

Safe Harbor?

By Mark S. Sidoti,  
Phillip J. Duffy  
and Scott J. Etish

Put yourself in the best position to meet this elusive standard.

# Getting to “Good Faith” under New Rule 37(f)

On December 1, 2006, Congress amended the FEDERAL RULES OF CIVIL PROCEDURE to address the developing area of electronic discovery. Perhaps no rule has been the subject of more discussion and debate than new

RULE 37(f), which provides that “[a]bsent 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.” FED. R. CIV. P. 37(f). While the case law interpreting RULE 37(f) and the other amended rules is only just beginning to develop, there is no serious question, even at this early stage, that federal courts are on the lookout for parties that have failed to exercise “good faith” in carrying out their legal obligations to preserve relevant electronically stored information (ESI).

### Key Requirements for Invoking Rule 37(f) Protection

The text of RULE 37(f) clearly implies a zone of protection for lost or discarded data. However, the few cases addressing

this new rule since its inception have made clear that the circumstances under which its purported protections would apply are actually quite rare, and that parties who liberally misconstrue the meaning of the RULE’s critical “good faith” requirement can be lulled into a false sense of security. In fact, in order to claim the protection of RULE 37(f), a responding party must demonstrate that (1) the information was lost due to the routine operation of an electronic information system, and (2) the routine operation of the information system was performed in “good faith.” Judicial decisions construing RULE 37(f) have held that its apparent protections will not apply to situations where data loss or destruction—however routine or automatic—resulted from a failure to institute procedures properly for the suspension of automatic destruction processes and the preservation of relevant evidence—that



■ Mark S. Sidoti is a director at Gibbons P.C., a New Jersey law firm with offices in Newark, New Jersey, New York City, Philadelphia, Trenton, New Jersey, and Wilmington, Delaware, where he chairs the firm’s Electronic Discovery Task Force. Mr. Sidoti frequently publishes and lectures on E-Discovery and information management best practices. He is membership chair of DRI’s Electronic Discovery Committee. Phillip J. Duffy is counsel at Gibbons P.C., where he is a senior member of the firm’s Electronic Discovery Task Force. Scott J. Etish is an associate at Gibbons. He is a member of the firm’s E-Discovery Task Force.

is, to act in good faith when a preservation obligation has been triggered. *See Doe v. Norwalk Community College*, 2007 WL 2066497 (D. Conn. July 16, 2007); *In Re Krause*, 367 B.R. 740 (Bankr. D. Kan. 2007); *United Medical Supply v. United States*, 77 Fed. Cl. 257, 259 (Fed. Cl. 2007); *Disability Rights Council v. Washington Metro. Transit Auth.*, 242 F.R.D. 139, 146 (D.D.C. 2007); *School-Link Technologies, Inc., v. Applied Resources, Inc.*, 2007 WL 677647 (D. Kan. Feb. 28, 2007); *Peskoff v. Faber*, 2007 WL 2416119 (D.D.C. Aug. 27, 2007).

Comprehending the true scope of protection offered by RULE 37(f) requires an understanding of the Rules Committee's intentions when it used the key words "routine," and "good faith." Here, the Rules Committee Notes are enlightening:

Rule 37(f) applies to information lost due to the routine operation of an information system only if the operation was in good faith. Good faith in the routine operation of an information system 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.... The good faith requirement of Rule 37(f) means that a party is not permitted to exploit the routine operation 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. When a party is under a duty to preserve information because of pending or reasonably anticipated litigation, intervention in the routine operation of an information system is one aspect of what is often called a "litigation hold." Among the factors that bear on a party's good faith in the routine operation of an information system are the steps the party took to comply with a court order in the case or party agreement requiring preservation of specific electronically stored information.

The foregoing commentary highlights the intimate relationship between protection under the Rule and the requirements for implementation of an effective litigation hold. Where litigation is filed, threatened, or seriously contemplated, counsel must take immediate steps to establish

and enforce a litigation hold, even if the documents or ESI would otherwise have been destroyed in the normal course pursuant to the company's document retention policy. *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 218 (S.D.N.Y., Oct. 22, 2003) (*Zubulake IV*). Accordingly, a party cannot reasonably expect to gain protection under RULE 37(f) for destroying ESI when a litigation hold was in place and where a party should have taken affirmative steps to ensure the preservation of documents relevant to litigation.

The recently released *The Sedona Principles, Second Edition* provides additional guidance regarding the factors courts will examine in attempting to determine whether a party acted in "good faith." THE SEDONA PRINCIPLES, SECOND EDITION: *Best Practices, Recommendations & Principles Addressing Electronic Document Discovery* (Sedona Conference Working Group Series 2007) ("*The Sedona Principles*"). Principle 14 states that "[s]anctions, including spoliation findings, should be considered by the court only if it finds that there was a clear duty to preserve, a culpable failure to preserve and produce relevant electronically stored information, and a reasonable probability that the loss of the evidence has materially prejudiced the adverse party." This Principle is consistent with the evolution of decisional law to date. *See, e.g., Zubulake IV*, 220 F.R.D. at 221 ("In order to receive an adverse inference instruction, *Zubulake* must demonstrate not only that UBS destroyed relevant evidence as that term is ordinarily understood, but also that the destroyed evidence would have been favorable to her.").

As is the case with the Rules themselves, the comments to *The Sedona Principles* are instructive and further define the contours of "good faith." In this regard, comment 14d of *The Sedona Principles* explains that "[m]any cases involving spoliation and sanctions examine the 'good faith' of the party that lost the evidence." The comment further provides that "good faith" has both a subjective and objective aspect, and, more importantly, sets forth the critical questions a court will pose in attempting to assess whether a party acted in "good faith":

(a) was there a standard litigation hold process and was it followed?

- (b) did the party adequately communicate litigation hold instructions to employees?
- (c) did the party periodically distribute litigation hold reminders?
- (d) did the party adequately investigate and identify the locations that were reasonably likely to contain unique and relevant electronically stored information?
- (e) has the party been cooperative and forthcoming in RULE 26(f) and 16(b) discussions?
- (f) has the party been reasonable and forthcoming in written discovery responses and depositions?
- (g) did the party take steps to secure relevant, unique electronically stored information that would otherwise be overwritten or deleted by automatic processes?
- (h) did the party take reasonable steps to ascertain whether orphaned or legacy data contain relevant information? and
- (i) was the electronic system designed and implemented solely with the intent of meeting business and technical needs or with the intent of thwarting discovery?

*The Sedona Principles*, cmt. 14d.

As the commentators note, while there "is no talismanic test of 'good faith,'... organizations that can answer most if not all of these questions in the affirmative should be presumed to have acted in good faith absent proof to the contrary." *Id.*

Perhaps most important among the foregoing factors is the duty, imposed on both counsel and parties, to follow up on efforts to preserve data, including effective implementation, communication and monitoring of compliance with litigation hold notices. Of course, this is not a new obligation. In fact, the obligation to oversee and ensure compliance with preservation obligations finds published case law support dating back as far as the 1997 decision in *In re Prudential Ins. Co. of Am. Sales Practices Litig.*, 169 F.R.D. 598 (D.N.J. Jan. 6, 1997), where Prudential was sanctioned \$1 million for its failure to ensure adequately that its key employees received a court ordered preservation notice and took proper steps to comply with the notice. 169 F.R.D. at 615 ([w]hen senior management fails to estab-

lish and distribute a comprehensive document retention policy, it cannot shield itself from responsibility because of [its underlying employees] actions”). The landmark *Prudential* decision was strongly reinforced in the *Zubulake* decisions, in which Judge Scheindlin held:

A party’s discovery obligations do not end with the implementation of a “lit-

Courts grappling with these issues will train their focus far more on actual implementation and execution of information management procedures and litigation holds.

igation hold”—to the contrary, that’s only the beginning. Counsel must oversee compliance with the litigation hold, monitoring the party’s efforts to retain and produce the relevant documents. . . . *In short, it is not sufficient to notify all employees of a litigation hold and expect that the party will then retain and produce all relevant information. Counsel must take affirmative steps to monitor compliance so that all sources of discoverable information are identified and searched.*

*Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422, 432 (S.D.N.Y. July 20, 2004) (“*Zubulake V*”) (court found willful destruction where key employees destroyed e-mail after being repeatedly warned by counsel, and counsel did not interview key employees in litigation or perform key word search of databases while creating and ensuring compliance with litigation hold) (emphasis added).

Similarly echoing RULE 37(f) and its commentary, *Sedona Principle* comment 14e states that “[t]he good-faith destruction of electronically stored documents and information in compliance with a reasonable records management policy should not

be considered sanctionable conduct *absent an organization’s duty to preserve the documents and information.*” *Sedona Principles*, cmt. 14e (emphasis added). This comment makes clear that there generally is no duty to preserve ESI when the party does not reasonably anticipate litigation, nor where the routine operation of a computer system deletes data that resides elsewhere on a company’s systems or in its files (such as may occur in a true disaster recovery back-up system). However:

This does not mean a party may use its records management policy as a pretext for destroying documents or electronically stored information with impunity. Once a party reasonably determines that electronically stored information in its custody or control may be relevant to pending or reasonably foreseeable litigation, the party should take reasonable steps to preserve that electronically stored information, even if its records management program calls for its routine destruction. Determining a party’s duty to preserve requires answering two separate questions: “when does the duty to preserve attach?” and “what evidence must be preserved?” Failure to properly preserve information may result in sanctions, including monetary fines, instructions to the jury commanding them to infer that the destroyed documents would be adverse to the interests of the responding party, and, in extreme cases, default judgments. Therefore, an organization’s records management policy should recognize that the organization will sometimes have to suspend its ordinary retention and disposition of records and should include procedures designed to implement such suspensions.

*The Sedona Principles*, cmt. 14e.

### Decisions Interpreting Rule 37

In this context and against this background, several courts have explored and attempted to define the parameters of “routine, good faith” computer operation and corporate and individual conduct since the enactment of RULE 37(f). Five decisions handed down in the first ten months of the rule’s existence, including *Doe*, *In Re Krause*, *United Medical Supply*, *Disability Rights Council*, and *School-Link*, collectively drive home the point that while the

phrase “good faith” is inherently subjective and means different things to different people, courts grappling with these issues will train their focus far more on actual implementation and execution of information management procedures and litigation holds, rather than upon whether policies merely “exist.” These five key decisions are briefly discussed below.

### *Doe v. Norwalk Community College*

In *Doe v. Norwalk Community College*, the plaintiff, who had been sexually assaulted by a professor at the college, sued the defendants alleging violations of Title IX of the Education Amendments of 1972, and negligent retention and supervision of the professor. 2007 WL 2066497 at \*1. An inspection of the defendants’ computers by the plaintiff’s forensic expert revealed that, shortly after the lawsuit was filed, the hard drives of key NCC witnesses were completely scrubbed of data. Moreover, in accordance with NCC information retention policies, other witnesses’ electronic mailboxes had been “altered destroyed or filtered” and certain computers had been decommissioned, cleared of data, and reissued to other users. *Id.* at \*2. Additionally, numerous key employees, including NCC’s Head of Human Resources, testified that they had never heard the term “litigation hold” and had never been instructed to refrain from destroying documents. *Id.* at \*4. Finally, no steps were taken to stop the destruction of back-up tapes after the obligation to preserve arose. *Id.*

Finding that the duty to preserve was triggered when the defendants first learned of the plaintiff’s allegations of sexual assault by the professor, the *Doe* court held that the defendants engaged in spoliation of evidence by failing to institute a litigation hold at that time. *Id.* In so holding and ultimately imposing an adverse inference sanction, the court expressly rejected the defendants’ claim that RULE 37(f) protected them from sanctions on several grounds. *Id.* First, the court held that the defendants’ failures to act affirmatively to prevent their computer systems and policies from destroying or altering information after the hold obligation was triggered, precluded them from claiming that the destruction was a result of the “good faith” operation of their computer systems.

*Id.* Second, the court held that the defendants did not have one consistent “routine” document retention system in place as is required to invoke the protections of RULE 37(f). Critically, in holding “that defendants’ failure to place a litigation hold and preserve emails and hard drives... [was] at least grossly negligent, if not reckless,” the court clearly signaled that the defendants’ conduct not only failed to meet the RULE 37 “good faith” standard, but was in fact tantamount to *bad faith*. *Id.* at \*5.

#### **In Re Krause**

In *Krause*, the United States instituted an adversary proceeding that was later joined by a Chapter 7 trustee, against defendant/debtor Krause, an attorney who had tax liabilities in excess of \$3 million dollars. 367 B.R. at 745. Following discovery, the Trustee sought sanctions, including entry of a default judgment, because of Krause’s “actions in wiping, erasing or otherwise eradicating” ESI on the hard drives of his two personal computers before he turned them over to the Trustee. *Id.* Discovery revealed that after the court had ordered him to turn over his desktop and a day before the actual turnover, Krause had installed GhostSurf, an internet security program that “wipes” files that may be infected with viruses or worms, but can also be set to purge deleted files routinely in such a way that the data is permanently overwritten, thereby preventing its recovery or restoration. *Id.* at 750. The court found that Krause had spoliated evidence by continuing his practice of routinely deleting e-mails after a litigation hold should have been initiated, and by later using GhostSurf to purge his computer of all traces of deleted files. *Id.* at 766. In so holding, the court expressly rejected Krause’s attempt to invoke the “safe harbor” protections of RULE 37(f) by his claim that both his e-mail deletions and his use of GhostSurf (purportedly for its “internet security” functions) constituted a “good faith” and “routine” operation of his computer systems. *Id.* at 767. Wiping a hard drive is not a routine computer maintenance task, the court held, and here it was carefully calculated to deprive the government of evidence. The court entered the severe sanction of a partial default judgment against Krause. There does not

appear to be any serious question based on these facts that Krause’s use of GhostSurf was not “designed and implemented solely with the intent of meeting business and technical needs,” but rather “with the intent of thwarting discovery.” See *The Sedona Principles*, cmt. 14d.

#### **Disability Rights Council v. Washington Metro. Transit Auth.**

In *Disability Rights*, District Judge and noted e-discovery authority John M. Facciola addressed discovery disputes between disabled individuals and the Equal Rights Center (plaintiffs) and the Washington Metropolitan Area Transit Authority. 242 F.R.D. at 140. The suit arose out of the plaintiffs’ allegations against the defendant for violations of the Americans with Disabilities Act, 42 U.S.C. §1983. The plaintiffs filed a motion to compel the defendant to produce backup tapes of electronic documents written and received since the filing of the lawsuit. *Id.* at 145. They maintained that the defendant failed to instruct its employees properly to preserve relevant electronic documents and should, therefore, be responsible for the cost of creating the backup tapes. Specifically, the defendant configured its Groupwise e-mail system so that all e-mails were automatically deleted after only 60 days. The only exception to this automatic deletion was when a user manually archived a particular e-mail. In practice, however, only three Transit Authority employees actually archived their e-mails, and, therefore, with the exception of these individuals, “there has been a universal purging of all possibly relevant and discoverable emails every sixty days at least since the complaint was filed three years ago.” *Id.* at 146 (“Remarkably, although the complaint in this case was filed on March 25, 2004, [defendant] acknowledges it did nothing to stop its e-mail system from obliterating all emails after sixty days until at the earliest June of 2006.”). Not surprisingly, Judge Facciola dismissed defendant’s argument that RULE 37(f) could protect defendant’s conduct in light of defendant’s failure to modify the automatic deletion system. The court observed: “[u]nderstandably, WMATA [defendant] does not defend its failure to prevent the automatic feature from operating during the course of this litigation. Its failure is indefensible.” *Id.* The

court also declared that RULE 37(f) was inapplicable because the plaintiffs were not seeking sanctions, but instead, that the defendant be required to search backup tapes for discoverable information previously deleted. *Id.*

#### **United Medical Supply v. United States**

In *United Medical*, the plaintiff contractor brought suit against the United States for lost profits, outstanding payments, and the value of its goodwill and reputation lost as a result of payment delays arising out of a requirements contract entered into between the parties in 1997 to provide medical supplies to military medical treatment facilities (MTFs). 77 Fed. Cl. at 259. On September 13, 2002, the plaintiff filed an adversary proceeding against the United States in bankruptcy court seeking recovery under the Contract Disputes Act of 1978 (CDA), 41 U.S.C. §609(a). *Id.* Plaintiff’s counsel sent a copy of the summons to Kathleen Shahan, a Justice Department attorney assigned to investigate earlier related claims, who then forwarded the complaint to the Office of General Counsel of the Defense Supply Center-Philadelphia (DSCP). On October 1, 2002, Anthony Amendolia, an attorney with the DSCP, sent the first of three e-mails to a group of alleged contact personnel at the MTFs to ensure that documents related to the litigation were not destroyed. *Id.* at 259–60. Amendolia’s e-mails were not received by a number of the MTFs (as the group e-mail list was later found to be defective), and he never confirmed whether the recipients had received his messages, even after many of the recipients failed to respond to a message requesting a “yes” or “no” response. *Id.*

In addition to this failure to institute a litigation hold properly, the *United Medical* court considered that “over a period of approximately five years, it repeatedly violated its obligation to maintain” records once it had knowledge of plaintiff’s claim. Therefore, the court assessed the severe sanctions of (1) prohibiting defense from cross-examining the plaintiff’s expert to the extent that the expert interpreted, to the plaintiff’s favor, gaps in the record created by the defendant’s spoliation and from adducing its own expert testimony interpreting the same gaps; and (2) requiring

the defendant to reimburse the plaintiff for any additional discovery-related costs, including attorney's fees, occurring after discovery began related to the defendant's failures to preserve documents, as well as the fees incurred in pursuing the spoliation matter. *Id.* at 271. The court explained that an injured party is not required to demonstrate bad faith in order for the court

An injured party is not required to demonstrate bad faith in order for the court to impose . . . spoliation sanctions.

to impose, under its inherent authority, spoliation sanctions for conduct occurring between the time the duty to preserve attached and, at the least, the filing of a formal discovery request. *Id.* at 268. In making this determination, the court provided that when a court addresses a sanctions motion for spoliation pursuant to either RULE 37 or under the court's inherent authority, "it must construct a sanction that is just and proportionate in light of the circumstances underlying the failure to preserve relevant evidence, as well as the punitive, prophylactic, remedial and institutional purposes to be served by such sanctions." *Id.* at 270 (explaining that under this balancing approach, "the judge should take pains neither to use an elephant gun to slay a mouse nor to wield a cardboard sword if a dragon looms") (citations omitted).

**School-Link Technologies, Inc. v. Applied Resources, Inc.**

Although sanctions for failing to preserve information were imposed in each of the foregoing decisions, not all courts have determined that sanctions must necessarily follow a finding that a party failed to preserve relevant documents in connection with a litigation hold. For example, in *School-Link*, the District of Kansas addressed a business dispute between plaintiff School Link Technologies, Inc.

and defendant Applied Resources, Inc. arising out of the defendant's refusal to deliver goods because of the plaintiff's alleged breach of contract. 2007 WL 677647, at \*1. The plaintiff moved for spoliation and RULE 37 sanctions, alleging that the defendant violated its discovery obligations by failing to implement a litigation hold to preserve relevant evidence in the custody of one of its employees and by failing to search for and gather documents responsive to its discovery requests adequately. *Id.* The plaintiff's contention that the defendant failed to implement a litigation hold was substantially bolstered by the deposition testimony of one of the defendant's employees, who testified "that she had never been contacted by Defendant or its attorneys and instructed to search, gather, and preserve documents relevant to this litigation." The same employee "testified that she received no request or instructions to search her computer and hard copies files for documents that were requested by Plaintiff." *Id.* at \*2. The court concluded that the defendant's duty to preserve documents and information relevant to the dispute extended to the employee because she was a "key player," and that the defendant breached such a duty by failing to instruct the employee to gather and preserve documents or information relating to the lawsuit. *Id.* at \*4. Still, the court denied the plaintiff's motion for sanctions because the plaintiff was unable to establish that spoliation had occurred, even though the defendant had breached its duty to preserve documents relevant to the litigation. *Id.* ("[t]he difficulty with this argument is that Plaintiff has not identified what documents and information were allegedly by [the employee]. Identification of these documents is necessary here. . ."). *Id.*

**Keys Lessons from the Rule 37(f) Decisions**

While each of these cases turns on its specific facts, several important themes are repeated in the various courts' analysis of whether a party acted in "good faith."

"Good Faith" requires that litigation holds interrupt normal course destruction processes and that affirmative steps be taken to prevent the destruction of relevant ESI if routine systems would destroy the information.

*See Doe v. Norwalk Community College*, 2007 WL 2066497, at \*2-4; *In Re Krause*, 367 B.R. at 769; *Peskov v. Faber*, 2007 WL 2416119, \*7; *Disability Rights Council of Greater Wash. v. Wash. Metro. Area Transit Auth.*, 2007 WL 1585452 (D.D.C. June 1, 2007) at \*5-6.

"Good Faith" requires that a litigation hold be timely initiated and that custodians properly disseminate instructions and follow-up to monitor compliance. *See Doe*, 2007 WL 2066497, at \*4; *School-Link Technologies, Inc. v. Applied Resources, Inc.*, 2007 WL 677647, at \*4 (D. Kan. Feb. 28, 2007); *United Medical Supply Co, Inc.*, 77 Fed. Cl. at 259.

Decommissioned computers and the handling of these important potential sources of discoverable information are also a key issue. In this regard, the *Doe* decision makes clear that this issue requires special attention. *Doe*, 2007 WL 2066497, at \*6.

**Practice Tips for Getting to Good Faith under Rule 37(f)**

In conclusion, it is clear that acting in "good faith" pursuant to RULE 37 requires parties to do more than simply draft a solid information management policy that might reference a procedure for preserving litigation documents. At the very least, making a successful showing of "good faith" under RULE 37 will require a party to demonstrate that hold orders were timely issued, effectively communicated and were accompanied by diligent follow up to ensure compliance. Indeed, whereas the issuance of a litigation hold occupied center stage in early e-discovery decisions and discussions, steps taken *after* issuance of a hold order have now become the focus of intense court attention. Significantly, in virtually every 2007 court decision interpreting "good faith" litigation hold efforts, the party being accused of spoliation and required to defend its efforts had taken some preliminary steps to institute a preservation process; however, those steps were ultimately deemed inadequate largely due to failures in their execution, resulting in the loss of relevant and discoverable data.

The cases decided to date make clear that while there are no bright-line criteria that will ensure a party avoids the wrath of a court for spoliation of evidence, the follow-

---

ing steps should be considered a guideline for ensuring that the party's efforts comport with the common judicial understanding of "good faith" under RULE 37(f):

- Institute a standard litigation hold as soon as litigation could be reasonably anticipated;
- Communicate the requirements of the litigation hold to all employees and periodically follow up with employees to ensure compliance. Repeated and substantive follow up is critical;
- Investigate and identify all locations that may contain relevant ESI. The impor-

tance of counsel coordinating with the client's IT department to ensure identification, investigation and possible preservation of all modes of communication can not be overstated. All sources of information must be investigated. These include, without limitation, servers, laptop and desktop computers, active and decommissioned PDAs, Blackberrys, removable/portable media and drives and personal home computers; and

- Take affirmative steps to prevent the destruction of relevant, unique ESI that may be deleted or overwritten by auto-

matic processes, including the recycling of back-up tapes if these tapes are the sole source of relevant ESI. Courts will have no compassion for a party that allows relevant ESI to be destroyed by virtue of a failure to suspend an automatic deletion feature of a computer system.

While the list is not meant to be exhaustive, these guidelines provide a good starting point for parties and counsel to put themselves in the best position to meet the elusive "good faith" standard of new RULE 37(f). 