Northwestern Journal of Technology and Intellectual Property

Volume 5
Issue 1 *Fall*

Article 1

Fall 2006

Rule 37(f) Meets Its Critics: The Justification for a Limited Preservation Safe Harbor for ESI

Thomas Y. Allman

Recommended Citation

Thomas Y. Allman, *Rule 37(f) Meets Its Critics: The Justification for a Limited Preservation Safe Harbor for ESI*, 5 Nw. J. Tech. & Intell. Prop. 1 (2006).
http://scholarlycommons.law.northwestern.edu/njtip/vol5/iss1/1

This Article is brought to you for free and open access by Northwestern University School of Law Scholarly Commons. It has been accepted for inclusion in Northwestern Journal of Technology and Intellectual Property by an authorized administrator of Northwestern University School of Law Scholarly Commons.

NORTHWESTERN
JOURNAL OF TECHNOLOGY
AND
INTELLECTUAL PROPERTY

Rule 37(f) Meets Its Critics: The Justification for a Limited Preservation Safe Harbor for ESI

Thomas Y. Allman

Fall 2006 VOL. 5, NO. 1

© 2006 by Northwestern University School of Law
Northwestern Journal of Technology and Intellectual Property

Copyright 2006 by Northwestern University School of Law
Northwestern Journal of Technology and Intellectual Property
Volume 5, Number 1 (Fall 2006)

Rule 37(f) Meets Its Critics:

The Justification for a Limited Preservation Safe Harbor for ESI

Thomas Y. Allman*

I. INTRODUCTION

¶1 As of December 1, 2006, Rule 37(f) of the Federal Rules of Civil Procedure ("Rule 37(f)" or "the Rule") will provide protection against rule-based sanctions for a party's inability to provide electronically stored information ("ESI") in discovery when that information has been lost as a result of the routine, good faith operation of an electronic information system.[1] This limitation reflects a concern that the threat of sanctions in those circumstances unfairly impacts primary conduct – the way in which users of electronically stored information manage their storage and retention of information.[2] While the frequency of the risk of sanctions in those circumstances is debatable - the reported cases are few – the issue to which the reassurance of Rule 37(f) is directed is the distortion of primary conduct resulting from that threat.[3]

¶2 A number of criticisms have been levied at Rule 37(f). For example, two typical criticisms are set forth in the Spring 2006 issue of the Northwestern Journal of Technology and Intellectual Property. The first, by the quasi-official historian of the E-

---

* ©2006 Thomas Y. Allman. Mr. Allman is currently Senior Counsel to Mayer, Brown, Rowe & Maw LLP. He previously served as Senior Vice-President and General Counsel of BASF Corporation from 1993 until 2004 and was an early advocate for e-discovery amendments. *See* Thomas Y. Allman, *The Need for Federal Standards for Electronic Discovery*, 68 DEF. COUNS. J. 206, 209 (2001). He is also a member of the Steering Committee of the Working Group on Best Practices for Electronic Document Retention & Production of the Sedona Conference, authors of the "Sedona Principles."

[1] Rule 37(f) will read in full as follows: "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." In this paper I sometimes refer to the proposed amendments to the Federal Rules of Civil Procedure as "the Rules" and the proposed amendment to Rule 37 as simply "the Rule." FED. R. CIV. P. 37(f).

[2] Given the potential volumes of ESI involved, and the uncertainties over "triggering" events, an inflexible preservation standard broking no exceptions can be met only by either saving information that is not required to be saved ("over-preservation") or by ignoring potential risks of sanctions and facing the prospect of having to settle cases on unfavorable terms if one "guesses wrong." Neither prospect is fair and Rule 37(f) is intended to bring some relief from this "Hobson's choice." *See* 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, at ¶ 6 (2006) (contending that Rule 37(f) fails to "thoroughly address the problem").

[3] As a Member of the Advisory Committee noted, "[t]here is real benefit in reassuring parties that if they respond to litigation reasonably, they will be protected." *See* Minutes, Civil Rules Advisory Committee Meeting (Apr. 15-16, 2004), at 20, *available at* http://www.uscourts.gov/rules/Minutes/CRAC0404.pdf [hereinafter "Advisory Committee Minutes (April 2004)"].

Discovery rules process, Kenneth Withers, argues that Rule 37 falls "far short of that [which] the original proponents had wanted"[4] and is unworthy of the label "safe harbor."[5] The second, outlined by Nathan Drew Larsen, analyzes the efficacy of the Rule under the Rules Enabling Act and argues that it raises the specter of possible "collusion" among producers to "configure" their systems to destroy data.[6]

¶3 These observations – implying that the Rule is both ineffective and dangerous at the same time - miss the mark and deserve a response. In this article, I evaluate the quality and accuracy of the criticisms. Part II examines the Rule as promulgated by the Supreme Court. Part III traces the Rule's evolution and Part IV examines the common criticisms of the Rule and explains why they are unfounded. Part V concludes by explaining why the Rule satisfies appropriate and achievable objectives in a manner which will be useful to all courts facing similar issues.

II. RULE 37(F)

¶4 Rule 37(f) was drafted by the Civil Rules Advisory Committee ("Advisory Committee") at its meeting in April, 2005[7] after consideration of comments on an initial proposal made at Public Hearings held by the Committee in San Francisco, Dallas and Washington, D.C.[8] The Advisory Committee is one of several committees formed by the Judicial Conference of the United States (the "Judicial Conference")[9] to study potential changes in the rules of practice and procedure in specific fields[10] and is empowered to submit rule proposals to the Judicial Conference Committee on Rules of Practice and Procedure (the "Standing Committee") for review and approval. Rule 37(f) was subsequently endorsed (along with the other proposed e-discovery Rules)[11] by the Standing Committee[12] and, after a favorable recommendation by the Judicial Conference,

---

[4] Kenneth Withers, Electronically Stored Information: The December 2006 Amendments to the Federal Rules of Civil Procedure, 4 NW. J. TECH. & INTELL. PROP. 171, 208 (2006).

[5] Withers prefers to call Rule 37(f) a "lighthouse," picking up on terminology suggested at a Sedona Conference discussion of the topic. *See* Kenneth Withers, We've Moved the Two Tiers and Filled in the Safe Harbor, 52 FED. LAWYER 50, 54 (2005) (the phrase "safe harbor" is "no longer apt, if it ever was").

[6] Nathan Drew Larsen, Evaluating The Proposed Changes to Federal Rules of Civil Procedure 37: Spoliation, Routine Operation and the Rules Enabling Act, 4 NW. J. TECH. & INTELL. PROP 212, 223-224 & 226 (2006).

[7] *See generally* Minutes, Civil Rules Advisory Committee (Apr. 14-15, 2005), *available at* http://www.uscourts.gov/rules/Minutes/CRAC0405.pdf [hereinafter "Advisory Committee Minutes (April 2005)"].

[8] Copies of the comments and transcripts of the remarks of over 200 witnesses are available at http://www.uscourts.gov/rules/e-discovery.html [hereinafter "Public Hearing Comments"]. The comments present a valuable snapshot of e-discovery concerns and current practices as of 2005 and contain insightful observations which played a role in formulation of the final form of the Amendments.

[9] The Judicial Conference of the United States is composed of the Chief Judges from each Circuit along with District Court representatives and is charged by statute with the responsibility to "carry on a continuous study of the operation and effect of the general rules of practice and procedure." 28 U.S.C. § 331 (2006).

[10] Other Advisory Committees have jurisdiction over proposed rules for Appellate Practice and for Bankruptcy, Criminal and Evidence matters. *See* Federal Rulemaking, http://www.uscourts.gov.

[11] Rule 37(f) is part of an integrated package of amendments to Rules 16, 26, 33, 34, 37, 45 and Form 35. *See* http://www.uscourts.gov/rules/EDiscovery_w_Notes.pdf.

[12] *See* JUDICIAL CONFERENCE OF THE UNITED STATES, REPORT OF THE JUDICIAL CONFERENCE COMMITTEE ON RULES OF PRACTICE AND PROCEDURE, at Rules App. C-83 (2005), *available at* http://www.uscourts.gov/rules/Reports/ST09-2005.pdf [hereinafter "STANDING COMMITTEE REPORT

by the Supreme Court in April, 2006[13] Assuming no complications, Rule 37(f) will come into effect in December, 2006.[14]

¶5 Requests for spoliation sanctions[15] are often sought where an inability to produce ESI during discovery results from a failure to preserve a source of ESI before active discovery is undertaken. The Rule does not differentiate between losses of ESI which are caused by events that occur before institution of litigation and those that occur afterwards. It also applies only to motions seeking "sanctions," and not to "the kinds of adjustments frequently made in managing discovery if a party is unable to provide responsive information."[16]

¶6 Rule 37(f) is intended to serve as part of a solution to the practical problems of ESI preservation and production.[17] The Advisory Committee chose not to enact detailed preservation rules but instead established a framework to encourage early voluntary agreement on preservation steps. Rule 26(f) establishes a "new paradigm"[18] of mandatory discussion of preservation and production issues involving ESI, which will hopefully yield an accommodation on preservation steps satisfactory to both parties. If not, the Court is empowered to enter specific orders to guide the parties.[19] A requesting party failing to identify or act on preservation issues will not be allowed to take a "gotcha" or ambush approach by waiting until too late to raise preservation issues.[20]

(2005)"]. The Standing Committee Report (2005) contains, as Appendix C, the May 27, 2005, Report of the Civil Rules Advisory Committee, amended July 25, 2005 [hereinafter "ADVISORY COMMITTEE REPORT (2005)"]. That Report contains the final form of Rule 37(f) and the related Committee Note and is an indispensable source of background and interpretive information regarding its evolution.

[13] *See* Transmittal Letters to Congress and Supreme Court Orders, http://www.uscourts.gov/rules/Letters_Orders.pdf.

[14] Under the Rules Enabling Act, 28 U.S.C. §§ 2071-2077, inaction by Congress will lead to the proposed Rules becoming effective on December 1, 2006.

[15] *See* William Robinson, *An Overview of Electronic Discovery*, 841 PLI/PAT 189 (2005) (collecting cases).

[16] These types of adjustments do not involve risk of case-ending spoliation sanctions that underlie the need for Rule 37(f). *See* STANDING COMMITTEE REPORT (2005), *supra* note 12, at Rules App. C-88 ("[A] court [can] order the responding party to produce an additional witness for deposition, respond to additional interrogatories or make similar attempts to provide substitutes or alternatives for some or all of the lost information.").

[17] *See* STANDING COMMITTEE REPORT (2005), *supra* note 12, at Rules App. C-83 ("[I]t can be difficult to interrupt the routine operation of computer systems to isolate and preserve discrete parts of the information they overwrite, delete, or update on an ongoing basis, without creating problems for the larger system. . . [and it] is also undesirable; the result would be even greater accumulation of duplicative and irrelevant data that must be reviewed, making discovery more expensive and time-consuming."). The Standing Committee Report (2005) contains both the final version of the Rules and the Committee Notes as promulgated and the introductory explanations to the Judicial Conference not found on the Administrative Office site noted above.

[18] *See* Thomas Y. Allman, *The Impact of the Proposed Federal E-Discovery Rules*, 12 RICH. J.L. & TECH. 13 (2006) (arguing that requesting parties must do a better job of articulating their discovery focus and producing parties must be prepared to candidly discuss steps taken to preserve source of potentially discoverable evidence).

[19] A related requirement in Rule 26(b)(2)(B) that a producing party must identify any potentially relevant inaccessible sources of ESI that it will not search means that contentious issues about preservation of those sources will also surface early. *See* STANDING COMMITTEE REPORT (2005), *supra* note 12, at Rules App. C-48 ("Whether a responding party is required to preserve unsearched sources of potentially responsive information that it believes are not reasonably accessible depends on the circumstances of each case. It is often useful for the parties to discuss this issue early in discovery.").

[20] *See generally* Treppel v. Biovail, 233 F.R.D. 363, 374 (S.D.N.Y. 2006) (criticizing requesting party's failure to even discuss search terms proposed by producing party as a "missed opportunity").

¶7 Accordingly, the need to invoke Rule 37(f) will hopefully exist only in isolated instances, such as challenges to preservation steps taken or not taken concerning inaccessible sources of information in the absent of an agreement or court order.[21] When invoked, Rule 37(f) will involve a two-step analysis.

¶8 First, a Court must determine if sanctions for the failure to produce lie pursuant to one of the provisions of the Federal Rules.

¶9 Second, a Court applying Rule 37(f) must determine whether, under all the circumstances, the failure to produce ESI in discovery resulted from circumstances which fall within the scope of the Rule. This will turn on whether the loss resulted from a "routine" and "good faith" operation of a covered "information system" and has not resulted in "exceptional circumstances."

A. Information Systems

¶10 An "information system" creates and manages electronically stored data, whether in the form of email, raw data, images or other electronic form. A wide variety of such systems are typically used to perform the range of important business and regulatory functions within an entity. As a normal or "routine" part of the operation of such systems, data is overwritten, deleted or modified by automatic or manually initiated processes, pursuant to the design or programming of the operating software.[22] The use of the phrase "routine operation" in reference to such an information system emerged during discussions at the April 2004 Advisory Committee meeting[23] to describe the normal aspects of systems that might result in data losses and which should be presumptively subject to the safe harbor under discussion.[24] Serving in that role, the phrase was part of the initial Rule 37(f) proposal published for Public Comment[25] and ultimately survived the subsequent revisions as a basic concept in Rule 37(f).[26]

¶11 The Committee Note to Rule 37(f) is neutral as to information technology, so it does not list specific examples of systems the Advisory Committee had in mind. However, the Standing Committee Report to the Judicial Conference mentions "programs

---

[21] As a practical matter, in most instances preservation of reasonably accessible sources of discoverable information will be sufficient and it will not be necessary to take steps to preserve inaccessible sources. *See* Thomas Y. Allman, *New Rules Should Clarify Expectations*, LAW TECH. NEWS (Aug. 2005) ("preservation obligations will take into consideration not only the potential relevance of information, but also its accessibility"). The Committee Note to Rule 37(f) states that inaccessible sources need be preserved only if a party "reasonably believes that the information on such sources is likely to be discoverable and not available from reasonably accessible sources." STANDING COMMITTEE REPORT (2005), *supra* note 12, at Rules App. C-87.

[22] STANDING COMMITTEE REPORT (2005), *supra* note 12, at Rules App. C-86-87.

[23] *See* Advisory Committee Minutes (April 2004), *supra* note 3.

[24] *See* Memorandum from Myles V. Lynk & Richard L. Marcus to the Advisory Committee on Civil Rules (Apr. 5, 2004), at 35 (recommending alternative language preventing imposition of sanctions where "failure resulted from the normal operation of the person's electronic information system"), *available at* http://www.kenwithers.com/rulemaking/civilrules/marcus040604.pdf.

[25] *See* COMMITTEE ON RULES OF PRACTICE AND PROCEDURE, REPORT OF THE CIVIL RULES ADVISORY COMMITTEE (May 17, 2004, revised Aug. 3, 2004) (containing final version of Rule 37(f) as issued for public comment), *available at* http://www.uscourts.gov/rules/comment2005/CVAug04.pdf [hereinafter "ADVISORY COMMITTEE REPORT (2004)"],.

[26] *See* ADVISORY COMMITTEE REPORT (2005), *supra* note 12, at 88 ("The present proposal carries forward a central part of the published proposal – the information must have been lost in the system's 'routine operation.'").

that recycle storage media kept for brief periods against the possibility of a disaster that broadly affects computer operations" and "programs that automatically discard information that has not been accessed within a defined period" as examples of "routine" operations in current technology.[27]

¶12 The fact that human involvement is part of the process does not make the operation causing the failure other than "routine," as is shown by the reference to the recycling of backup media, which is instituted by members of an IT function pursuant to a retention schedule.[28] The "routine" aspect of the operation is the physical recycling process. Similarly, the pressing of the "delete" key by users initiates a "routine" feature of the email system, incidental to its operation."[29]

¶13 In other words, the issue under Rule 37(f) is whether the feature causing destruction is a normal part of that process, not whether some other approach could have been used. A feature added to an existing system solely for the purpose of deleting information needed in litigation would receive short shrift.[30]

B. Culpability

¶14 The key differentiating factor in applying Rule 37(f), however, is the presence or absence of "good faith" in the routine operation of the information system. It is only those losses resulting from "good faith" operations which are exempted from sanctions. It is clear that mere negligence or inadvertence in operating an otherwise reasonable information system does not bar a finding that the entity was acting in good faith. As a Member of the Advisory Committee stated during the April 2005 meeting of the Advisory Committee, "[G]ood faith lies at a point intermediate between negligence and recklessness. It assumes the party has a reasonable litigation hold, and did not deliberately use the system's routine destruction functions. 'If you know it will disappear and do nothing, that is not good faith…[t]he line is conscious awareness the system will destroy information.'"[31] Rule 37(f) thus represents the state of mind which must exist to be exempt from sanctions.[32]

---

[27] STANDING COMMITTEE REPORT (2005), *supra* note 12, at Rules App. C-83.

[28] The draft Committee Note to Rule 37(f), written after the April 2005 meeting, referred to "automatic features" in routine operations. *See* ADVISORY COMMITTEE REPORT (2005), *supra* note 12, at 87. The reference to "automatic" was deleted from the final draft of the Committee Note to emphasize that human involvement is not a disqualification. Thus, the final Committee Note simply refers to "features" which are "essential to the operation of electronic information systems." ADVISORY COMMITTEE REPORT (2005), *supra* note 12, at 106.

[29] *See* Concord Boat Corp. v. Brunswick, No. LR-C-95-781, 1997 WL 33352759, at *6 (E.D. Ark. 1997) (fact that employees decide whether or not to delete email does not require finding of bad faith when some email is lost); Ian C. Ballon, *How Companies Can Reduce the Costs and Risks Associated with Electronic Discovery*, 15 COMPUTER LAW. 8 (1998) (arguing that email deletion is not equivalent to document destruction).

[30] *See* Lewy v. Remington Arms Co., 836 F.2d 1104, 1112 (8th Cir. 1988) (a corporation cannot blindly destroy documents and expect to be shielded by a seeming innocuous document retention policy); *See also* Mastercard Int'l v. Moulton & KTM Media, No. 03 Civ. 3613 VMMHD, 2004 WL 1393992 (S.D.N.Y. 2004) (deliberate and inexcusable conduct in consciously deleting information).

[31] Advisory Committee Minutes (2005), *supra* note 7, at 42.

[32] As a practical matter, Rule 37(f) limits the impact of *Residential Funding Corp. v. DeGeorge Financial Corp.*, 306 F.3d 99, 107-8 (2d Cir. 2002) (adverse inference can be granted for negligent conduct), in the context of "routine, good faith" loss of ESI from information systems. Interestingly, since *Residential Funding* provided the rule of decision for *Zubulake v. US Warburg, LLC (Zubulake V)*, 229

¶15 Determining the application of Rule 37(f) requires an assessment as to whether the features causing the loss were operated without a disqualifying culpability.[33] In making the assessment, the issue should be whether the process involved was "reasonably calculated" to achieve its goals, not whether perfect results were achieved.[34]

C. Exceptional Circumstances

¶16 Rule 37(f) will not apply in those rare circumstances where the conduct of the party seeking relief from sanctions has resulted in such a degree of prejudice that it is unfair to restrict the power of the court. The Standing Committee Report to the Judicial Conference explained that the clause was added to provide "flexibility" in the event of "serious prejudice" resulting from the loss.[35]

III. EVOLUTION OF RULE 37(F)

¶17 Before turning to the specific criticisms of the Rule, it is helpful to understand its evolution during the five years preceding adoption in April, 2005.

A. Original Proposals

¶18 The roots of Rule 37(f) can be fairly traced to the mini-conferences held by the Discovery Subcommittee of the Advisory Committee at its request[36] at Hastings[37] and Brooklyn[38] Law schools during 2000. Both mini-conferences featured panels of judges, lawyers and technical consultants with extensive experience in e-discovery and both identified issues about meeting preservation expectations as major concerns.

F.R.D. 422 (S.D.N.Y. 2004), one can speculate about whether a different form of sanction might have been considered in that case had Rule 37(f) been in effect at that time.

[33] As the Standing Committee Report explained, "The Advisory Committee [in enacting Rule 37(f)] revised Rule 37(f) to adopt a culpability standard intermediate between the two published versions [of culpability]." STANDING COMMITTEE REPORT (2005), *supra* note 12, at Rules App. C-84-85.

[34] *See* Thomas Y. Allman, *Ruling Offers Lessons for Counsel on Electronic Discovery Abuse*, 19 WASH. LEGAL FOUND. LEGAL BACKGROUNDER, at 3 (Oct. 14, 2004) ("where there is uncertainty about the timing and nature of disputes and the individuals involved, a sliding scale approach balancing the type of case involved with the number of sources of potentially discovery information is sufficient to meet preservation requirements"), *available at* http://www.wlf.org/upload/101504LBAllman.pdf.

[35] STANDING COMMITTEE REPORT (2005), *supra* note 12, at Rules App. C-85 ("The exceptional circumstances provision adds flexibility not included in the published drafts") and Rules App. C-86 ("This provision recognizes that in some circumstances a court should provide remedies to protect an entirely innocent party requesting discovery against serious prejudice arising from the loss of potentially important information.").

[36] The Advisory Committee assigned to its Discovery Subcommittee the task of identifying any "issues peculiar to electronic discovery that might justify rules amendments" at its October 1999 Meeting in Kennebunkport, Maine. Minutes, Civil Rules Advisory Committee Meeting (Oct. 14-15, 1999), *available at* http://www.uscourts.gov/rules/Minutes/1099mnCV.pdf.

[37] Minutes, Discovery Subcommittee Meeting at Hastings College of the Law, San Francisco, Cal. (Mar. 27, 2000). A summary of the remarks prepared by an attendee (Andrew Mastin of Pillsbury, Madison & Sutro) is on file with the author.

[38] Minutes, Discovery Subcommittee Meeting at Brooklyn Law School, New York, N.Y. (Oct. 27, 2000). A summary of the remarks prepared by an attendee (Ashish Prasad of Mayer, Brown & Platt) is on file with the author.

¶19 In December 2000, after reflecting on discussions at the Brooklyn Conference and my experiences as one responsible for litigation compliance,[39] I wrote to (then) Magistrate Judge John Carroll, Chair of the Discovery Subcommittee[40] to suggest adoption of a targeted safe harbor rule exempting the continued good faith operation of disaster recovery and other systems from rule-based sanctions unless a prior order was issued requiring their preservation.[41] I also suggested that only willful violations of preservation orders should justify imposition of sanctions. As far as I can tell, this was the first explicit suggestion for a preservation safe harbor, which I amplified in other articles.[42]

¶20 The ensuing period saw case law evolve on a number of basic e-discovery issues[43] in District Court opinions[44] and enactment of some local rules on specific aspects of e-discovery.[45] It was also during this period that the *Sedona Conference*®[46] was organized

---

[39] At the time, I was serving as both a General Counsel and Chief Compliance Officer of a large corporation and had encountered many of the concerns discussed at Brooklyn.

[40] Judge Carroll now serves as Dean of the Cumberland School of Law of Sanford University, located in Birmingham, Alabama. *See* http://cumberland.samford.edu (last accessed July 26, 2006).

[41] *See* Letter, Thomas Allman to The Hon. John L. Carroll, U.S. Magistrate Judge (Dec. 12, 2000), *available at* http://www.kenwithers.com/articles ("no sanctions or other relief" should be "predicated upon a failure to maintain or preserve documents or data, including electronically stored information," without proof of a "willful failure to preserve such documents or data" in response to a specific document request and a party need not "suspend or alter the operation in good faith of disaster recovery or electronic or computer systems absent a court order issued upon good cause shown." Evidence of reasonable steps being taken to notify computer custodians of relevant preservation obligations would serve as "prima facie evidence of compliance" with those preservation obligations.).

[42] *See* Allman, *supra* note *, at 206 (suggesting a limitation in Rule 34 on the need to suspend or alter "the operation in good faith of disaster recovery or other electronic or computer systems absent court order issued upon good cause shown"). *See also* Thomas Y. Allman, *The Case for a Preservation Safe Harbor in Requests for E-Discovery*, 70 DEF. COUNS. J. 417 (2003); Thomas Y. Allman, *A Preservation Safe Harbor in e-Discovery*, ANTITRUST SOURCE (July 2003) (emphasizing the use of the "accessibility" to identify the types of information to which preservation obligations should presumptively attach).

[43] The concept of the "accessibility" of electronically stored information was used in the first *Zubulake* decision to differentiate among various types of storage media in regard to cost-shifting. *See* Zubulake v. UBS Warburg (*Zubulake I*), 217 F.R.D. 309 (S.D.N.Y. 2003). Inherent in such an assessment was the concept of avoiding undue burden or cost, which ultimately was adopted in proposed Rule 26(b)(2)(B) as the differentiating factor between the "two-tiers" of ESI discovery. For example, in *Medtronic Sofamor Danek, Inc. v. Gary Karlin Michelson et al.*, No. 01-2373-M1V, 2003 U.S. Dist. LEXIS 8587 (W.D. Tenn. 2003), the District Court found it to be an "undue" burden to require the restoration of the 996 network backup tapes at issue and ordered cost-sharing under a formula subject to a protocol.

[44] The limits of the case by case method in regard to e-discovery law is described vividly and with a great deal of insight in Robert Douglas Brownstone, *Collaborative Navigation of the Stormy E-Discovery Seas*, 10 RICH. J.L. & TECH. 53, at ¶ 29 (2004) ("As in other contexts, there are four reasons why we will get very old if we wait for the adjudicative process to finish that task [developing e-discovery principles]. First, 'most reported discovery cases come from trial courts and have little precedential value.' Second, there is generally very little guidance from courts of appeals, because few discovery cases get appealed. Third, when such cases are appealed, the level of appellate review is deferential, leaving most discovery determinations within the discretion of the trial judge. Fourth, the reported decisions tend to involve obstructionist conduct at the most egregious end of the spectrum, thus arguably offering insufficient guidance to those acting in a mainstream manner.").

[45] *See* STANDING COMMITTEE REPORT (2005), *supra* note 12. The District Courts in Arkansas, Wyoming, Kansas and New Jersey promulgated a variety of Local Rules and procedures and the District Court of Delaware, through its Chief Judge, promulgated a default standard for parties that could not agree.

[46] The Sedona Conference is the author of various resources related to the discovery of ESI, most notably the *Sedona Principles*, issued in draft form in early 2003 and in final form in January 2004, containing fourteen "best practice" recommendations. *See generally The Sedona Principles: Best Practice Recommendations & Principles for Addressing Electronic Document Production* (Sedona Conference

and bar associations, legal publications and litigation support vendors held scores of conferences on e-discovery.[47] A key milestone was the publication of the "prescient"[48] Law Journal article on e-discovery by Northwestern Law Professor Martin C. Redish.[49] Professor Redish famously noted that society and the rule-making process must be prepared to limit the search for truth to take into account other elements of the litigation matrix, such as the need to provide predictable standards of primary behavior.[50]

¶21 In April 2003, after soliciting and receiving further input on the topic,[51] the Discovery Subcommittee informed the Advisory Committee that "after more than three years of considering these issues, the Subcommittee believes that the time for more concrete action has arrived."[52] The Subcommittee delivered a comprehensive set of proposals for consideration by the Advisory Committee in September 2003[53] and after preliminary review at its October 2003 meeting,[54] the Advisory Committee scheduled a two-day Conference on E-Discovery at Fordham University Law School (the "Fordham Conference") for February 2004 to discuss them.

B. The Fordham Conference

¶22 The Fordham Conference was attended by a cross-section of the bench and bar with members of the Standing Committee of the Judicial Conference. Members of the technical and consulting community were also present. Participants were furnished with copies of the Subcommittee proposals in advance of the meeting.

Working Group Series, 2005 Version), *available at* http://www.thesedonaconference.org [hereinafter "*Sedona Principles*"]. *See also ABA Civil Discovery Standards*, A.B.A. SEC. LITIG. ELEC. DISCOVERY TASK FORCE, Report 103B, Amendments to the Civil Discovery Standards (revised Aug. 2004).

[47] Kenneth Withers, *Two Tiers and a Safe Harbor: Federal Rulemakers Grapple with E-Discovery*, FED. LAWYER, at 3 (Sept. 2004), *available at* http://www.kenwithers.com/articles/tf/0904.pdf.

[48] *See* Nelson & Rosenberg, *supra* note 2, at 22 (noting that Prof. Redish's article preceded rash of e-discovery cases); *see also* Martino v. Wal-Mart, 908 So. 2d 342, 347 (Fla. 2005) (Wells, J., concurring) (citing Redish article as basis for raising "serious constitutional and practical concerns" regarding assertion that preservation duties were triggered two years before filing of suit).

[49] Martin Redish, *Electronic Discovery and the Litigation Matrix*, 51 DUKE L.J. 561 (2001) (criticizing a strict liability rule requiring constant review of backup media for documents that could at some later point be deemed relevant upon threat of sanctions for incorrect predictions).

[50] *Id.* at 623.

[51] For example, Lawyers for Civil Justice ("LCJ"), a defense oriented coalition of corporate and outside counsel and the leadership of various defense bar groups emphasized the need for a safe harbor. LCJ pointed out inconsistent jurisprudence on the application of preservation obligations and listed specific anecdotal instances of the need for relief. Suggested amendments included a "safe harbor" which would exempt a producing party from sanctions "for the continued good faith operation of business systems absent a specific order or unobjected discovery demand which was willfully disregarded." *See* Letter, Rex Lindner, President LCJ, to Peter McCabe, Secretary, Committee on Rules of Practice and Procedure, December 2002, reproduced in LCJ Comments to Civil Rules Advisory Committee (Mar. 12, 2004) (on file with author).

[52] Myles V. Lynk & Richard L. Marcus, *Discovery Subcommittee Report on Electronic Discovery* (Apr. 14, 2003), *available at* http://www.kenwithers.com/rulemaking/index.html.

[53] Memorandum from Rick Marcus to Advisory Committee, *E-Discovery Rule Discussion Proposals* (Sept. 15, 2003) *available at* http://www.kenwithers.com/rulemaking/civilrules/marcus091503b.pdf.

[54] See Minutes, Civil Rules Advisory Committee Meeting (Oct. 2-3, 2004) ("The central focus [of the Fordham Conference] will be to advise the Advisory Committee and the Standing Committee whether we need rules, and if so what the rules might be.").

¶23 In regard to preservation and spoliation issues, the Subcommittee recommended altering Rule 26 or adding a new Rule 34.1 to emphasize that parties need not suspend the "operation in good faith" of "disaster recovery or other [computer] systems" provided that one day's backup was retained. The proposal also stated that information in inaccessible form did not have to be preserved unless a court ordered the party to do so.[55] As a second and "complementary" step to these changes, the Subcommittee also recommended that a new Rule 37(f) be added to make it clear that no sanctions would be issued for a failure to produce ESI unless the party "willfully or recklessly" deleted or otherwise made ESI unavailable after having been served with a request that described it with reasonable certainty.[56]

¶24 A separate panel discussion at the Fordham Conference was devoted to safe harbor issues, with the author participating.[57] Not surprisingly, the panelists were not in complete agreement either on the need for a safe harbor rule or on the specific components required should one be adopted.[58]

C. Published Proposals - August 2004

¶25 The Advisory Committee met in April 2004[59] to decide whether to initiate the rulemaking process. The Discovery Subcommittee had met prior to the meeting and a revised set of e-discovery recommendations was before the Advisory Committee.[60] By the conclusion of the meeting, it had agreed to proceed and had settled on a proposed package of e-discovery amendments, including a proposed Rule 37(f) and related Committee Note.[61] These materials were ultimately published by the Standing Committee (along with proposed amendments to the Bankruptcy, Criminal and Evidence rules) in August 2004 with public comments due by mid-February 2005.[62]

---

[55] *See* Participant Memoradum, Conference on Electronic Discovery, Fordham Law School, New York, N.Y. (Feb. 20-21, 2004), at 34-38, *available at* http://uscourts.gov/rules/E-Discovery_Conf_Agenda_Materials.pdf.

[56] *Id.* at 39.

[57] *See Panel Discussions: Panel Four: Rule 37 and/or A New Rule 34.1: Safe Harbors for E-Document Preservation and Sanctions*, 73 FORDHAM L. REV. 71 (2004) (quoting panel members Andrew Scherffius (Moderator), Thomas Allman, Stephen Morrison, Laura Owens and Anthony Tarricone) [hereinafter "*Panel Discussions*"].

[58] *Id.* at 73-83. *Compare* Comments by Tarricone (accusing the panel of losing its 'moral compass" since the safe harbor will allow regular suspension policies to continue without concern for public safety, public interest and public good) *with* Comments by Allman (parties which engage in good faith efforts to preserve information should not be sanctioned if it turns out later, judging in retrospect, that the information was not adequately preserved).

[59] *See* Advisory Committee Minutes (April 2004), *supra* 4, at 22.

[60] *See* Lynk & Marcus, *supra* note 52, at 36. (The Subcommittee abandoned its suggestion for a separate rule entitled a "Duty to Preserve" and noted that "a preservation duty might look odd if it purported to regulate a party's behavior before a suit was filed in federal court. Limiting the use of sanctions should pose fewer difficulties than trying to articulate a duty of preservation . . . ").

[61] The initial Advisory Committee Report prepared after the Advisory Committee Meeting but before the Standing Committee meeting was dated May 17, 2004. *See* ADVISORY COMMITTEE REPORT (2004), *supra* note 25.

[62] The initial Advisory Committee Report was revised on August 3, 2004 after discussions with the Standing Committee. ADVISORY COMMITTEE REPORT (2004), *supra* note 25. The Standing Committee Request for Comments included both the Civil Rules report and the reports regarding the respective proposed amendments to Bankruptcy, Criminal and Evidence rules. Standing Committee Request for Comments (Aug. 9, 2004) (on file with author).

¶26 Proposed Rule 37(f) provided, in relevant part, that ". . . a court may not impose sanctions under these rules on the [producing] party for failing to provide [ESI] if: (1) the party took reasonable steps to preserve the information after it knew or should have known the information was discoverable in the action; and (2) the failure resulted from loss of the information because of the routine operation of the party's electronic information system."

¶27 Some Members at the Advisory Committee meeting objected to attaching disqualifying consequences to the lower range of the "fault" spectrum (negligence)[63] and insisted that only willful or reckless conduct should deny protection under Rule 37(f). Accordingly, the Advisory Committee prepared and the Standing Committee approved inclusion of a footnote requesting comments "on whether the culpability or fault that takes a party outside any safe harbor should be something higher than negligence[64] and included an example "to focus comments and suggestions."[65]

¶28 The Advisory Committee did not promulgate a separate rule spelling out preservation obligations. Instead, the proposed Committee Note described a three part analysis for use in evaluating the reasonable steps needed to preserve electronically stored information.[66] First, the outer limit of information to be preserved would be determined by the existing limits on the scope of discovery established by Rule 26(b)(1).[67] Second, given that amended Rule 26(b)(2) conditioned the discovery of inaccessible ESI on issuance of a court order, the Note observed that "[i]n most instances, a party acts reasonably by identifying and preserving reasonably accessible electronically stored information that is discoverable without court order."[68] The third factor was what the party then knew about the nature of the litigation, which "should inform its judgment about what subjects are pertinent to the action and which people and systems are likely to have relevant information."[69]

---

[63] *See* Welsh v. United States, 844 F.2d 1239 (6th Cir. 1988) (finding that destruction of potentially relevant evidence can occur along a "continuum of fault" ranging from innocence through the degrees of negligence to intentionality with resulting penalties which vary correspondingly).

[64] ADVISORY COMMITTEE REPORT (2004), *supra* note 25, at 32.

[65] ADVISORY COMMITTEE REPORT (2004), *supra* note 25, at 32-33. In relevant part, the alternative provided that "[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 (1) the party intentionally or recklessly failed to preserve the information; or (2) the party violated an order in the action requiring the preservation of the information."

[66] ADVISORY COMMITTEE REPORT (2004), *supra* note 25, at 34.

[67] Rule 26(b)(1) limits party managed discovery to "any matter, not privileged, that is relevant to the claim or defense of any party, including the existence, description, nature, custody , condition, and location of any books, documents, or other tangible things and the identify and location of persons having knowledge of any discoverable matter." A court may order "discovery of any matter relevant to the subject matter involved in the action" for good cause. The Amendments do not change this provision.

[68] The draft Committee Note to Rule 37(f) acknowledged, however, that in some instances, "reasonable care" may require preservation of electronically stored information that is not reasonably accessible if the party "knew or should have known" that it was "discoverable in the action and could not be obtained elsewhere. ADVISORY COMMITTEE REPORT (2004) *supra* note 25, at 34-35 (preservation may be less burdensome than access and is necessary to support discovery if good cause is shown).

[69] ADVISORY COMMITTEE REPORT (2004), *supra* note 25, at 35.

D. The 2005 Public Hearings and Comments

¶29 The response to Rule 37(f) was mixed at the public hearings held in San Francisco, Dallas and Washington in January and February 2005. Representatives of public and private entities generally favored some form of safe harbor, noting that the fear of sanctions for inadvertent loss of ESI had created an unfair chilling effect[70] and had distorted business processes by encouraging over-retention of information.

¶30 However, some supporters of the safe harbor concept also expressed concern about the fact that, as written, the protection afforded by Rule 37(f) apparently could be lost by merely negligent or inadvertent conduct.[71] A typical comment was made by a representative of The City of New York Law Department, which argued that it was unfair to subject a party to sanctions for the conduct of a low level employee who may negligently delete electronic information despite reasonable preservation efforts by City attorneys and management personnel.[72]

¶31 Some opponents argued that there was no empirical proof of a need to act based on the paucity of reported decisions citing entities for anything other than willful misconduct.[73] Others argued that proposed Rules 26(b)(2) and 37(f) would encourage corporate entities to shift information from being reasonably accessible to becoming increasingly inaccessible, with the additional burden of access being imposed on the requesting party.[74] Some commentators also criticized the Committee Note for failing to adequately state the need to preserve inaccessible information for later review to determine if it should be produced.[75]

---

[70] As a representative of the Association of Corporate Counsel (ACC) noted, "[B]usinesses create records retention policies for many business-related reasons, having nothing to do with litigation [but] the threat that implementing even a legitimate policy could subject a company to sanctions, has delayed or even scuttled the implementation of corporate electronic data retention policies. Public Hearing Comments, *supra* note 8, Testimony of Lawrence La Sala, Ass't General Counsel, Textron (Feb. 11, 2005) (04-CV-095), at 369.

[71] A representative of the Department of Justice noted, for example, that "[m]any federal agencies have large quantities of electronic data and are involved frequently in litigation [and it] can be very difficult to disseminate discovery-related retention requirements to all relevant persons within an agency, particularly if multiple offices in various geographic locations are involved." Public Hearing Comments, *supra* note 8, Testimony of Peter D. Keisler, Assistant Attorney General, U.S. Department of Justice (Feb. 15, 2005) (04-CV-203), at 8-9.

[72] Public Hearing Comments, *supra* note 8, Testimony of Lawrence S. Kahn, Chief Litigating Assistant, City of New York Law Department (Feb. 15, 2005) (04-CV-220), at 4-5.

[73] A study published by an Advisory Committee Member during the debate noted that (based on reported decisions) courts did not sanction for the "smallest infractions," although they sometimes "sanction[ed] negligent but prejudicial conduct. *See* Shira Scheindlin & Kanchana Wangkeo, *Electronic Discovery Sanctions in the Twenty-First Century*, 11 MICH. TELECOM. TECH. L. REV. 71, 94 (2004) (reporting on the results of a review of 45 Federal and 21 State sanction cases).

[74] *See, e.g.*, Ronald Hedges, *A View from the Bench and the Trenches: A Critical Appraisal of Some Proposed Amendments to the Federal Rules of Civil Procedure*, 227 F.R.D. 123, 139 (2005) (noting the ATLA argument that the amendments are an attempt to constrict plaintiffs rights to discovery); *see also* James Rooks, *Abridged Too Far: Discovery Rights and the Campaign for Special E-Discovery Rules*, EDD 18 (Special Advertising Supplement) at EDD 21 (2005) (arguing that corporations will routinely purge information).

[75] The assertion was that a party could label otherwise discoverable information as inaccessible, destroy it before discovery began and then plead that it did not know it was discoverable. The Committee Notes to Rule 26(b)(2) and the Committee Note to Rule 37(f) were amended to emphasize that the underlying preservation obligations are not modified by the proposed rules and must be evaluated separately. *See* STANDING COMMITTEE REPORT (2005), *supra* note 12, at Rules App. C-85 ("To respond to concerns that

E. Final Form of Rule 37(f)

¶32 In the end, after considering the matter from all angles, the Advisory Committee decided to simplify Rule 37(f) during their meeting of April 2005. The Committee dropped the reference to preservation obligations and court orders and adopted a concise rule limiting sanctions for losses resulting from the "routine, good faith" operation of an information system unless "exceptional circumstances" exist.[76] The intention expressed at the meeting was to use "good faith" as a culpability excluder which would operate midway between denial of exemption for merely negligent conduct and one which would require proof of willful or reckless conduct.[77]

¶33 The Committee Note to Rule 37(f) was also shortened, thus deleting the three-part analysis of preservation obligations. New language was added to clarify that "[a] party's identification of sources of electronically stored information as not reasonably accessible does not relieve the party of its common-law or statutory duties to preserve evidence."[78] Finally, the affirmative role of good faith in determining how a party should react to those preservation obligations was added.[79]

¶34 After some further minor modifications,[80] the amended Rule 37(f) was submitted to and approved by the Standing Committee at its June 15-16, 2005 Meeting[81] in its final form.[82]

IV. CRITICISMS

A. Limited Effectiveness

¶35 Some have questioned whether Rule 37(f) was worth the effort. For example, in his survey piece in the Spring Issue of this Journal, Ken Withers argues that

---

the proposed rule [Rule 37(f)] would insulate routine destruction of information on sources a party identifies as not reasonably accessible, the Notes to both Rules 37(f) and 26(b)(2) have been revised to make clear that there is no necessary linkage between these rules.").

[76] The revised version of Rule 37(f), based on the alternative form proposed earlier, was proposed near the close of the meeting and adopted by a 9-2 vote in order to "recouple" the amendment to the rules package. As revised, Rule 37(f) 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 solely as a result of the routine, good-faith operation of the party's electronic information system." *See* Advisory Committee Minutes (April 2005), *supra* note 7, at 43.

[77] *See* STANDING COMMITTEE REPORT (2005), *supra* note 12, at Rules App. C-85.

[78] *Id.*

[79] "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." *Id.* at C-87. The Note also points out that "good faith" may require active intervention in the routine operation of some systems to prevent the loss of information as part of a "litigation hold." *Id.*

[80] *See* ADVISORY COMMITTEE REPORT (2005), *supra* note 12, at 86. The phrase "solely" was deleted and the reference to "an" electronic information system was substituted for "the party's" information system.

[81] *See* Minutes, Standing Committee Meeting (June 15-16, 2005), at 26-29.

[82] For a pithy comparison between the August 2004 version of Rule 37(f) and the final form of Rule 37(f) - and an explanation for the changes - see "Changes Made After Publication and Comment," part of the Standing Committee Report at Rules App. C-88-89. No comparable comparison exists to guide analysis of the changes in the Committee Notes (other than by physically comparing the Note reproduced in the Advisory Committee Report (2004) with the Note reproduced in the Standing Committee Report (2005).

the final Rule, with its qualifications, is ineffective and unnecessary."[83] In a variation on that theme, another recent article criticizes Rule 37(f) for not providing sufficient "bright line" preservation guidelines, especially in regard to inaccessible information.[84] The authors of that article contend that proposed Rule 37(f) will have "little, if any, practical impact" because courts "will continue to have significant discretion to impose sanctions for a 'wrong guess' as to the precise moment when a litigation hold should be implemented."[85] Others argue that Rule 37(f) is too limited in its application.[86]

¶36 These criticisms prompt several responses. First, it is certainly true that Rule 37(f) differs from the initial proposals which contemplated intervention to require suspension of routine operations of information systems only when and if a court ordered them for good cause.[87] In this regard, the original proposals were more akin to the safe harbor in the Private Securities Litigation Reform Act of 1995 (the "Reform Act") which provides (as one alternative) an exemption from civil liability for forward-looking statements accompanied by appropriate cautionary language.[88] This approach was ultimately rejected because of a concern it would lead to excessive resort to preservation orders.[89] Accordingly, the more flexible but less predictable approach based on retrospective "good faith" standard for preservation efforts was substituted by Advisory Committee.

¶37 It can be argued that the Committee approach is far more practical than the original suggestion. Rule 37(f) is not tied to any particular technology or any particular set of preservation practices.[90] New fact patterns will continue to evolve and Rule 37(f)

---

[83] Withers, *supra* note 4, at 208. Withers argues that Rule 37(f) "bears little resemblance to the model rule advocated by corporate defense attorneys early in the Advisory Committee's five year study of electronic discovery." *Id.* at 207. Withers calls the earlier proposals "a solution in search of a problem" because there was "no evidence that 'case killer' sanctions had ever been levied by a federal judge without a finding, express or implied, of gross negligence or intentional destruction. *Id.* at 207-8. He views current Rule 37(f) as not a safe harbor rule at all, but "more a framework for analysis, restating the law of sanctions in the spoliation context." *Id.* at 207. With his emphasis only on reported decisions, not on the fear of such sanctions that actually motivates parties to avoid risking decisions, Withers falls into the same trap as others who have not had the responsibility for planning and implementation of preservation steps in the face of massive ESI demands.

[84] *See* Nelson & Rosenberg, *supra* note 2, at ¶ 55 (only practical effect is to encourage general use of electronic document retention systems).

[85] *Id.*

[86] For example, one article contends that the proposed rule would protect a corporation from sanctions for inadvertently permitting a backup tape to be automatically overwritten, but not for failing to prevent employees from deleting relevant emails under similar circumstances. *See* Elaine Ki Jin Kim, *The New Electronic Discovery Rules: A Place for Employee Privacy*, 115 YALE L.J. 1481 (2006) (citing no authority for conclusion).

[87] *See* Allman, *supra* note *, at 209 (suggesting a limitation in Rule 34 on the need to suspend or alter "the operation in good faith of disaster recovery or other electronic or computer systems absent court order issued upon good cause shown").

[88] *See* 15 U.S.C. §§ 77z-2(c)(1)(A), 78u-5(c)(1)(A). *See* In re Theragenics Corp. Sec. Litig., 105 F. Supp. 2d 1342, 1352-59 (N.D. Ga. 2000) (enacted because "sizeable bipartisan majorities of both houses of Congress became persuaded that the private securities litigation system was seriously out of balance").

[89] *See* Thomas Allman, *The Proposed Federal E-Discovery Rules*, SL088 ALI-ABA 105, 116 (2006) (the Advisory Committee did not couple a mandatory discussion of preservation issues with a default provision regarding preservation orders because of concern for premature issuance of preservation orders).

[90] As, for example, the suggestion that saving a single day's total volume of data generated by an enterprise for each lawsuit filed should be made a prerequisite to asserting a preservation safe harbor. In point of fact, of course, such a rigid and impractical requirement would simply require that all information be saved forever given the volume of ongoing litigation typically encountered.

will be available for use in circumstances where it is clear that reasonable efforts were made but losses to discovery nonetheless occurred. Courts will now have the flexibility to identify losses due to "routine, good faith" operations with the help of the *Sedona Principles*, especially Principles 5,[91] 9,[92] 11[93] and 12.[94] Additional help is on the way from that quarter.[95] Moreover, because the outcome of any particular challenge to preservation practices cannot be predicted, a premium will be placed on the development and implementation of good faith policies and practices..

¶38 Seen from this perspective, therefore, Rule 37(f) is analogous to the alternative version of the safe harbor under the Private Securities Act (and the equivalent SEC Rule) which provides exemption from liability for forward looking statements that are made in "good faith" on the basis of reasonable assumptions.[96]

¶39 To some, the approach in Rule 37(f) suggests a return to the "pre-*Zubulake*" era, in which a number of courts recognized a broad duty to preserve back-up tapes without considering any limitations on g preservation obligations.[97] This is clearly a misreading of the impact of the amendments in general and Rule 37(f) in particular.

¶40 For example, when a producing party is faced with making plans for pre-discovery preservation, the focus on accessibility of information set forth in Rule 26(b)(2) is far from neutral in its impact. The clear intention of the Advisory Committee in adopting Rule 37(f) was that inaccessible sources of information need not be preserved when the party has a reasonable belief in the inaccessibility of the source and in the availability of the relevant information on active systems and when the party is acting in good faith.[98] If decisions are challenged by a motion for sanctions, the test of under Rule

---

[91] "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." *Sedona Principles*, *supra* note 46, Sedona Principle 5.

[92] "Absent a showing of special need and relevance a responding party should not be required to preserve, review, or produce deleted, shadowed, fragmented or residual data or documents." *Sedona Principles*, *supra* note 46, Sedona Principle 9.

[93] "A responding party may satisfy its good faith obligation to preserve and produce potentially responsive electronic data and documents by using electronic tools and processes, such as data sampling, search, or the use of selection criteria, to identify data most likely to contain responsive information." *Sedona Principles*, *supra* note 46, Sedona Principle 11.

[94] "Unless it is material to resolving the dispute, there is no obligation to preserve and produce metadata absent agreement of the parties or order of the court." *Sedona Principles*, *supra* note 46, Sedona Principle 12.

[95] As of this writing, two Sedona Commentaries, one on email management and one on litigation holds are nearing completion and should be issued for public review and comment by the end of 2006.

[96] *See* 17 CFR § 240.3b-6 (identical to Rule 175 of the Securities Act of 1933, 17 CFR §230.175).

[97] *See* Nelson & Rosenberg, *supra* note 2, at ¶ 50 (Rule 37(f) threatens to undermine the *Zubulake* holding that duty of preservation extended only to backup tapes of "key players" containing otherwise unavailable data). It is not clear, however, just how useful that observation may be from a planning point of view. *See* Eric Friedberg, *To Recycle or Not to Recycle, That is the Hot Backup Tape Question*, 201 PLI/Crim 205 (2005) ("Judge Scheindlin fashioned an exception [in *Zubulake*] that swallows much of this rule").

[98] The original Committee Note explaining the "two-tier" rule provided that "[i]n most instances, a party acts reasonably by identifying and preserving reasonably accessible electronically stored information that is discoverable without court order." ADVISORY COMMITTEE REPORT (2004), *supra* note 25, at 34. Although that language was not included in the final Committee Note, the primary reason was that the Advisory Committee did not wish to imply that there were no circumstances where otherwise inaccessible sources of information did not need to be preserved. STANDING COMMITTEE REPORT (2005), *supra* note 12, at Rules App. C-44. As a general proposition, however, the original observation remains valid.

37(f) should be whether the preservation process adopted and followed was "reasonably calculated" to achieve an appropriate result.[99]

¶41 Moreover, once discovery commences, the mandatory requirement in Rule 26(f) of early discussion and resolution of identified preservation issues - a first for the Federal Rules - clearly requires affirmative action by the requesting party with knowledge of preservation steps undertaken. The producing party has the responsibility under Rule 26(b)(2)(B) to identify the sources of potentially responsive information which it does not intend to search or use for production. An unsatisfied requesting party seeking information must seek an appropriate order[100] or waive the right to seek sanctions later for non-production.[101]

¶42 Finally, the failure of individual users to perfectly comply with vague litigation hold instructions is entitled to protection under Rule 37(f). Delivery of a litigation hold notice under reasonable conditions should operate as a rebuttable presumption that appropriate steps were undertaken and that any loss despite that notice fits within the safe harbor.[102]

B. Inherent Power to Sanction

¶43 A major criticism of Rule 37(f)[103] is that it addresses only sanctions under the federal rules, which generally do not apply prior to commencement of litigation.[104] Indeed, one Commentator refers to Rule 37(f) as providing only a form of "false harbor"

---

[99] Sedona Principle 5, *supra* note 91. *See also* STANDING COMMITTEE REPORT (2005), *supra* note 12, at Rules App. C-83 ("It can be difficult to interrupt the routine operation of computer systems to isolate and preserve discrete parts of the information they overwrite, delete, or update on an ongoing basis, without creating problems for the larger system. It is unrealistic to expect parties to stop such routine operation of their computer systems as soon as they anticipate litigation. It is also undesirable; the result would be even greater accommodation of duplicative and irrelevant data that must be review, making discovery more expensive and time-consuming.").

[100] A requesting party may and should seek an order compelling discovery to raise the issue of whether the information must be preserved until discoverability is resolved. *See* STANDING COMMITTEE REPORT (2005), *supra* note 12, at Rules App. C-43 (noting that producing party may also raise the issue affirmatively by a motion for a protective order).

[101] *See, e.g.*, Applied Telematics v. Sprint Commc'ns Co., No. Civ.A. 94-46031996 WL 33405972 (E.D. Pa. 1996) (refusing adverse inference instruction because "plaintiff failed to pursue" other sources to obtain the information after learning of its unavailability); *see also* Treppel v. Biovail, 233 F.R.D. 363 (S.D.N.Y. 2006) (Francis, M.J.) (refusal by requesting party to agree on search methodology was based on "a misconception" of the scope of discovery obligations and "a missed opportunity").

[102] Implementation of a reasonable "litigation hold" process should be seen as a reason shift the burden of proof to a party seeking sanctions. *See* Anita Ramasastry, *The Proposed Federal E-Discovery Rules: While Trying to Add Clarity, the Rules Still leave Uncertainty*, FindLaw's Writ (Sept. 14, 2004), http://writ.news.findlaw.com/ramasastry/20040915.html ("If a party took reasonable steps to notify the custodian of electronic information at the company of the need to preserve certain information, it should be deemed to have made out a prima facie – that is, an initial, though rebuttable – case that it fits within the safe harbor.").

[103] I do not accept as serious the argument that Rule 37(f) will somehow mislead federal and state courts to the position that no preservation obligations exist until after a civil action is filed. *See* Stephen Herman, *ATLA Annual Convention Reference Materials, Proposed Federal Rule Changes on E-Discovery*, 2 Ann.2005 ATLA-CLE 1959 (2005) (reproducing letter of January 19, 2005 to Advisory Committee). No minimally informed litigator or court could possible believe that the Advisory Committee intended such a result.

[104] *See* David Isom, *Electronic Discovery Primer for Judges*, 2005 FED. CTS. L. REV. 1 (2005) (arguing that the initial draft of the safe harbor rule would have only very limited impact because it does not "abridge" the power of a court to act outside the rules).

because courts are likely to ignore Rule 37(f) and apply their inherent power to sanction.[105]

¶44 Courts often cite their inherent powers to sanction when it is unclear that rule-based sanction authority exists.[106] Such authority is generally found in Rule 37(b)(2), which applies when a party fails to obey a discovery order or in Rule 37(c), which applies to a failure to make initial disclosures under Rule 26(a)(1) or to supplement or amend previous discovery.

¶45 However, it is unlikely that courts will deliberately invoke their inherent power in order to reach a different result on the same facts as would exist under Rule 37(f). Most courts understand that the limitation to the "rule-based" qualification was not based on anything other than the fact that the Advisory Committee and Standing Committee were simply respectful of the limits of rulemaking power.[107] Accordingly, the natural tendency of most courts will be to use Rule 37(f) as a "guidepost" or reference point in exercising their inherent powers. The power to sanction pre-litigation conduct is subject to the Supreme Court's admonition in *Chambers v. Nasco* that courts should act with great care and only when the Rules "are not up to the task."[108]

¶46 A respect for carefully drafted Rule limitations in the face of more expansive inherent power is not unknown. For example, in the case of *Brandt v. Vulcan, Inc.*, the Seventh Circuit refused to suggest that a court should exercise its inherent powers to sanction discovery misconduct where the District Court had concluded that it lacked power to do so because of limitations under Rule 37(b)(2).[109] And in *Convolve Inc. v. Compaq Computer Corp.*, Magistrate Judge Francis relied upon the intitial version of proposed Rule 37(f) in absolving a party of the failure to undertake to preserve certain "ephemeral" information in the absence of a discovery order.[110]

C. Policy Impact

¶47 A number of recent articles castigate Rule 37(f) as encouraging improper or illegal corporate conduct. A recent Student Note, for example, asserts that Rule 37(f) will "eliminate the possibility of judicial sanctions when parties evade discovery requests" because parties can "destroy potentially incriminating documents using a

---

[105] Henry Noyes, *Is E-Discovery So Different That it Requires New Discovery Rules? An Analysis of Proposed Amendments to the Federal Rules of Civil Procedure*, 71 TENN. L. REV. 585, 652 (2004) (discussing original version of Rule 37(f)).

[106] *See, e.g.*, Mosaid Techs. Inc. v. Samsung Elecs. Co., 348 F. Supp. 2d 332 (D.N.J 2004) (failure to institute a litigation hold). *See* Iain Johnston, *Federal Courts Authority to Impose Sanctions for Prelitigation or Preorder Spoliation of Evidence*, 156 F.R.D. 313 (1994) ("the two main sources for remedying acts of spoliation are Federal Rule of Civil Procedure 37 and the courts' inherent authority to sanction").

[107] As early as its October, 2003 meeting, the Advisory Committee had been concerned about its authority to promulgate a preservation rule that applied prior to commencement of litigation under the Rules Enabling Act, 28 U.S.C. §§ 2071-2077. *See* Minutes, Civil Rules Advisory Committee Meeting (Oct. 2-3, 2003), at 37 (preservation guidance may be beyond the "proper scope" of the Enabling Act).

[108] 501 U.S. 32, 50 (1991).

[109] 30 F.3d 752, 756 n.9 (7th Cir. 1994). The Seventh Circuit admitted that the lower court had the authority to act under its inherent authority to sanction parties for discovery abuse but refused to find an abuse of discretion despite the "troubling" actions highlighted below.

[110] 223 F.R.D. 162, 177 (S.D.NY. 2004).

document retention policy."[111] Further, since "the rules are biased in favor of big companies," they will "make their electronic document storage system as inaccessible as possible."[112] Other articles predict that Rule 37(f) will cause "corporations" to "adopt comprehensive data deletion" based on "purported" good-faith desire to reduce data storage costs[113] because "[the] subversion of document retention policies is shared by many in corporations across America."[114]

¶48 This type of *ad hominem* attack on private corporations is quite unfair. First, it ignores the fact that public entities have been equally strong in their support for a preservation safe harbor.[115] Second, it also ignores the ample civil and criminal sanctions applicable to those who might decide to act in to avoid their obligations in discovery. As the Standing Committee Report noted in response to an analogous argument about Rule 26(b)(2)(B), "a party that makes information "inaccessible" because it is likely to be discoverable in litigation is subject to sanctions now and would still be subject to sanctions under the proposed rule changes."[116]

¶49 Generally speaking, an entity has the right to manage and dispose of its information. *See The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age* (Sedona Conference Working Group Series, September 2005), *Guideline* 3: "An organization need not retain all electronic information ever generated or received." Indeed, the Supreme Court endorsed this principle in *Arthur Andersen LLP v. United States*.[117]

¶50 However, corporate policies involving destruction of information sought in discovery must be both reasonable in purpose and reasonable as applied in a particular case.[118] It is not, for example, reasonable to institute a policy to intentionally destroy information for the primary purpose of preventing a known future adversary from obtaining the information in litigation. *See, e.g.*, *Rambus, Inc. v. Infineon Technologies*, 220 F.R.D. 264, 286 (E.D. Va. 2004) ("[E]ven valid purging programs need to be put on hold when litigation is reasonably foreseeable").[119]

¶51 Moreover, criminal sanctions may be implicated by deliberate attempts to withhold information in anticipation of certain types of proceedings. For example, in the

---

[111] Rebecca Rockwood, *Shifting Burdens and Concealing Electronic Evidence: Discovery in the Digital Era*, 12 RICH. J.L. & TECH. 16, at ¶ 28 (2005).

[112] *Id.*

[113] Daniel Garrie et al., *Hiding the Inaccessible Truth: Amending The Federal Rules to Accommodate Electronic Discovery*, 25 REV. LITIG. 115, 128 (Winter 2006).

[114] Lloyd van Oostenrijk, *Paper or Plastic?: Electronic Discovery and Spoliation In The Digital Age*, 42 HOUS. L. REV. 1163, 1185 (2005).

[115] Withers astutely notes that the proposal for a safe harbor "was grounded in the fear of many in corporate America (and in the government sector) that electronic information systems were far too large and complex to manage with the degree of certainty needed to fulfill the duty of preservation, and that no party should face sanctions arising out of circumstances beyond their control." *See* Withers, *supra* note 4, at 207.

[116] STANDING COMMITTEE REPORT (2005), *supra* note 12, at Rules App. C-45.

[117] 544 U.S. 696, 704 (2005) (Document retention policies are "common in business" and may be used to explain - and justify - the loss of information in appropriate circumstances.).

[118] *See* Stevenson v. Union Pac. R.R. Co., 354 F. 3d 739, 747-48 (8th Cir. 2004) (upholding sanctions for destruction of voice tape pursuant to retention policy).

[119] *Compare* Hynix Semiconductor Inc. v. Rambus Inc., No. C-00-20905 RMW, 2006 WL 565893 (N.D. Cal.) *with* Samsung Elecs. Co. v. Rambus, Inc., No. Civ.A. 3:05CV406, 2006 WL 2038417 (E.D. Va.) (involving same course of conduct but with differing interpretations of the corporate motives involved).

wake of the Enron scandal, Congress stiffened existing criminal penalties and added new violations for one who knowingly alters or destroys documents with the intent to impede a federal investigation or proceeding or "in relation to or contemplation of such matter or case."[120]

D. Disincentive to Invest

¶52 Nathan Drew Larsen argues that by focusing on losses which result from "routine" operations the Advisory Committee has inadvertently created an incentive in Rule 37(f) for producing parties to fail to invest in technology which is less destructive of data.[121]

¶53 This argument is a variation of the contention that Rule 37(f) will encourage producing parties to place information into inaccessible sources to avoid preservation and production obligations and is equally fallacious. It ignores the fact that the moving force in information technology is not litigation but business concerns.[122] As the Standing Committee Report notes: "[M]any witnesses and comments [at the Public Hearings] rejected the argument that the rule would encourage entities or individuals to "bury" information that is necessary or useful for business purposes or that regulations or statutes require them to retain."[123] Moreover, the argument overstates the intended purpose of that phrase. A "routine" operation is merely part of process.[124] Its use in Rule 37(f) is not intended to freeze technological innovation but merely to indicate that the feature causing the loss is typically part of the system at that time.[125]

---

[120] 18 U.S.C. § 1519 (2002). As one in-house lawyer testified at the Public Hearing of January 12, 2005, "I think it would be insanity beyond belief for anybody, any serious lawyer, to advise their client that, oh, yeah, this is a way to get rid of something that might come back to bite us. Because the moment you have that thought you're engaging in basically criminal conduct." Public Hearing Comments, *supra* note 8, Testimony of Greg McCurdy (Jan. 12, 2005) (04-CV-001), at 10.

[121] Larsen, *supra* note 6, at 226. The author also argues that a "routine" operation is synonymous with one which is "customary," as judged by the practice of other entities, which could create an incentive for industry to collude "either explicitly or tacitly" to reduce litigation risk by configuring their systems in a manner more destructive of data. *Id.*

[122] The General Counsel of Intel Corporation testified at the San Francisco Public Hearing that while it would be feasible to recast backup media into a method that would be more searchable, there would be no reason for that to be done from a business sense since backup tapes perform their function well. Public Hearing Comments, *supra* note 8, Testimony of Bruce Sewell (Jan. 12, 2005) (004-CV-016), at 16 ("[F]rankly, I have enough grief within my job [just] trying to manage [the legal] business").

[123] STANDING COMMITTEE REPORT (2005), *supra* note 12, at Rules App. C-44 to -45.

[124] An example of such useage is when spoliation sanctions are not imposed for destruction of information pursuant to a document retention policy which occurs "[as] a matter of *routine* with no fraudulent intent." Lewy v. Remington Arms Co., 836 F.2d 1104, 1112 (8th Cir. 1988) (emphasis added) (quoting *Gumbs v. Int'l Harvester, Inc.*, 718 F.2d 88, 96 (3rd Cir. 1983)).

[125] Prof. Redish argued in 2003 that a safe harbor's viability should be tested by comparing it to industry practice "and the reach of currently available technology." Letter from Martin Redish, Professor of Law, to Lee Rosenthal, Judge (Dec. 8, 2004), *available at* http://www.kenwithers.com/rulemaking/civilrules/ed52.pdf. He contended that a litigant should not be permitted to adopt an "unnecessarily aggressive document destruction policy." *Id.* This would appear to impose conditions beyond that adopted by the Advisory Committee in Rule 37(f), which is both technology neutral and properly takes no position on what level of investment is required. The Redish proposal, however, was based on requiring only a "reasonable" program for destruction of information and lacked the requirement that the program be operated in "good faith" as is now present in Rule 37(f). That requirement provides additional and sufficient protection from the concern about improper motive raised by Prof. Redish.

E. Vague Standard

¶54 The "good faith" standard of Rule 37(f) has also been criticized as too vague because parties will "continue to be subject to varying standards for determining when sanctions should be imposed."[126]

¶55 There is, of course, some truth to that observation. However, Courts are often called upon to apply standards involving an assessment of "good faith" to determine exemptions from liability[127] or to assess rights and obligations.[128]

¶56 In applying Rule 37(f) on a case-specific basis,[129] Courts will be employing the classic "excluder" function attributed to Professor Robert Summers.[130] Under this astute observation, "good faith" has no inherent meaning, but serves to exclude examples of bad faith conduct, which are identified on an ad hoc basis over time. For example, as the Committee Note makes clear, willful continuance of an operation involving destruction when preservation obligations are known are to be excluded from being treated as a "routine, good faith" operation of that system.[131] In Mosaid Technologies v. Samsung Electronics, for example, the producing party made no attempt to justify its failure to modify the automatic deletion of e-mail for several years, thereby making it impossible to produce any of the technical email needed in the patent litigation. The destruction in that case was neither routine nor in good faith.[132]

¶57 Assessing losses against a "good faith" standard presents a subjective issue, which may vary from case to case, since the personnel involved "may well have been

---

[126] Van Oostenrijk, *supra* note 114, at 1201 (questioning whether a line can be drawn between negligent and reckless or intentional conduct and whether the difference rally matters).

[127] Examples include the Delaware Business Judgment Rule and the alternative safe harbor under the Private Securities and Rule 3b-6 of the Securities Act of 1934 under which a safe harbor from liability can only be defeated by proof of actual knowledge of the false or misleading nature of a forward-looking statement subject to the rule. *See* 1 PRINCIPLES OF CORP. GOVERNANCE § 4.01, Amer. Law Inst. (1994) ("a director or officer who makes a business judgment in good faith fulfills [his duty to perform his functions in good faith] if the director or officer… (3) rationally believes that the business judgment is in the best interests of the corporation"); Eric Freidman, *Changing Currents for Directors' Duties*, CORPORATE LAW AND PRACTICE, Practicing Law Inst. (2005) (the business judgment rule provides exculpation from personal liability for bad business decisions).

[128] *See* Bunge Corp. v. Recker, 519 F.2d 449, 452 (8th Cir. 1975) (a lack of "good faith" in administering contract involves actions "not prompted by an honest mistake but rather by some interested or sinister motive"). *See generally* Gerard Mantese, *The UCC and Keeping the (Good) Faith*, 70 MICH. BUS. L.J. 270 (1991).

[129] *See* Reilly v. Natwest Martkets Groups, Inc., 181 F. 3d 253, 267 (2d Cir. 1999), *cert. denied*, 528 U.S. 1119 (2000).

[130] *See* Robert Summers, *'Good Faith' in General Contract Law and the Sales Provisions of the Uniform Commercial Code*, 54 VA. L. REV. 195 (1968). *See also* Robert Summers, *The General Duty of Good Faith – Its Recognition and Conceptualization*, 67 CORNELL L. REV. 810 (1982) (summarizing developments in the ensuing period and clarifying the meaning of "good faith" in a variety of contexts).

[131] It is clear that a party may not "exploit" a routine operation "in order to destroy specific stored information that it is required to preserve." STANDING COMMITTEE REPORT (2005), *supra* note 12, at Rules App. C-87 (The Committee Note points out that "good faith" may require active intervention in the routine operation of some inaccessible sources of information as part of a "litigation hold.").

[132] Mosaid Technologies v. Samsung Electronics, 348 F. Supp. 2d 332 (D.N.J. 2004). *See also* Computer Assoc. Int'l, Inc. v. Am. Fundware, Inc., 133 F.R.D. 166, 169 (D. Colo. 1990) (the Court determined that a producing party acted willfully when it destroyed a copy of a source code it knew would be the subject of a discovery request and therefore the destruction "could not be excused as a bona fide business practice").

guided by different mental states."[133] For example, a typical email management policy[134] requires that users identify and save email and attachments that meet business, regulatory or other criteria and delete the rest. Much as paper records are thrown away by employees making judgment calls about the necessity of retaining information and automatic deletion is often used to enforce the policy. This avoids the need for excessive storage and unnecessary review during discovery and also reduces the risk of inadvertent production of privileged information.

¶58 Thus, if information is lost by user or automatic action, the "good faith" criterion will help distinguish among those situations where sanctions should be applied and those where they should not.[135] There will be examples of lax or negligent oversight which may still qualify as "good faith."[136]

¶59 The practice of recycling backup media presents a similar issue. These sources of ESI are not generally used for ongoing business purposes and can be difficult and costly to access.[137] Under some circumstances, a duty may exist to suspend their recycling and preserve them for potential discovery.[138] However, due to the complexity

---

[133] Morris v. Union Pac. R.R., 373 F. 3d 896, 903 (8th Cir. 2004) ("[V]ariances in key personnel, nuances in fact situations or even different credibility assessments of identical evidence can lead to varying conclusions about the formation of a corporate intent.").

[134] There is an important distinction between obligations adopted as a matter of policy to retain information because of business or regulatory requirements and the duty to preserve information for discovery in litigation. Most preservation obligations arise as a necessary implication of the common-law of sanctions and relate to the need to preserve information for trial. *See* Silvestri v. General Motors Corp., 271 F.3d 583 (4th Cir. 2001). However, retention policies can involve literally thousands of regulatory requirements also which require that entities act to retain information in addition to those which business requirements require. Only a few of the underlying regulatory requirements expressly or automatically mandate or create preservation obligations enforceable by the law of sanctions in litigation. *See* Byrnie v. Town of Cromwell Bd. of Educ., 243 F.3d 93, 109 (2d Cir. 2001) (for a preservation obligation to attach, "the party seeking the inference must be a member of the general class that the regulatory agency sought to protect in promulgating the rule").

[135] For example, deletion of information may occur despite a duty to preserve but not prevent its recovery from other sources. *See* Se. Med. Supply, Inc. v. Boyles, Moak & Brickell Ins., Inc., 822 So. 2d. 323 (Miss. Ct. App. 2002), where computer files were destroyed pursuant to a routine business procedure "in good faith" and without any prejudice to the case. Deletion of information pursuant to policy, but without notice to opposing counsel after institution of litigation, might qualify if done without intention to interfere with the litigation. *Compare* ABC Home Health Serv., Inc. v. IBM, Corp., 158 F.R.D. 180 (S.D. Ga. 1994) (applying an adverse inference instruction regarding lost files despite the fact that the requesting party never complained about their loss, important files in controversy were not deleted and the court did not find intentional deletion).

[136] *See, e.g.*, DaimlerChrysler Motors v. Bill Davis Racing, No. Civ.A. 03-72265, 2005 WL 3502172 (E.D. Mich.) (failure to prevent automatic deletion of email was merely negligent and not willful).

[137] *See* Public Hearing Comments, Testimony of Ed Amdahl (Feb. 14, 2005) (04-CV-241), at 2 (noting that daily back-ups to tape are made in order to have disaster recovery capabilities, that they are not accessed in the ordinary course of business and that approximately 100 tapes are taken offsite daily at a cost of $9,500 a day which, if not recycled, would cost in excess of $3.5M a year).

[138] While there is some authority suggesting that corporations need not routinely preserve backup tapes, exceptions posited to that rule render it ineffective as a planning principle. *See* Zubulake v. UBS Warburg, LLC, 220 F.R.D. 212, 217-18 (S.D.N.Y. 2003) ("*Zubulake IV*") (while a general obligation to keep all backup tapes would "cripple" a corporation, tapes containing information about "key players" should be kept if the information is not otherwise available). The net result, not surprisingly, is advice from many outside counsel to the effect that all recycling of backup tapes should be suspended upon the first hint of any meaningful litigation.

of the issue and without clear guidelines on when that duty is triggered, it is often difficult to consistently implement the duty to act.[139]

¶60 One compelling indicia of "good faith" will be if there is evidence that the loss occurred during an operation pursuant to a reasonable policy in the absence of improper motive. In this regard, Rule 37(f) reflects the existing law in a majority of Circuits, which hold that a court should not issue an adverse inference instruction unless there is an affirmative showing of intentional destruction amounting to "bad faith."[140] One recent article, otherwise critical of Rule 37(f), acknowledges that the Rule will authorize the "general use of electronic document retention systems."[141] To paraphrase Justice Stewart in another context, the advantage to Rule 37(f) is that courts will know "good faith" when they see it.[142]

V. CONCLUSION

¶61 Rule 37(f) represents a carefully considered policy judgment reconciling two sometimes competing policy considerations: the need for preservation of potentially responsive ESI for use in litigation and the need to minimize the unnecessary intrusion into productive use of the systems involved. Its impact is carefully targeted and depends upon court endorsement, which cannot be gamed in advance. Spoliation of potential evidence "occurs along a continuum of fault- ranging from innocence through the degrees of negligence to intentionality."[143] Rule 37(f) reflects a judgment that as to ESI lost through the routine operation of information system, only when fault lies along the higher ends of that spectrum are sanctions to be used.

Rule 37(f) should help to encourage public and private entities alike to act in good faith and undertake reasonable steps to accommodate preservation needs. Both requesting and producing parties have an interest in its effective use, which complements the other advances in the e-discovery amendments. It hopefully provides a template for those courts which face similar requests for sanctions under their inherent powers. As such, it more than meets the original intent of the proponents and should endure in its appropriate role for many years to come.

---

[139] *See* Keir v. Unumprovident Corp., No. 02 Civ. 8781(DLC), 2003 WL 21997747, *13 (S.D.N.Y. 2003) (despite good faith efforts to comply with a preservation order, the court nonetheless faced a situation where certain of the backup tapes supporting the 888 computer servers were "lost" due "to the fault of no one").

[140] *See* Morris v. Union Pac. R.R., 373 F. 3d 896, 901-3 (8th Cir. 2004) (reversing adverse inference jury instruction because of lack of intentional destruction on the part of claims agent). *Compare* Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d 99, 107-8 (2d Cir. 2002) (adverse inference sanctions can be available in the Second Circuit when ESI is lost as the result of merely negligent conduct). Rule 37(f) clearly supersedes that holding in the limited situation where a loss of ESI results from the routine, good faith operation of an information system.

[141] Nelson & Rosenberg, *supra* note 2, at ¶ 49.

[142] Responsible producing parties generally "get it." The author argued at the Fordham Conference that "it is my impression [from] talking with many corporate executives from different companies that they now all understand their preservation obligations. The real test ought to be whether or not in good faith they have attempted to meet those obligations." *Panel Discussions*, *supra* note 57, at 76.

[143] Welsh v. United States, 844 F. 2d 1239, 1246 (6th Cir. 1988).