LOS ANGELES
Daily Journal

WEDNESDAY,
NOVEMBER 8, 2006
Vol. 119. No. 215

SINCE 1888

OFFICIAL NEWSPAPER OF THE LOS ANGELES SUPERIOR COURT AND UNITED STATES SOUTHERN DISTRICT COURT

Focus

A Safe Harbor in E-Discovery

By Joseph S. Wu

There has been much public criticism about how little the new Rule 37(f) will protect litigants from sanctions for destroying computer-based information after the new Federal Rules of Civil Procedure go into effect on Dec. 1. In fact, many references today to the new rules are filled with sarcastic undertones. Commentators criticize Rule 37(f) as more like a shallow harbor filled with reefs, implying that the rule provides practically no protection from the heavy elements facing litigants in the growing world of electronic data discovery.

But is it really too early to bury Rule 37(f)? Or is the rule so watered-down that its real effect will be negligible?

Rule 37(f) does in fact eliminate the greatest risk to companies with substantial volumes of electronically stored information (ESI). But litigants will need to shelter themselves from the real risk of sanctions relating to ESI management and discovery under the new rules.

The Marathon Debate

The advisory committee took on this issue after heavy lobbying by businesses and agencies who deal routinely with vast amounts of ESI. The committee reported on how these parties begged for a safe harbor against evidence spoliation charges due to inadvertent loss of ESI. Altering or losing ESI is an every day phenomenon — a business necessity — that is automated and embedded within computer systems. And with the increasing amount of harsh discovery sanctions issued by courts, businesses and agencies alike contend that it is too difficult to meet preservation obligations short of a full freeze on the use of business computers systems — an impossible scenario.

The advisory committee was sympathetic. It noted: "It would be good to draft a rule, if it can be done, that offers protection to a party who behaves reasonably," and "reasonable steps do not always preserve everything. Things slip through. That's the point of the safe harbor." [Minutes, Civil Rules Advisory Committee, April 15-16, 2004].

But as the committee struggled through the form and scope of the proposed safe harbor, the debate boiled down to two key questions. First, if the safe harbor proposal just reflects existing case law, is it really needed? And if the safe harbor proposal moves beyond existing case law, is it really appropriate? The final Rule 37(f) language, adopted by the U.S. Supreme Court without comment, states:

"Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronic stored information lost as a result of the routine, good-faith operation of an electronic information system."

In these brief words, the committee expressed its intent to reaffirm existing case law — without going further — so courts may continue to be free to exercise their discretion to fashion fact-specific remedies where appropriate.

Meeting the Drafters' Goals

Rule 37(f) offers almost complete immunity (absent exceptional circumstances) from sanctions that result from the loss of discoverable ESI from routine good-faith destruction. The drafters had to carefully define the scope of this immunity to minimize potential abuse. Indeed, for courts to accept such a "thou shall not" directive from the drafters, there had to be some form of an escape valve to allow judges room to exercise sound discretion in exceptional circumstances.

The wisdom of an "exceptional circumstance" exception is shown by District Court Judge Shira A. Scheindlin's survey of sanctions awarded in federal courts since January 2000 (available at http:www.mttlr.org/voleleven/scheindlin.pdf). After surveying 66 opinions granting sanctions in the discovery context, Scheindlin concluded that "the courts seems to be 'getting it right'" in that sanctions seem always accompanied by some additional level of consideration — other than the mere following of a party's routine records management practices. These other considerations include the extent of the prejudice to the requesting party and the degree of willfulness or bad faith by the producing party. In view of the results from Scheindlin's study, the drafters had to overcome the first question of whether a Rule 37(f) was really necessary.

The drafters concluded that it was. First, the committee felt that, on balance, it was important to adopt Rule 37(f) to promote attention and discussion of this very difficult issue. Rule 37(f) works in conjunction with Rule 26(a)(1) (the new initial disclosure requirements) and Rule 26(f) (the early meeting of counsel obligations) to force litigants to address the ESI issue, including the scope of ESI preservation, up front. If anything, early attention will minimize any real consequences of prejudice a party

may arguably suffer resulting from the loss of ESI during routine destruction. By including Rule 37(f) under these new rules and specifically requiring good faith from all parties — including the implementation specific acts to halt the automatic routine destruction of potentially discoverable ESI (litigation holds), Rule 37(f) gives teeth to other vital portions of the new rules that emphasize ESI preservation (Rules 26(a)(1)(B) and 26(f)).

Second, the committee wanted to address litigants' fears that they may be sanctioned for allowing discoverable ESI to be lost through routine operation of their computer information systems — especially something out of the litigants' reasonable control. The committee recognized that regardless of a company's size, all computer systems alter and delete information and, as such, ordinary computer operations themselves create the reality that potentially discoverable ESI would be lost with no culpable conduct by the parties. And, on balance, in view of significant public comment for a safe harbor provision under the new rules, for the committee not to include the proposed Rule 37(f) under these new rules may have had greater unintended consequences. By including 37(f) with the new rules, the drafters provided litigants an expressed assurance that they will not be faulted, absent exceptional circumstances, for losing discoverable ESI under routine operations.

Finally, it would be erroneous to view Rule 37(f) as requiring sanctions simply because an immunity under Rule 37(f) may not otherwise be available. For example, just because a party may not have acted immediately to halt the routine destruction of ESI does not mandate automatic sanctions under Rule 37. Conversely, just because potentially discoverable ESI may be lost by an intervening affirmative act by a rogue employee does not always require sanctions from the court.

As Scheindlin explained to a group of in-house counsel in San Diego two weeks ago, the factors that courts consider before issuing sanctions include the level of prejudice suffered by the requesting party in view of the lost ESI and the culpable state of mind of the producing party who lost the ESI. Depending on the interplay between these factors, sanctions are not always mandatory in situations where discoverable ESI are lost.

And even where appropriate, courts have demonstrated appropriate restrain in exacting sanctions to meet the severity of the prejudice upon or misdeed by the affected parties. Measured sanctions range from monetary fines, to evidence preclusion, to striking claims and defenses, to shifting relative burdens of proof, to adverse inference instructions, and ultimately default judgment against the party that lost the ESI.

Even when circumstances take a party outside the Rule 37(f) immunity, sanctions are never automatic, and, absent a greater showing of prejudice and/or culpability, parties can still find protection even outside Rule 37(f).

Making the Harbor Safe

While it may be difficult to predict how Rule 37(f) will be applied after Dec. 1, here are two key perspectives for litigants to keep in mind as everyone seeks to find their own shelter under Rule 37(f).

First, Rule 37(f) is meant only to protect ESI lost as a result of the ordinary operation of a computer system. These are systems designed to meet a party's technical and business needs, which automatically alter and/or overwrite information without any specific direction or interference by (or even the specific awareness of) the operator. An act taken to interfere with such routines or any ESI destruction motivated by nontechnical or business needs may be outside the protection of Rule 37(f).

Second, the added requirement of good faith under Rule 37(f) is a reminder to all litigants to pause and think about ESI retention before proceeding with routine records destruction. To take affirmative action to alter or delete ESI that is not subject to routine destruction will often be viewed as lacking in good faith. Similarly, to do nothing and allow discoverable ESI to be subject to routine destruction when the data should be preserved can be viewed to be lacking in good faith.

The committee notes warned that a party "may not exploit the routine operations 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." On the other hand, taking affirmative action to halt the routine destruction of discoverable ESI (such as a litigation hold) shows of good faith. As the committee notes explained, good faith often will involve an intervening act by a party to modify or suspend certain features of its routine deletion operation to prevent the loss of ESI that is subject to a preservation obligation.

Being Thankful

To understand the great lengths the drafters have gone through to arrive at the proposed Rule 37(f) is to appreciate the protection Rule 37(f) offers companies with substantial electronically stored information. Now litigants have the assurance that they will most likely not be faulted for their routine, good faith destruction of ESI — at least prior to the legal trigger of a preservation duty. Therefore, perhaps the most significant Rule 37(f) take-away is the importance of having an effective records management system in place to automatically manage and monitor all company ESI (and paper records) and, when ESI is no longer required, to have them destroyed promptly consistent with company policy.

As one in-house counsel noted several months ago, corporations should have an absolute right to destroy company records — subject only to limited legal preservation requirements. Come December, at least we will have Rule 37(f) to help litigants sleep a little better even as their company ESI continue to be altered and destroyed on their business computer systems every second of the day.

Joseph S. Wu is a partner at the San Diego office of Sheppard Mullin Richter & Hampton and a member of its business trials and intellectual property practice groups. He is chairman of the firm's national e-discovery team.