

Safe Harbor and Sanctions under Rule 37

By Robert W. Pass and Michael K. Winston

Perhaps no facet of e-discovery has engendered more fear and loathing by those who maintain substantial amounts of electronic information than the duty to preserve (and produce) relevant electronic evidence, and the imposition of sanctions for failing to satisfy that duty. What was a non-issue for many lawyers prior to the advent of e-discovery, spoliation of evidence suddenly became a serious risk to both the client and counsel. In response to ongoing uncertainties about the scope of the duty to preserve and produce electronically stored information (ESI), the new rules of civil procedure attempt to bring a degree of guidance to litigants and the courts. Among these new rules, Rule 37(f) attempts to provide what many have referred to as a “safe harbor” from discovery sanctions. While the ultimate impact of Rule 37(f) will be determined through real-world application, it should not be viewed as a panacea for all potential ESI discovery problems, nor has it overturned the substantial body of case authority that permits sanctions to be imposed pursuant to a court’s inherent authority to deal with conduct of parties.

The ESI Environment

To anyone involved in litigation, it may seem that a veritable cottage industry has arisen in e-discovery sanctions. Litigation in which at least one party has substantial ESI may seem less about winning on the merits and more about avoiding losing on ESI spoliation. Cases indeed can be won and lost on just such issues with sanctions ranging from payment of costs and fees to the entry of an adverse judgment.

These heightened risks are not the

result of a wholesale decline in ethics and good faith among lawyers and businesses in approaching their discovery obligations, but in large part stem from fundamental differences between ESI and paper discovery. These differences begin with the sheer volume and pervasiveness of ESI.

The growth of ESI is unprecedented and epic. The Sedona Conference projected that in 2003 alone, emails sent in the United States in a single day nearly exceeded the number of mail messages handled by the U.S. Postal Service in an entire year. See *The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Production* (July 2005), p. 4. And that number is growing. It has been estimated that 93 percent of all documents (including email) are created in electronic form. More importantly, over five years ago it was estimated that about one-third of all such documents exist *only* in electronic form. There can be little doubt that percentage is higher today.

The Sedona Principles identify characteristics of ESI that make it inherently different from traditional paper documents. They include: the volume and ease of duplication of ESI; ESI’s persistence (a deleted email is not necessarily erased); the ease of changing ESI, and the automatic nature of some changes by computer systems; the existence of metadata, which can give information about the creation, authors, and changes to documents; the potential of ESI to become unreadable by the obsolescence or discarding of operating systems necessary to read it; and the ease of dispersion of ESI to multiple recipients.

In addition, to control the sheer volume of ESI that serves no continu-

ing business need (mainly email), many organizations employ electronic programs that routinely and automatically eliminate ESI under various protocols. An example is the automatic recycling of disaster recovery or backup tapes. Moreover, in organizations where litigation is a frequent, if not daily, event, unless ongoing discriminating decisions are made about what must be preserved, the only way to avoid sanctions may be to save everything. Save everything directives, however, rapidly lead to enormous storage and system costs, along with a host of other undesirable consequences. While no one argues that the law requires an organization to preserve all of its ESI, potential litigants must determine what ESI must be preserved, while understanding that their decision will be judged in hindsight with potentially severe sanctions being the penalty for a poor decision.

Current Sanctions Methodologies

New Rule 37(f) speaks of creating an exemption from sanctions “[a]bsent exceptional circumstances” for “routine, good-faith operation of an electronic information system.” How these new terms will be defined and harmonized with existing case authority is unknown. Historically, the bulk of reported decisions imposing severe sanctions, such as dismissal, adverse inference jury instructions, the treating of important facts as established, or the exclusion of important witnesses, have come in cases in which the loss of ESI was willful, in bad faith, or grossly negligent. Merely negligent loss has generally not been so severely treated. (See “Case Notes” on page 37.)



However, not all courts have required “bad faith” to impose serious sanctions. Indeed, as time passes, courts may grow less tolerant of a party’s “mere negligence” in discharging its e-discovery obligations. One influential court has announced that such a point has already arrived. *See Zubulake*, 229 F.R.D. at 422.

As a practical matter, the greatest risks come from failing to understand what ESI exists on a system, deciding whether the ESI needs to be preserved, knowing how to preserve and retrieve it, and policing organizational compliance with policies and litigation directives. While it is easy to wish for clear and specific universal standards for what must be preserved, it seems unlikely that there will be any such comprehensive standards any time soon and the new Federal Rules offer scant guidance.

Safe Harbor?

The considerable uncertainties regarding what information must be preserved for litigation in cases where ESI was at issue led to pleas for a reliable, predictable safe harbor. Specifically, litigants and their counsel asked for rules that defined as clearly as possible the systems that need not be interrupted before and during litigation and also for clear guidance on what types of ESI did not need to be preserved. Probably, the most frequently cited need was for direction as to whether disaster recovery tape recycling had to be interrupted.

Judicial decisions prior to the new rules rendered the landscape somewhat less uncertain for parties seeking to avoid sanctions, but they did not satisfy the call for concrete rules or principles that give uniform direction. And, while individual influential courts and jurists entered the fray, in the final analysis, these individual cases and other courts may differ in their conclusions and approaches. *See, e.g., Zubulake v. UBS Warburg LLC*, 220

FR.D. 212 (S.D.N.Y. 2003) (“As a general rule, . . . inaccessible backup tapes . . . those typically maintained solely for the purpose of disaster recovery . . . may continue to be recycled . . .”). New Rule 37(f) attempts to fill some of the void created by the rapid advance of technology and the dramatic increase in ESI.

The new rule provides that 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.

Although the rule is arguably the result of intense efforts by a substantial part of the bar to obtain some form of absolute safe harbor, neither the rule nor the Official Committee Notes published with it use or mention that term. Nor do they discuss the rule in terms of specific, named operations of an electronic information system. Most notably, neither the Committee Notes nor the rule specifically mentions disaster recovery tape recycling.

That said, the *Report of the Civil Rules Advisory Committee of the Committee on Rules of Practice and Procedure of the Judicial Conference of the United States* (July 25, 2005), gives “examples” of “routine operation” as including:

- “programs that recycle storage media kept for brief periods against the possibility of a disaster that broadly affects computer operations”
- “automatic overwriting of information that has been ‘deleted’”
- “programs that change metadata . . . to reflect the latest access to particular . . . information”
- “programs that automatically discard information that has not been accessed within a defined period or that exists beyond a defined period without affirmative effort to store it for a longer period”

So, what does the new Rule 37(f) mean for those seeking a practical application of its terms? That will be debated, perhaps at length, as district and circuit courts define and apply its terms to real-life litigation unfolding before them.

Routine Operation of a System

The new rule applies to “routine operation[s]” of a system. The Committee Notes describe this phrase as referring to the way in which computer systems are “generally designed, programmed, and implemented to meet the party’s technical and business needs.” The Advisory Committee Report refers to “programs” and to things that occur “automatically.” It might, therefore, be argued that the rule does not cover loss or destruction that involves human decision-making at the time of its loss, regardless of good faith. Conceivably, this could include disaster tape recycling that involves human decision-making as to when and even which tapes to recycle.

Good Faith

The rule applies only to the “good-faith” operation of electronic information systems. While this may sound fairly simple, the Committee Notes indicate that good faith may require interrupting the routine operation of a computer system to preserve information that would otherwise be routinely eliminated. (“Good faith . . . may involve a party’s intervention to modify or suspend certain features of that routine operation to prevent the loss of information, if that information is subject to a preservation obligation.”)

This facet of the rules is important and easy to overlook: The safe harbor for routine operation of a system may not be satisfied unless the routine operation is affirmatively interrupted. This arises from the fact that the rules do not address or affect the preservation obligation because that is a matter of substantive law. *See* Rules Enabling

Act, 28 U.S.C. § 2072(b) (the Rules “shall not abridge, enlarge or modify any substantive right.”). Thus, the good-faith provision of the rule arguably serves more to articulate a culpability standard (good faith) than to give specific direction as to what routine system operations may continue to operate.

Even less clear is whether the rule’s good-faith qualification speaks to systems that have been designed to function as “document destruction” systems, the focus of which is to eliminate predictably discoverable information rather than to meet the business needs of the organization. Existing case law indicates that an organization cannot rely on a document retention policy adopted for such a purpose. *See Remington v. Lewy Arms Co.*, 836 F.2d 1104 (8th Cir. 1988); *E*Trade Securities LLC v. Deutsche Bank AG*, 230 FR.D. 582 (D. Minn. 2005) (document retention policy cannot be created primarily to eliminate foreseeably discoverable information). Arguably, the strength of such a view has been somewhat undercut by the Supreme Court’s decision in *Arthur Andersen LLP v. United States*, 544 U.S. 696, 704 (2005), in which the Court noted that document retention policies “are created in part to keep certain information from getting into the hands of others,” and that this in and of itself is a normal and permissible business practice. However, the extent, if any, to which *Arthur Andersen* has an impact on “good faith” under Rule 37(f) is far from clear because the decision predates the new rule.

Sanctions “Under These Rules”

Rule 37(f) applies only to sanctions imposed “under these rules,” meaning the Federal Rules of Civil Procedure. The Committee Notes observe that Rule 37(f) “does not affect other sources of authority to impose sanctions or rules of professional responsibility.” Rule 37(f), therefore, would not

EXAMPLES OF SANCTIONS FOR DIFFERENT TYPES OF SPOILIATION

- *Leon v. IDX Systems Corp.*, 464 F.3d 951 (9th Cir. 2006).
Plaintiff ran hard drive “wiping” program on business laptop erasing 2,200 files; dismissal of suit as sanction entered.
- *E*Trade Securities LLC v. Deutsche Bank AG*, 230 F.R.D. 582 (D. Minn. 2005).
Adverse inference instruction granted for erasure of hard drives and failure to preserve email backup tapes used as archive.
- *3M Innovative Properties Co. v. Tomar Electronics*, 2006 WL 2670038 (D. Minn. 2006).
Adverse inference instruction and deeming certain facts established granted as sanction for failure to establish litigation hold, resulting in loss of emails.
- *Z4 Technologies, Inc. v. Microsoft Corp.*, 2006 WL 2401099 (E.D. Tex. 2006).
Failure to produce key email, enhanced damages in patent infringement action granted.
- *Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422 (S.D.N.Y. 2004).
Deletions of emails in violation of litigation hold and own records retention policy; adverse inference instruction granted.
- *Optowave Co. Ltd. v. Nikitin*, 2006 WL 3231422 (M.D. Fla. 2006).
Adverse inference instruction recommended for reformatting of hard drives, erasing files and emails after notice of litigation received; defendant was computer expert.
- *Ridge Chrysler Jeep, LLC v. Daimler Chrysler Services North America LLC*, 2006 WL 2808158 (N.D. Ill. 2006).
Dismissal sanction based on willful withholding and destruction of electronic records.
- *Consolidated Aluminum Corp. v. ALCOA, Inc.*, 2006 WL 2583308 (M.D. La. 2006).
Failure to suspend automated email deletion program for litigation hold; negligent failure to preserve; adverse inference instruction denied.

appear to govern sanctions imposed under a court’s inherent powers, which is a frequent source of sanctions and the only source when there has been no order entered requiring the production or preservation of the information. The safe harbor would also, therefore, appear to be inapplicable to prelitigation loss of ESI because any loss of ESI would not be in violation of a court order.

However, this limitation should not be read to imply a view by the drafters that entirely different standards should apply when proceeding under a court’s inherent powers. Rather, it appears to simply acknowledge an inherent limit on what the rules of civil procedure can reach. While only time will tell, it would seem anomalous for courts to now ignore or deviate markedly from Rule 37(f) when proceeding under their inherent powers.

To do so would create a needless dichotomy of approach that could effectively render Rule 37(f) meaningless because, in theory, courts may always elect to proceed under their inherent powers.

Indeed, even before the adoption of new Rule 37(f), courts did not employ materially different sanctions standards when proceeding under Rule 37(b) or their inherent powers. Prior to Rule 37(f), Rule 37 simply contained no standards upon which courts could draw, and certainly none that focused on ESI. Now that there is a sanctions rule specific to ESI, which contains some standards, and which has the implicit support of both the Supreme Court and Congress, it seems unlikely that courts will use their inherent powers to dispose of sanctions motions in a manner inconsistent with Rule 37(f).

Relation of Rule 37(f) to Inaccessible ESI Under Rule 26(b)(2)

Amended Rule 26(b)(2) provides that “A party need not provide discovery of [ESI] from sources that the party identifies as not reasonably accessible because of undue burden or cost. . . .” This protection may be overcome upon a showing of good cause by the requesting party under the guidelines in Rule 26(b)(2)(C). An obvious question is how the sanctions standards of Rule 37(f) (“good-faith operation . . .”) relate to the right under Rule 26(b)(2) not to provide discovery of [ESI] that is not “reasonably accessible because of undue burden or cost.”

The Committee Notes to Rule 37(f) offer little guidance: “Whether good faith would call for steps to prevent the loss of information on sources that the party believes are not



reasonably accessible under Rule 26(b)(2) depends on the circumstances of each case.” The Notes go on to suggest, however, that “[o]ne factor” in determining good faith is whether the party “reasonably believes that the information on such sources is likely to be discoverable and not available from reasonably accessible sources.”

Rule 26(b)(2) speaks to the obligation to “provide discovery” and does not explicitly address preservation. As the Committee Notes to Rule 26(b)(2)

points out, “a party’s identification of sources of [ESI] as not reasonably accessible does not relieve the party of its common-law or statutory duties to preserve evidence.” As already discussed, the rules steer clear of offering views or standards on preservation obligations.

In theory, therefore, the two rules do not directly interact or inform each other. However, prior to the adoption of new Rule 37(f), case law had already begun to lean toward the view that the

preservation obligation does not generally extend to inaccessible information, particularly disaster recovery backup tapes. *See, e.g., Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212 (S.D.N.Y. 2003).

Safe Harbor by Other Means?

No discussion of a safe harbor would be complete without mention of newly amended Rules 26(f) and 16 (discussed in detail in John Barkett’s article, page 10). The former forces

parties to discuss at their initial conference “any issues relating to preserving discoverable information” The court may enter an order under Rule 16 addressing these issues, particularly if an agreement is reached. While a Rule 26(f) conference is obviously most directly relevant to the preservation issues arising after litigation is filed, it is an opportunity to create a safe harbor by express agreement. While the chances of actually succeeding at such

an agreement in any given case are unpredictable, making a serious effort may be worthwhile. As a producing party, having made a documented, serious effort and proposal about preservation may well be relevant to any later sanctions motions. More importantly, understanding what your opponent claims it and your client should preserve may provide you with valuable ammunition to move for entry of an order establishing case specific

preservation obligations or guidelines. In many cases, taking proactive action with the opposition and the court to establish a safe harbor in the form of reasonable, understood preservation obligations might be the safest harbor of all.

ROBERT W. PASS and MICHAEL K. WINSTON are shareholders at Carlton Fields PA in the Tampa and West Palm Beach, Florida offices.



THE BENEFITS OF MEMBERSHIP

SEEING BOTH SIDES WITH THE SECTION OF LITIGATION

ISSUE CENTERS

Get the latest news and insightful analysis on the issues that change the way we practice law. Covering e-discovery, attorney-client privilege, and the Class Actions Fairness Act, the online Issue Centers make it easy to find the Section's best thinking on major issues.

www.abanet.org/litigation/issuescenter

 SECTION of LITIGATION
AMERICAN BAR ASSOCIATION