary means. At the same time, the proposal maintains a party's right to discover such information if the requesting party can show that the ESI is relevant and that the need for it outweighs the burdens of discovery. In addition, this proposed amendment – in conjunction with the proposed "safe harbor" amendment to Rule 37(f) - would help minimize unwarranted disruption of necessary and routine computer operations involving information that is not "reasonably accessible." See Part B, infra.

The Advisory Committee has provided in its proposed Note several non-exclusive examples of ESI that are not "reasonably accessible," including information stored for disaster recovery purposes, "legacy" data from obsolete systems, and deleted data that is recoverable only by extraordinary means. The Committee Note also refers to "metadata" in a way that implies such information is generally not "reasonably accessible."[1] The proposed Note also draws a helpful contrast between those examples and "active" databases that are regularly used or accessed.

The Committee has asked for comments on whether the term "reasonably accessible" needs further clarification. API believes that the term as used in the proposed revision to Rule 26(b) is adequate and consistent with other rules that rely generally on an element of reasonableness. The term also provides important flexibility for dealing with the widely varied and constantly evolving systems for storing ESI. However, API believes that it would be helpful for the Note to Rule 26(b) to link the concept of "reasonably accessible" ESI with "active" ESI that is stored in anticipation of future use and in a manner that provides for efficient retrieval, and to link the concept of ESI that is not "reasonably accessible" to data that cannot be efficiently retrieved, including information stored on backup tapes for potential emergencies, and information stored as a mere artifact of a computer system with no anticipation of future use.. In addition, API suggests that the Note more clearly emphasize that "metadata" normally is not considered "reasonably accessible."

API also urges that the Note confirm that the reference in proposed Rule 26(b)(2) to "identification" of ESI that is not "reasonably accessible" does not create a new obligation to identify specific information or documents. The proposed Note (at 13) strongly implies that the proposed Rule would only require the responding party to identify general categories or "types" of information (e.g., "disaster-recovery") or the nature of difficulty that retrieval would entail (e.g., recovery of legacy data on obsolete systems). However, API believes it would be helpful

[1] The Committee Note (at 14) cites the *Manual for Complex Litigation* (4th ed.), §11.446, discussion of metadata as an example of information that should be discoverable only upon a showing of need or shared expenses.

for the final Note to clarify that the Rule only requires "identification" of general categories of inaccessible information (e.g., "backup tapes") and that the obligation to "identify" does not require specificity comparable to a privilege log.[2] Such a clarification would eliminate potential ambiguity in the Rule and help avoid contentious and wasteful motions practice.

Finally, API agrees with other commenters[3] who have recommended that either amended Rule 26(b) itself or the Note specify that the parties share the costs of preserving or producing ESI that is not "reasonably accessible" whenever a court compels discovery of such information. Such an allocation of costs would be within the authority of the court and generally would be appropriate in this situation where, by definition, preservation and retrieval of ESI will be difficult and unreasonably expensive. It would also be consistent with the practice in states like California, Texas and New York where cost sharing has been recognized as an effective deterrent to excessive ESI discovery requests.[4]

B. API Supports a Reasonable "Safe Harbor"

The proposed Rule 37(f) would create a narrow "safe harbor" from sanctions for failing to provide discovery of ESI that has been lost due to the routine operation of computer systems (e.g., automatic recycling, overwriting, alteration) unless the responding party violated an order requiring preservation of such information, or the party failed to take reasonable steps to preserve the ESI after it knew or should have known that the information was discoverable. As indicated in the Committee Report (at 18), this proposed "safe harbor" dovetails with the proposed two-tier system of Rule 26(b)(2) since ESI that is not "reasonably accessible" under the latter Rule would not normally be considered discoverable under proposed Rule 37(f) absent a court order requiring discovery for good cause.

API strongly agrees with other commenters that a reasonable "safe harbor" would be an appropriate way to resolve the conflict between the necessity to continue operating computer systems that routinely overwrite, alter or delete data and the risk that such routine operations might result in onerous sanctions for spoliation. The Committee Report expressly recognizes that conflict and acknowledges that suspending automated operations to avoid the risk of sanctions could be prohibitively expensive and disruptive and generally would not be warranted since large quantities of relevant ESI normally are reasonably accessible and can be effectively preserved through a "litigation hold." See Committee Report at 17-18. API agrees with the Committee's observations.

API also agrees with various other commenters that the "safe harbor" should be revised to allow sanctions only for the loss of information specified in a court order. According to the proposed Note, the "safe harbor" might not apply in some cases where ESI is lost even when the

---

[2] In fact, if the obligation to identify information that is not reasonably accessible were construed to require specificity comparable to a privilege log, the obligation would vastly increase the burden of electronic discovery and thus be counterproductive.

[4] At a minimum, the Rule or the Note should create a presumption that the requesting party pay for all or a substantial portion of the costs for discovery of ESI that is not "reasonably accessible" unless the requesting party makes a strong showing that the "inaccessible" ESI is both relevant and necessary (e.g., that "reasonably accessible" alternative information is not available).

information is not "reasonably accessible," and even when there is no applicable court order, if the responding party somehow "knew or should have known" that the information was discoverable. See proposed Note at 35. The proposed Note gives little guidance as to how a party would know that "not reasonably accessible" ESI is discoverable absent a court order, given that proposed Rule 26(b)(2) presumes such information is not discoverable without a "good cause" order.

This potential exception would introduce significant uncertainty as to when the safe harbor applies and could effectively nullify the provision. An effective "safe harbor" will achieve its purpose of allowing routine and necessary computer operations to proceed normally only when its applicability is predictable and the producing party can rely on its protection with certainty. An appropriate way to provide that certainty and predictability is to revise the proposed language to authorize sanctions for loss of data through routine computer operations only when the producing party violates a court order requiring preservation of specified information.

Finally, in response to the Advisory Committee's request for comments on the degree of culpability that would void the "safe harbor" and justify sanctions, API agrees with the suggestion in footnote ** in the Committee's Report that a high degree of culpability is warranted in light of the "uncertainties created by the dynamic nature of computer systems and the information they generate and store." Moreover, a high standard is appropriate in light of the narrowness of the "safe harbor;" the need to create an effective barrier to excessive or abusive discovery and sanctions practices; the great difficulty and cost of tracking and preserving enormous volumes of ESI that in many instances would be of little or no use in the litigation; and the availability of reasonable methods (e.g., "litigation holds" on reasonably accessible ESI in active files) to preserve relevant ESI. Therefore, API agrees with the suggestion in footnote ** that sanctions should be applied only in cases of "intentional or reckless" behavior by the responding party.

In light of the above comments, one preferable alternative to the versions of the "safe harbor" language in the text of proposed Rule 37(f) would be:

"A court may not impose sanctions under these rules on a party for failing to provide electronically stored information deleted or lost as a result of the routine operation of the party's electronic information system unless the party intentionally or recklessly violated an order issued in the action requiring preservation of specified information."

Conclusion

API hopes that these comments will aid the Committee in its important task of amending the Federal Rules to address the real and increasingly troublesome problems posed by discovery of ESI under current procedures. API encourages the Committee to adopt reasonable and appropriate amendments at the earliest opportunity.