"Good Faith" Safe Harbor of FRCP 37(f) to Prevent Drowning in *Zubulake*?

by Mia Mazza and Ashley Sternberg

You likely have heard that a series of amendments to the Federal Rules of Civil Procedure addressing the discovery of "electronically stored information" took effect on December 1, 2006. You may not know, however, that among those changes is new Rule 37(f), which protects parties from sanctions (including preclusion of evidence at trial and "adverse inference" jury instructions) where evidence has been spoliated "as a result of the routine, good-faith operation of an electronic information system." Depending on how courts interpret Rule 37(f), it could signal a shift toward focusing upon "good faith" as the relevant legal concept when considering potential sanctions for spoliation. That would be an improvement over the current approach, most prominently set forth in *Zubulake v. UBS Warburg LLC*,[1] as discussed below.

Under federal law, a company is required to preserve all documents and data that it "knows, or reasonably should know, will likely be requested" in pending or reasonably foreseeable litigation matters.[2] This creates a vexing challenge for large companies as the "reasonably should know" standard is often applied close to or during trial, based on what evidence ended up being relevant, from a "20/20 hindsight" perspective. Thus, the federal standard for preservation of evidence seemingly requires psychic ability: at the time the duty to preserve arises, the company may not have received a complaint or preservation letter, yet it nevertheless is expected to identify and safeguard all information that may turn out to be potentially relevant.

Large companies have worked hard to keep up with their duty to preserve evidence, but it has been difficult and costly. The proliferation of email and other electronically stored information (ESI) in corporations has increased exponentially the volume of data potentially relevant to any litigation. Moreover, companies retain and use ESI in a variety of different forms, and in a multiplicity of locations, including servers, backup tapes, desktops, laptops, PDAs, home computers, and so forth, many of which are hard to reach. Nearly all large companies have adopted automatic processes for the deletion or overwriting of data due to the high cost of storage and the legitimate business need to dispose of data that are no longer needed for business or other purposes. Each time a new litigation matter arises or an existing matter expands in scope, the company is expected to initiate or expand a "litigation hold" on any manual or automatic processes that might delete relevant information, while the disposal of all nonrelevant information continues.

The decision of what to include in the scope of a "litigation hold" is thus of great importance. It is a decision made by human beings, usually in-house lawyers. For most large companies, at any given time, there are dozens, if not hundreds, of reasonably foreseeable litigation matters on the horizon, each necessitating its own "litigation hold." Given this web of overlapping decisions made by in-house lawyers on a daily basis, it is difficult to imagine that any company is able to perfectly execute all of its "litigation holds" all of the time. This reality is acknowledged by Sedona Principle No. 5, which provides:

> The obligation to preserve electronic data and documents requires reasonable and good faith efforts to retain information that may be relevant to pending or threatened litigation. However, it is unreasonable to expect parties to take every conceivable step to preserve all potentially relevant data.[3]

But the little-known fact about the preservation duty under federal law before the rules amendments is this: federal case law does not incorporate this "reasonable and good faith efforts" standard. Rather, a company is faced with the continual threat of adverse inference or trial evidence sanctions in any matter for which its "litigation hold" implementation was reasonable but imperfect.

To be blissfully ignorant about these issues is not to know the name Laura Zubulake. Her case against UBS Warburg sent shockwaves throughout the world of civil litigation. *Zubulake*—an otherwise routine individual action for employment discrimination—generated a series of five influential opinions on the duty to preserve electronic evidence. Ms. Zubulake discovered that certain UBS employees had deleted potentially relevant email despite being directed by UBS to preserve those data. UBS had taken steps to preserve backup tapes containing those deleted emails, but it inadvertently misplaced some of the tapes, thereby losing some of the emails. Shortly before trial, Ms. Zubulake successfully argued that the court should impose an adverse inference sanction against UBS; that is, instruct the jury it could assume that the missing emails would have supported Ms. Zubulake's case.[4] The jury later returned a $29 million verdict against UBS.

With *Zubulake*, companies received the disconcerting message that even with a reasonable plan for document preservation in place, there is little room for human error. The fifth and final *Zubulake* opinion held that when a party fails to take "*all necessary steps* to guarantee that relevant data are preserved and produced," any resulting spoliation is potentially sanctionable, even if it was merely negligent.[5] This is troubling in light of the court's holding in *Zubulake IV* that "[o]nce the duty to preserve attaches, *any destruction of documents is, at a minimum, negligent*," unless caused by events outside of the party's control.[6]

Published in Trial Evidence, Volume 15, Number 2, Winter 2007.

Under the *Zubulake* standard, it appears that almost any destruction of potentially relevant evidence amounts to per se negligence, and is therefore potentially sanctionable at trial.[7]

This is true regardless of whether the producing party acted in good faith in the discharge of its duty to preserve. A law review article by Judge Shira Scheindlin—the author of the *Zubulake* opinions—observes that "courts have made clear that a finding of bad faith is not required to impose discovery sanctions."[8]

In today's world of ESI, the standards of *Zubulake* are virtually impossible for most companies, and particularly large companies, to meet every time they are required to execute a "litigation hold." And their opponents know it. As a result, it is now not uncommon for a party to cause a pending litigation matter to degenerate into a collateral proceeding about what information the company is allowed to be spoliated and what kind of "adverse inference" or other sanction is an appropriate punishment for that spoliation. Not surprisingly, large companies are clamoring for some acknowledgment from the courts that "litigation holds" cannot be executed perfectly, but rather are expected to be done reasonably and in good faith.

New Rule 37(f) could provide a platform for that acknowledgment. The new rule, intended to be a "safe harbor" for producing parties, provides:

> **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.[9]

At a minimum, new Rule 37(f) requires greater culpability before sanctions will issue than the apparent *per se* negligence approach of *Zubulake*.[10] Yet while new Rule 37(f) is undoubtedly an improvement over *Zubulake*, will it truly change the paradigm? The answer to that question will depend largely on how courts interpret the phrase "routine, good-faith operation of an electronic information system."

A narrow interpretation of the quoted phrase would find that data have been "lost as a result of the routine, good-faith operation of an electronic information system" only where a computer does something other than what a human told it to do. Requesting parties will take (and have taken) the position that this is what the drafters of new Rule 37(f) had in mind when they crafted the rule. But this interpretation would continue the current legal trend of requiring parties to execute "litigation holds" perfectly, and it would allow for sanctions to be avoided only in the rare instance when the party's perfect "litigation hold" was thwarted by an imperfect machine. This interpretation does not create a "safe harbor" of any meaningful sort.

A broader and better interpretation would find that data have been "lost as a result of the routine, good-faith operation of an electronic information system" under a wider range of scenarios, including scenarios in which a human being, operating in good faith, failed to tell a computer to cease autodeletion or overwriting in the first place. For example, if a company's legal department properly knew when to trigger a "litigation hold," and executed a reasonable hold at the appropriate time and in good faith, but failed to include a particular custodian in the hold, and the custodian later turned out to be relevant to the action, that custodian's documents that were automatically deleted would be "lost as a result of the routine, good-faith operation of an electronic information system."

Only time will tell what courts will make of the new Rule 37(f); it potentially signals a much-needed change in the framework for e-discovery sanctions. For the concept of "good faith" to gain traction as it should, however, vigorous advocacy by producing parties will be needed to ensure that the broader interpretation is what courts adopt in applying Rule 37(f).[11] ■

Endnotes

1. *See* Zubulake v. UBS Warburg LLC (*Zubulake IV*), 220 F.R.D. 212 (S.D.N.Y. 2003); Zubulake v. UBS Warburg LLC (*Zubulake V*), 229 F.R.D. 422 (S.D.N.Y. 2004).
2. *See, e.g.*, MOSAID Techs. Inc. v. Samsung Elecs. Co., 348 F. Supp. 2d 332 (D.N.J. 2004).
3. The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production 48 (Jonathan M. Redgrave et al. eds., 2005).
4. *Zubulake V*, 229 F.R.D. at 439–40.
5. *Id*. at 431 (emphasis added).
6. *Zubulake IV*, 220 F.R.D. at 220 (emphasis added).
7. Commentators have noted that *Zubulake* and other recent cases seem to impose a nearly strict liability retention standard. *See, e.g.*, Michael R. Nelson & Mark H. Rosenberg, *A Duty Everlasting: The Perils of Applying Traditional Doctrines of Spoliation to Electronic Discovery*, 12 Rich. J.L. & Tech. 14 (2006).
8. Shira A. Scheindlin & Kanchana Wangkeo, *Electronic Discovery Sanctions in the Twenty-First Century*, 11 Mich. Telecomm. Tech. L. Rev. 71, 80–81 (2004).
9. Judicial Conference of the U.S., Summary of the Report of the Judicial Conference Committee on Rules of Practice and Procedure C-84 (2005) *available at* http://www.uscourts.gov/rules/Reports/ST09-2005.pdf.
10. *See id.* at C-84–85. The original draft of Rule 37(f) contained two alternatives for the minimum culpability required to impose sanctions. One version required the party seeking safe harbor under the rule to demonstrate that it took reasonable steps to preserve the information once it knew that information was discoverable. The other version used a higher culpability threshold, barring sanctions unless the party intentionally or recklessly destroyed the information. After considering public comment, the Advisory Committee adopted the good faith standard as "a culpability standard intermediate between the two [proposed] versions."
11. Producing parties should likewise argue that the carve-out permitting sanctions in "exceptional circumstances" should be used infrequently so as not to let the exception swallow the rule.