

2010

Sea Change or Status Quo: Has the Rule 37(e) Safe Harbor Advanced Best Practices for Records Management?

Philip J. Favro

Follow this and additional works at: <https://scholarship.law.umn.edu/mjlst>

Recommended Citation

Philip J. Favro, *Sea Change or Status Quo: Has the Rule 37(e) Safe Harbor Advanced Best Practices for Records Management?*, 11 MINN. J.L. SCI. & TECH. 317 (2010).

Available at: <https://scholarship.law.umn.edu/mjlst/vol11/iss1/12>

Sea Change or Status Quo: Has the Rule 37(e) Safe Harbor Advanced Best Practices for Records Management?

Philip J. Favro*

“Is this maybe just hopeful thinking? Are we perhaps coming to a point where litigation requirements and business practices and best practices can become one and the same?”

—Judge James D. Walker, Jr., Public Comment on Proposed Changes to the Federal Rules of Civil Procedure, 2005.

I. Introduction	318
II. Rule 37(e)—Promoting Best Practices for Records Management in Litigation	321
A. Background Giving Rise to Rule 37(e)	321
1. No Duty to Preserve All Electronically Stored Information	322
2. Relevant Information to Be Retained after Duty to Preserve Attaches	323
3. Limited Guidance from Pre-Rule 37(e) Decisions	323
B. Rule 37(e)’s Effort to Balance Corporate and Litigation Imperatives	325
1. A Limited Safe Harbor Protects Litigants from Excessive Preservation Obligations	325
2. The Safe Harbor Does Not Insulate Organizations from Reasonable Litigation Demands	326
3. The Safe Harbor Established an Intermediate Standard for Imposing Discovery Sanctions	328
C. A National Standard for Guiding Records	

© 2010 Philip J. Favro.

* Philip J. Favro is senior counsel with Packard, Packard & Johnson. Mr. Favro advises clients regarding government procurement practices, licensing and enforcing patent rights, and protocols for preserving electronic data.

	Management Decisions in Connection with Litigation.....	332
III.	Key Trends from Rule 37(e) Records Management Jurisprudence	332
	A. Records Management Strategy Must Consider Accountability to Third Parties.....	333
	B. The Good, the Bad, and the Ugly—Examples of Reasonable and Unreasonable Records Management Policies.....	334
	1. The Good— <i>Gippetti v. United Parcel Service, Inc.</i>	335
	2. The Bad— <i>Connor v. Sun Trust Bank</i>	336
	3. The Ugly— <i>Keithley v. Home Store.com</i>	338
	4. Reasonable Retention Policies Can Effectively Address Organizational Needs in Relation to Litigation Requirements	339
	C. Modifying Records Management Policies: Timing and Scope Are Everything	339
	1. Whether and What Aspects of a Retention Policy Require Modification	340
	2. Harmonizing Retention Practices and Litigation Imperatives Requires an Effective Management Team.....	341
IV.	Suggested Practices for Addressing Litigation Requirements in Connection with Records Management Protocols	342
	A. Timely Implement an Effective Retention Policy... ..	342
	B. Prepare for Lawsuits in Advance of Actual Litigation.....	343
	C. Closely Follow Records Management Practices	343
	D. Do Not Exclusively Rely on the Safe Harbor for Protection	344
V.	Conclusion.....	344

I. INTRODUCTION

Nothing surprises us anymore when it comes to the world of electronic discovery. Legion are the tales of over-reaching discovery requests, terabyte productions, and astronomical production costs. The 2006 amendments to the Federal Rules of Civil Procedure were supposed to change all that. After all, weren't the amended rules designed to streamline the discovery process, allowing parties to focus on substantive issues while

making discovery costs more reasonable?¹ Instead, it seems the rules have spawned more collateral discovery disputes than ever before about preservation and production issues. Is it any wonder that many are questioning whether the so-called ESI amendments² are living up to their billing?³

Despite the overall shortcomings of the amendments, one rule is helping to clarify preservation and production burdens for electronically stored information: Federal Rule of Civil Procedure 37(e).⁴ Rule 37(e) provides refuge from sanctions for spoliation of evidence when electronically stored information has been destroyed pursuant to the routine, good faith operation of an electronic information system.⁵ Put in layman's terms, litigants may avoid sanctions even though their computer servers delete e-mail and other electronic data according to the server's programmed operation.⁶ This so-called "Safe Harbor" is only available when the "routine operation" is carried out in "good faith" such that relevant data is retained after a preservation duty attaches.⁷

1. See COMM. ON RULES OF PRACTICE & PROCEDURE, JUDICIAL CONFERENCE OF THE U.S., SUMMARY OF THE REPORT OF THE JUDICIAL CONFERENCE COMMITTEE ON RULES OF PRACTICE AND PROCEDURE 22–24 *2005) [hereinafter REPORT] available at <http://www.uscourts.gov/rules/Reports/ST09-2005.pdf>.

2. FED. R. CIV. P. 34 advisory committee's note (2006 Amendment to subdivision (a)) (generally describing computer-generated material as "electronically stored information" or ESI).

3. See Mary Mack, *Total Revamp of Federal Rules of Civil Procedure?*, DISCOVERYRESOURCES.ORG, Apr. 9, 2005, <http://www.discoveryresources.org/library/case-law-and-rules/total-revamp-of-federal-rules-of-civil-procedure/>.

4. Originally enacted as Federal Rule of Civil Procedure 37(f), an overall restyling of the Federal Rules in December 2007 caused it to be re-numbered as Federal Rule of Civil Procedure 37(e). Compare FED. R. CIV. P. 37 advisory committee's note (2006 Amendment) (explaining the operation of the new ESI rule), with STEVEN BAICKER-MCKEE ET AL., FEDERAL CIVIL RULES HANDBOOK 2008 803 (2007) (explaining how the 2007 amendments renumbered the rules).

5. FED. R. CIV. P. 37(e); see *KCH Serv., Inc. v. Vanaire, Inc.*, No. 05-777-C, 2009 WL 2216601, at *1 (W.D. Ky. Jul. 22, 2009).

6. See *Columbia Pictures Indus. v. Bunnell*, No. CV 06-1093FMCJXC, 2007 WL 2080419, at *13–14 (C.D. Cal. May 29, 2007) (holding the Safe Harbor insulated defendants from sanctions despite their failure to retain data stored in the random access memory of their computers), *aff'd*, 245 F.R.D. 443 (C.D. Cal. 2007).

7. FED. R. CIV. P. 37 advisory committee's note (2006 Amendment); *Ripley v. District of Columbia*, No. 06-1705 (EGS), slip op. at 9 (D.D.C. Jul. 2, 2009) (holding Rule 37(e) would not shield defendants from monetary

As first proposed and enacted, the Safe Harbor was championed as a protection against absurd preservation obligations.⁸ The rule would allow “corporate America,” along with governments, universities, and others, to safely eliminate electronic materials that did not have business value.⁹ And this policy in turn would reduce operating costs associated with data retention.¹⁰ At the same time, organizations would maintain electronically stored information pertinent to litigation.¹¹

Now that Rule 37(e) has been in place for three years, it is worth examining whether the Safe Harbor has lived up to this billing. The transition from concept to rule has not been seamless.¹² The Safe Harbor has been subject to criticism from a number of attorneys and legal scholars.¹³ It has also caused some confusion with respect to when a party should suspend its computer system to preserve relevant information.¹⁴ On the other hand, the new rule and its progeny of case law have provided guidance to organizations in preparing records

sanctions given their failure to operate their e-mail system in good faith); *MeccaTech, Inc. v. Kiser*, No. 8:05CV570, 2008 WL 6010937, at *9 (D. Neb. Apr. 2, 2008) (finding that Rule 37(e) was not applicable given defendants’ intentional destruction or withholding of electronic data).

8. See COMM. ON RULES OF PRACTICE & PROCEDURE, JUDICIAL CONFERENCE OF THE U.S., PUBLIC HEARING ON PROPOSED AMENDMENTS TO THE FEDERAL RULES OF CIVIL PROCEDURE, 93–94, 147–48, 365–72 (Feb. 11, 2005) [hereinafter PUBLIC HEARING] available at <http://www.uscourts.gov/rules/e-discovery/CVHearingFeb2005.pdf>; Thomas Y. Allman, *The Case for a Preservation Safe Harbor in Requests for E-Discovery*, 70 DEF. COUNS. J. 417 (2003).

9. See PUBLIC HEARING, *supra* note 8, at 369–70; REPORT, *supra* note 1, at app. C-83.

10. See PUBLIC HEARING, *supra* note 8, at 369–70.

11. FED. R. CIV. P. 37 advisory committee’s note (2006 Amendment); *C.f. Gippetti v. United Parcel Serv., Inc.*, No. C07-00812 RMW (HRL), 2008 WL 3264483, at *2 (N.D. Cal. Aug. 6, 2008) (denying discovery sanctions where the defendant had no reason to think that certain information purged pursuant to a routine data destruction system was relevant to discovery).

12. See REPORT, *supra* note 1, at app. F-7–8 (listing pros and cons of adopting the new rule).

13. See *id.*; PUBLIC HEARING, *supra* note 8, at 25–26 (asking critical questions about the new rule); Daniel Renwick Hodgman, *A Port in the Storm?: The Problematic and Shallow Safe Harbor for Electronic Discovery*, 101 NW. U. L. REV. 259, 282 (2007) (expressing ambivalence about the adequacy of the Safe Harbor).

14. See *infra* Part II.B.2.

retention policies.¹⁵ While not causing a sea change, Rule 37(e) is moving records management beyond the status quo. Organizations are receiving guidance on how to bring their policies in line with litigation requirements.

This Article will consider these subjects in the following pages. Part II of this Article will delve into the background, text and purpose of the Safe Harbor as they relate to document management and preservation. It will also describe the intermediate standard for imposing sanctions that was crafted in connection with Rule 37(e). Part III will review key case law that has evolved since the implementation of Rule 37(e). It will additionally detail some best practices for records management derived from those decisions. In Part IV, this Article will describe some suggestions that litigants may follow to implement these best practices.

II. RULE 37(e)—PROMOTING BEST PRACTICES FOR RECORDS MANAGEMENT IN LITIGATION

To understand why Rule 37(e) is helping companies with their document management efforts, it is worth exploring the background of the rule itself, along with its text and the corresponding Advisory Committee Note. This part will analyze why cases issued before the promulgation of Rule 37(e) were limited in their capacity to develop cogent e-discovery principles. It will also show that only a uniform national standard could provide needed clarity so litigants could confidently implement document retention protocols.

A. BACKGROUND GIVING RISE TO RULE 37(e)

The Safe Harbor has its origins in case law that began to develop in the mid-to late-1990s as e-mail and other electronic information became ubiquitous.¹⁶ Decisions issued by scattered jurisdictions in the ensuing years described parties' preservation obligations with respect to computer data. The reasoning from those decisions seemed to provide guidance on

15. See *infra* Part III.

16. The principles regarding preservation inherent in Rule 37(e) may be traced back to analogous decisions addressing productions of paper documents. See, e.g., *Kozlowski v. Sears, Roebuck & Co.*, 73 F.R.D. 73 (D. Mass. 1976) (affirming default judgment sanction for defendant's refusal to address its problematic document retention system).

which litigants—particularly organizations generating large amounts of data—could rely to develop reasonable retention policies.

1. No Duty to Preserve All Electronically Stored Information

In *Concord Boat Corp. v. Brunswick Corp.*, it was held that companies had no duty to preserve all of their e-mail communications.¹⁷ Keeping every single e-mail could not be a workable standard, even if all such e-mail was arguably pertinent to future litigation.¹⁸ Such a burden would expose litigants to cost prohibitive and impractical preservation requirements.¹⁹ Similar logic is found in *Zubulake v. UBS Warburg LLC*, which reasoned that an organization's operations would be "crippled" if it were forced to retain all of its paper and electronic data.²⁰

This view also found support in professional journals²¹ and academic scholarship²² published before the enactment of Rule 37(e).²³ Given the burdens associated with data preservation, it was even posited that relevant data should not be preserved until the issuance of an applicable discovery order.²⁴

17. *Concord Boat Corp. v. Brunswick Corp.*, No. LR-C-95-781, 1997 WL 33352759, at *4–5 (E.D. Ark. Aug. 29, 1997).

18. *Id.* at *4.

19. *Id.* at *5.

20. *Zubulake v. UBS Warburg LLC (Zubulake IV)*, 220 F.R.D. 212, 217 (S.D.N.Y. 2003); see also *Wiginton v. CB Richard Ellis*, No. 02 C 6832, 2003 WL 22439865, at *4 (N.D. Ill. Oct. 27, 2003) ("A party does not have to go to 'extraordinary measures' to preserve all potential evidence . . . [i]t does not have to preserve every single scrap of paper in its business.") (citing *China Ocean Shipping (Group) Co. v. Simone Metals Inc.*, No. 97 C 2694, 1999 WL 966443, at *3 (N.D. Ill. Sept. 30, 1999) and *Danis v. USN Commc'ns, Inc.*, No. 98 C 7482, 2000 WL 1694325, at *32 (N.D. Ill. Oct. 20, 2000)).

21. See e.g., SEDONA CONFERENCE WORKING GROUP ON BEST PRACTICES FOR ELECTRONIC DOCUMENT RETENTION & PRODUCTION, THE SEDONA PRINCIPLES: BEST PRACTICES RECOMMENDATIONS & PRINCIPLES FOR ADDRESSING ELECTRONIC DOCUMENT PRODUCTION 20 (2004) ("At a minimum, organizations need not preserve every shred of paper, every e-mail or electronic document, and every backup tape.").

22. See, e.g., Martin H. Redish, *Electronic Discovery and the Discovery Matrix*, 51 DUKE L.J. 561, 621, 623 (2001) (arguing that companies should not be required to maintain all electronic data as this would be impractical and cost prohibitive).

23. *Id.* at 624.

24. *Id.* Such a view finds little support in the case law that has developed since the enactment of Rule 37(e). See *infra* Part III.

2010]

37(e) SAFE HARBOR

323

2. Relevant Information to Be Retained after Duty to Preserve Attaches

Even though pre-Rule 37(e) case law did not require litigants to preserve all information, it typically expected them to maintain data once they knew or should reasonably have known such data would be relevant to anticipated or actual litigation.²⁵ This standard seemed to apply regardless of the given circumstances of a particular case. On the one hand, a preservation duty could be triggered at the time an action begins.²⁶ In *Concord Boat Corp. v. Brunswick Corp.*, plaintiff's filing of a complaint provided notice that relevant materials should be retained.²⁷ On the other hand, the duty to preserve in *Inventory Locator Service, LLC v. PartsBase, Inc.* did not arise until almost 16 months after the action commenced.²⁸ In contrast to those cases, the obligation to preserve attached in *E*Trade Securities LLC v. Deutsche Bank* well before the complaint was filed since litigation was already anticipated by the parties at that time.²⁹

3. Limited Guidance from Pre-Rule 37(e) Decisions

Though helpful in giving some direction on data retention, the guidance provided by pre-Rule 37(e) case law was limited at best.³⁰ The decisions in question were typically issued by trial courts and did not carry precedential value.³¹ Case holdings

25. See, e.g., *Zubulake IV*, 220 F.R.D. at 217–18; *Wiginton*, 2003 WL 22439865, at *4.

26. *Concord Boat Corp. v. Brunswick Corp.*, No. LR-C-95-781, 1997 WL 33352759, at *4 (E.D. Ark. Aug. 29, 1997).

27. *Id.*

28. *Inventory Locator Serv., LLC v. PartsBase, Inc.*, No. 02-2695-MaV, 2005 WL 6062855, at *13 (W.D. Tenn. Oct. 19, 2005).

29. *E*Trade Sec. LLC v. Deutsche Bank, AG*, 230 F.R.D. 582, 584 (D. Minn. 2005) (ordering sanctions against the defendant due to its systemic destruction of evidence after the duty to preserve was triggered).

30. See Robert Douglas Brownstone, *Collaborative Navigation of the Stormy e-Discovery Seas*, 10 RICH. J.L. & TECH. 53, ¶ 29 (2004), at <http://law.richmond.edu/jolt/v10i5/article53.pdf>.

31. *Id.* But see *Morris v. Union Pac. R.R.*, 373 F.3d 896, 905 (8th Cir. 2004) (reversing adverse inference instruction where evidence had been destroyed pursuant to a routine document retention policy before a preservation duty attached); *Residential Funding Corp. v. DeGeorge Fin. Corp.*, 306 F.3d 99, 108 (2d Cir. 2002) (holding that an adverse inference sanction may be imposed for negligent destruction of evidence).

were also frequently inconsistent,³² resulting in confusion for organizations trying to implement good faith retention practices.³³ For example, different courts applied varying standards of culpability to determine whether sanctions were appropriate for litigants' failure to preserve electronically stored information. The Second Circuit applied a negligence standard when issuing a negative inference jury instruction.³⁴ That meant litigants could be sanctioned if they knew or should have known that data they caused to be deleted would be relevant in litigation.³⁵ In contrast, the Tenth and Eleventh Circuits refused to do so absent a finding of bad faith and intentional misconduct.³⁶ Still other jurisdictions required an intermediate standard before considering such a drastic measure.³⁷

Besides the inconsistencies, many decisions failed to appreciate that retention policies have a crucial impact on the success of an organization.³⁸ Under such policies, organizations program their servers to catch phishing e-mails, quarantine suspected viruses, and block junk mail.³⁹ Computer systems are also designed to archive and delete stale e-mail.⁴⁰ By

32. See REPORT, *supra* note 1, at 23.

33. *Id.*; see PUBLIC HEARING, *supra* note 8, at 371–72.

34. *Residential Funding*, 306 F.3d at 108 (“The sanction of an adverse inference may be appropriate in some cases involving the negligent destruction of evidence because each party should bear the risk of its own negligence.”).

35. *Id.*

36. *Aramburu v. Boeing Co.*, 112 F.3d 1398, 1413 (10th Cir. 1997) (finding that bad faith is a condition precedent to issuing an adverse inference instruction); *Turner v. Public Serv. Co. of Colo.*, 563 F.3d 1136, 1149–50 (10th Cir. 2009) (“But if the aggrieved party seeks an adverse inference to remedy the spoliation, it must also prove bad faith.”); *Bashir v. Amtrak*, 119 F.3d 929, 931 (11th Cir. 1997) (failing to preserve evidence will result in a negligent inference instruction upon a showing of bad faith); *Phillips v. Aaron Rents, Inc.*, 262 F. App’x. 202, 210 (11th Cir. 2008).

37. See, e.g., *Stevenson v. Union Pac. R.R. Co.*, 354 F.3d 739, 747 (8th Cir. 2004) (rejecting negligence standard and instead holding that “[T]here must be some indication of an intent to destroy the evidence for the purpose of obstructing or suppressing the truth in order to impose the sanction of an adverse inference instruction”); *Med. Lab. Mgmt. Consultants v. Am. Broad. Cos., Inc.*, 306 F.3d 806, 824 (9th Cir. 2002) (same).

38. See PUBLIC HEARING, *supra* note 8, at 369; Allman, *supra* note 8, at 420.

39. PUBLIC HEARING, *supra* note 8, at 369.

40. *Id.*; REPORT, *supra* note 1, at app. C-83.

preventing an influx of spam and by eliminating aged e-mails, open space is created on existing servers.⁴¹ This process, in turn, permits companies to reduce operating expenses since they are not obligated to expand server capacity to house data that has little or no business value.⁴² Issuing case-determinative sanctions for pursuing best business practices—particularly based on a negligence standard—arguably places an undue burden on companies.⁴³

Nevertheless, legal considerations—including litigation—must play a part in the planning and implementation of retention policies.⁴⁴ To ignore those considerations in fashioning and suspending automatic deletion protocols could expose an organization to liability even for the most reasonable discovery demands. How could these countervailing considerations be harmonized?⁴⁵

B. RULE 37(e)'S EFFORT TO BALANCE CORPORATE AND LITIGATION IMPERATIVES

1. A Limited Safe Harbor Protects Litigants from Excessive Preservation Obligations

The answer was a *limited* Safe Harbor.⁴⁶ As envisioned by the Advisory Committee, the Safe Harbor would shield organizations from sanctions when data was “lost as a result of the routine, good faith operation of an electronic information system.”⁴⁷ In its Judicial Conference Report, the Advisory Committee took pains to emphasize the unreasonable burdens that parties would face without the Safe Harbor.⁴⁸ Indeed, it

41. PUBLIC HEARING, *supra* note 8, at 369.

42. See Redish, *supra* note 22, at 623. These same considerations apply to data stored on back-up tapes for archival or disaster recovery purposes. See also PUBLIC HEARING, *supra* note 8, at 369.

43. See REPORT, *supra* note 1, at app. C-84.

44. Phillip M. Adams & Assoc., L.L.C. v. Dell, Inc., 621 F. Supp. 2d 1173, 1193 (D. Utah 2009); Kozlowski v. Sears, Roebuck & Co., 73 F.R.D. 73 (D. Mass. 1976).

45. See Cache La Poudre Feeds, LLC v. Land O'Lakes, Inc., 244 F.R.D. 614, 623. (D. Colo. 2007) (explaining that parties often face an “intractable dilemma: either preserve voluminous records for a [sic] indefinite period at potentially great expense, or continue routine document management practices and risk a spoliation claim at some point in the future”).

46. FED. R. CIV. P. 37(e).

47. *Id.*

48. REPORT, *supra* note 1, at app. C-83.

appeared the Committee was marching lockstep with the business community's view that the Safe Harbor was *the* answer to their document preservation problems.⁴⁹ For example, if companies were required to suspend their retention policies at the moment litigation was anticipated, the upsurge in retained data could overwhelm many computer systems.⁵⁰ It is also questionable whether such data would be relevant in litigation.⁵¹ As a result, the Advisory Committee concluded that it would be "[u]nrealistic to expect parties to stop such routine operation of their computer systems as soon as they reasonably anticipate litigation."⁵²

Thus, it appeared that companies could continue using their records management policies to rid themselves of unwanted data without being sanctioned. This general rule was subject to certain exceptions, of course.⁵³ But the point for organizations was that courts would now be forced to examine a litigant's document retention protocols through more than just the lens of litigation. Courts—at least in theory—would have to consider the nature and motives behind a company's decision-making process. Organizations might finally have a fighting chance in court.⁵⁴

2. The Safe Harbor Does Not Insulate Organizations from Reasonable Litigation Demands

While the Safe Harbor provided some key protections to corporate America, the new rule also addressed some of the lingering concerns from the plaintiffs' bar.⁵⁵ The Safe Harbor only applied to data that was destroyed due to the ordinary

49. PUBLIC HEARING, *supra* note 8, at 365–72.

50. REPORT, *supra* note 1, at app. C-83; Redish, *supra* note 22, at 623.

51. REPORT, *supra* note 1, at app. C-83.

52. *Id.* at app. C-83, F-7.

53. *See infra* Part III.

54. Thomas Y. Allman, *Defining Culpability: The Search for a Limited Safe Harbor in Electronic Discovery*, 2 FED. CTS. L. REV. 65, 83 (2007) (“[B]y assuring public and private entities, both large and small, that common sense will be applied to the review of their preservation decisions, it should help break the logjam for those that have desired, but hesitated, to implement realistic and balanced policies and procedures to meet their business and litigation needs.”).

55. PUBLIC HEARING, *supra* note 8, at 25–26 (arguing that a prior draft of the Safe Harbor seemed to “encourage the destruction rather than the retention” of data).

functions of a computer system.⁵⁶ It did not prevent sanctions when data was manually deleted.⁵⁷ For example, the Safe Harbor afforded no protection to a company that relied on its individual employees to manually archive and delete electronic data.⁵⁸ Nor could it shelter bad faith data destruction,⁵⁹ such as intentionally deleting database information,⁶⁰ e-mails,⁶¹ web pages,⁶² metadata,⁶³ software,⁶⁴ data on hardware⁶⁵ or other records once the duty to preserve attached.⁶⁶

The Safe Harbor would also yield in other “exceptional circumstances.”⁶⁷ An organization *could* be required to modify certain aspects of a retention policy once a preservation duty was triggered.⁶⁸ Companies could not simply allow their

56. The Safe Harbor does not apply to the destruction of paper documents. See Phillip M. Adams & Assoc., L.L.C. v. Dell, Inc., 621 F. Supp. 2d 1173, 1191 (D. Utah 2009); FED. R. CIV. P. 37 advisory committee’s note (2006 Amendment).

57. See Phillip M. Adams, 621 F. Supp. 2d at 1192.

58. *Id.*; Connor v. Sun Trust Bank, 546 F. Supp. 2d 1360, 1376–77 (N.D. Cal. 2008).

59. Keithley v. Home Store.com, Inc., No. C-03-04447 SI (EDL), 2008 WL 3833384, at *16 (N.D. Cal. Aug. 12, 2008).

60. *Id.*, at *11.

61. Pandora Jewelry, LLC v. Chamilia, LLC, No. CCB-06-3041, 2008 WL 4533902, at *8–9 (D. Md. Sept. 30, 2008) (holding the Safe Harbor did not apply since defendant was grossly negligent for failing to preserve e-mail).

62. Arista Records LLC v. Usenet.com, Inc., 608 F. Supp. 2d 409, 430–36 (S.D.N.Y. 2009) (holding that the Safe Harbor did not insulate defendants from adverse inference sanction where they failed to preserve relevant web pages after a preservation duty was triggered).

63. See Philip J. Favro, *A New Frontier in Electronic Discovery: Preserving and Obtaining Metadata*, 13 B.U. J. SCI. & TECH. L. 1, 20 (2007).

64. KCH Serv., Inc. v. Vanaire, Inc., No. 05-777-C, 2009 WL 2216601, at *1 (W.D. Ky. Jul. 22, 2009) (holding the Safe Harbor would not protect defendants from an adverse inference sanction given their deletion of software and their unreasonable failure to keep other electronic data after the duty to preserve attached).

65. Stratienco v. Chattanooga-Hamilton County Hosp. Auth., No. 1:07-CV-258, 2009 WL 2168717, at *4 (E.D. Tenn. Jul. 16, 2009) (holding that defendants’ re-imaging of hard drive after duty to preserve attached fell outside the scope of the Safe Harbor).

66. *In re Krause*, 367 B.R. 740, 766–68 (D. Kan. 2007) (holding that defendants’ use of a wiping software was not protected under the Safe Harbor); Nucor v. Bell, 251 F.R.D. 191, 204 (D.S.C. 2008) (ordering sanctions for defendant’s destruction of a USB flash drive).

67. FED. R. CIV. P. 37(e).

68. FED. R. CIV. P. 37 advisory committee’s note (2006 Amendment) (“Good faith in the routine operation of an information system may involve a

computer systems to destroy relevant data at the same time they obliterated useless information.⁶⁹ A litigant's action or inaction on this issue would undoubtedly bear on whether the operation of its computer systems had been in good faith.⁷⁰

This has certainly turned out to be true. Most courts applying Rule 37(e) have issued sanctions for spoliation when a party has failed to suspend particular aspects of its computer systems after a preservation duty attached.⁷¹ Thus, the Advisory Committee did impose a duty to stop the routine destruction of electronic data in certain circumstances despite its earlier misgivings about doing so.⁷² And though this duty did not extend to *all* data, it was broad enough to encompass materials considered relevant to perceived or pending litigation.⁷³

3. The Safe Harbor Established an Intermediate Standard for Imposing Discovery Sanctions

Despite some confusion regarding when a litigant's preservation duty arose, the Advisory Committee was clear regarding the measure for imposing discovery sanctions.⁷⁴ The

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.”).

69. *Id.*; see *Peskoff v. Faber*, 244 F.R.D. 54, 60 (D.D.C. 2007).

70. See *Disability Rights Council of Greater Wash. v. Wash. Metro. Transit Auth.*, 242 F.R.D. 139, 146 (D.D.C. 2007).

71. See, e.g., *Arista Records LLC v. Usenet.com, Inc.*, 608 F. Supp. 2d 409, 430–36 (S.D.N.Y. 2009); cases cited *infra* Part III.C.1. *But see Escobar v. City of Houston*, No. 04-1945, 2007 WL 2900581, at *19 (S.D. Tex. Sept. 29, 2007) (holding the Safe Harbor protected defendant from sanctions despite neglecting to suspend the overwriting features to its electronic communications server).

72. FED. R. CIV. P. 37 advisory committee's note (2006 Amendment) (“The good faith requirement of Rule 37[e] 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.”). The Advisory Committee's confusing statements on this issue seem to evince its position that “there is considerable uncertainty as to whether a party—particularly a party that produces large amounts of information—nonetheless has to interrupt the operation of the electronic information systems it is using to avoid any loss of information because of the possibility that it might be sought in discovery, or risk severe sanctions.” REPORT, *supra* note 1, at app. C-83.

73. *Id.*; see *infra* Part III.B.

74. REPORT, *supra* note 1, at app. C-83.

Committee deemed an intermediate standard best suited for determining whether sanctions should issue for data lost as the result of a computer system's operation.⁷⁵

The intermediate benchmark resulted from a compromise between two competing proposals in the original draft rule. As initially designed, the proposed rule would have imposed sanctions based on a negligence standard.⁷⁶ In an effort to balance this provision, the Advisory Committee alternatively proposed that sanctions be imposed for reckless or intentional conduct.⁷⁷

Each proposal, however, was sharply criticized for its shortcomings.⁷⁸ The negligence standard was attacked since it essentially afforded no protection from sanctions than that already developed by case law.⁷⁹ Indeed, it was worse than the status quo because a litigant could arguably be punished for "any mistake in interrupting the routine operation of a computer system."⁸⁰ For instance, a party could possibly be sanctioned for failing to suspend a records management policy despite preserving an alternative source of that deleted data.⁸¹ In contrast, the intentional standard was considered too lenient; sanctions might not issue for genuinely nefarious conduct.⁸² Moreover, it might be too difficult for litigants to

75. *Id.* ("The present proposal establishes an intermediate standard, protecting against sanctions if the information was lost in the 'good faith' operation of an electronic information system.")

76. *Id.*, at app. C-84; see *Inventory Locator Serv., LLC v. PartsBase, Inc.*, No. 02-2695-MaV, 2005 WL 6062855, at *13 n.8 (W.D. Tenn. Oct. 19, 2005) (finding support in the earlier version of Rule 37(e) that defendant's preservation duty did not attach until nearly sixteen months after the action was commenced); *Convolve, Inc. v. Compaq Computer Corp.*, 223 F.R.D. 162, 177 (S.D.N.Y. 2004) (citing to the early draft version of Rule 37(e) as support for its holding that no sanctions should issue for data destruction).

77. REPORT, *supra* note 1, at app. C-84.

78. *Id.*

79. *Id.*

80. *Id.*; see *Escobar v. City of Houston*, Civil Action No. 04-1945, 2007 WL 2900581, at *19 (S.D. Tex. Sept. 29, 2007) (refusing to order sanctions for destruction of electronic data where alternative source of requested evidence was produced in discovery).

81. REPORT, *supra* note 1, at app. C-84; see *Gippetti v. United Parcel Serv., Inc.*, No. C07-00812 RMW (HRL), 2008 WL 3264483, at *4 (N.D. Cal. Aug. 6, 2008); *Escobar*, 2007 WL 2900581, at *18-19; *Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey*, 497 F. Supp. 2d 627, 641 (E.D. Pa. 2007).

82. REPORT, *supra* note 1, at app. C-84.

establish the necessary intent for sanctions to issue under such a standard.⁸³

Ultimately, an intermediate standard, with the touchstone of “good faith,” became the operative benchmark under Rule 37(e).⁸⁴ Though its criteria were somewhat nebulous, a good faith standard would ultimately provide courts with leeway to appropriately balance a litigant’s conduct under the circumstances of a case.⁸⁵ Such an approach resembled the manner in which the Eighth Circuit previously decided *Stevenson v. Union Pacific Railroad Co.*⁸⁶ and *Morris v. Union Pacific Railroad.*⁸⁷

In *Stevenson*, the Eighth Circuit affirmed a negative inference instruction issued by the trial court.⁸⁸ That sanction was ordered for defendant Union Pacific’s destruction of recorded voice radio communications between railroad dispatchers and the crew of a train that had just struck plaintiff’s vehicle.⁸⁹ The taped conversation had been erased prior to the commencement of litigation pursuant to defendant’s policy of reusing voice tapes by overwriting their contents after ninety days.⁹⁰ Though erased several months prior to litigation, the court held that evidence of the communications should have been maintained.⁹¹ The tape was the only source of evidence reflecting the observations the train crew made just after the accident occurred.⁹² Moreover, the defendant had kept similar voice tapes in other circumstances when the tapes would absolve the company of liability.⁹³ And

83. *Id.*; see *Morris v. Union Pac. R.R.*, 373 F.3d 896, 902–03 (8th Cir. 2004) (describing the difficulty in establishing intent).

84. REPORT, *supra* note 1, at app. C-85. *But see* *Keithley v. Home Store.com, Inc.*, No. C-03-04447 SI (EDL), 2008 WL 3833384, at *3 (N.D. Cal. Aug. 12, 2008) (declaring that violations of Rule 37 may invite sanctions even for negligent conduct).

85. See *United Med. Supply v. United States*, 77 Fed. Cl. 257, 269–70 (2007) (noting that, among other things, Rule 37(e) was causing courts to reconsider “enhanced proof requirements . . . in favor of a flexible intent requirement”).

86. *Stevenson v. Union Pac. R.R. Co.*, 354 F.3d 739 (8th Cir. 2004).

87. *Morris v. Union Pac. R.R.*, 373 F.3d 896 (8th Cir. 2004).

88. *Stevenson*, 354 F.3d at 747–48.

89. *Id.*

90. *Id.* at 747.

91. *Id.* at 748.

92. *Id.*

93. *Id.*

though no effort was made to keep the tape, the defendant ensured that other, possibly exculpatory evidence was preserved.⁹⁴ Such details confirmed that defendant's conduct was intentional and negated its showing that destruction of the tape was in good faith.⁹⁵

In contrast, the Eighth Circuit in *Morris* vacated an adverse inference instruction in a strikingly similar case.⁹⁶ Like *Stevenson*, *Morris* involved a plaintiff who had been injured in a train collision.⁹⁷ And just as in *Stevenson*, Union Pacific had allowed a taped conversation between a train crew and railroad dispatchers to be erased in connection with its ninety-day retention policy.⁹⁸ Regardless, the Eighth Circuit found an adverse inference instruction was not appropriate.⁹⁹ Unlike *Stevenson*, it concluded that Union Pacific did not intentionally eliminate the taped conversation.¹⁰⁰ Nor was there anything to suggest that some evidence was maintained while other, more crucial proof was destroyed.¹⁰¹ In the end, there was no evidence that belied the defendant's good faith.¹⁰²

Though it reached opposite results in *Stevenson* and *Morris*, the Eighth Circuit's reasoning is instructive. The court did not limit its analysis to merely determining whether or not information was eliminated by the routine operation of a computer system.¹⁰³ Instead, it weighed various factors to glean the defendant's intentions and decide whether sanctions were appropriate.¹⁰⁴ In like manner, courts should evaluate the circumstances of a given matter to understand whether data was lost in good faith or not.¹⁰⁵

94. *Id.* at 747.

95. *Id.* at 747–48.

96. *Morris v. Union Pac. R.R.*, 373 F.3d 896, 903 (8th Cir. 2004).

97. *Id.* at 898.

98. *Id.* at 899–900.

99. *Id.* at 902–03.

100. *Id.* at 902.

101. *Id.*

102. *Id.* at 902–03.

103. *Stevenson v. Union Pac. R.R. Co.*, 354 F.3d 739, 748–49 (8th Cir. 2004); *Morris*, 373 F.3d at 902.

104. *Stevenson*, 354 F.3d at 748–49; *Morris*, 373 F.3d at 902.

105. See THE SEDONA CONFERENCE WORKING GROUP ON ELECTRONIC DOCUMENT RETENTION & PRODUCTION, THE SEDONA CONFERENCE, THE SEDONA PRINCIPLES: BEST PRACTICES RECOMMENDATIONS & PRINCIPLES FOR ADDRESSING ELECTRONIC DOCUMENT PRODUCTION 72 (Jonathan M. Redgrave

C. A NATIONAL STANDARD FOR GUIDING RECORDS
MANAGEMENT DECISIONS IN CONNECTION WITH LITIGATION

As finalized, Rule 37(e) struck a balance between competing forces.¹⁰⁶ On the one hand, the Safe Harbor could protect organizations from arbitrary retention obligations.¹⁰⁷ On the other hand, aggrieved parties could still seek relief for evidence destruction caused by bad faith, grossly negligent conduct, and ordinary negligence.¹⁰⁸ A uniform benchmark had thus been established that could guide organizations' choices for records management in connection with litigation.¹⁰⁹ As discussed in Part Three, the resulting Safe Harbor jurisprudence would delineate some key trends that would further assist in this process.

III. KEY TRENDS FROM RULE 37(e) RECORDS
MANAGEMENT JURISPRUDENCE

In the years that have passed since Rule 37(e) was adopted, various courts have addressed the Safe Harbor. In very few instances have courts invoked the rule to shield parties from sanctions.¹¹⁰ Regardless of the final result,

et al. eds., 2d ed. 2007) [hereinafter 2007 SEDONA PRINCIPLES] (providing various suggestions for how courts can evaluate an organization's good faith for purposes of applying Rule 37(e)); *see also* THE SEDONA CONFERENCE WORKING GROUP ON ELECTRONIC DOCUMENT RETENTION & PRODUCTION, THE SEDONA CONFERENCE, THE SEDONA CONFERENCE COMMENTARY ON LEGAL HOLDS: THE TRIGGER & THE PROCESS 9–10 (Conor R. Crowley et al. eds., 2007) [hereinafter SEDONA CONFERENCE COMMENTARY ON LEGAL HOLDS] (listing factors to consider when determining whether litigation is “reasonably anticipated”).

106. *See* REPORT, *supra* note 1, at app. F-8.

107. *See id.* at app. C-83.

108. Pandora Jewelry, LLC v. Chamilia, LLC, No. CCB-06-3041, 2008 WL 4533902, at *8 (D. Md. Sept. 30, 2008).

109. Subject to certain conditions, courts may still issue sanctions independent of Rule 37(e) under their inherent authority. Escobar v. City of Houston, No. 04-1945, 2007 WL 2900581, at *17 n.5 (S.D. Tex. Sept. 29, 2007); Allman, *supra* note 54, at 14–15.

110. *See, e.g.*, Sue v. Milyard, No. 07-cv-01711-REB-MJW, slip op. at 2 (D. Colo. Aug. 6, 2009), 2009 WL 2424435 (holding that the deleted video footage was destroyed pursuant to the “normal operating process of the camera's computer system” before a preservation duty was triggered); Southeastern Mechanical Services, Inc. v. Brody, No. 8:08-CV-1151-T-30EAJ, slip op. at 3-4 (M.D. Fla. July 24, 2009), 2009 WL 2242395 (finding in part that plaintiff had no duty to preserve certain backup tapes); Escobar, 2007 WL 2900581, at *17–19 (holding that sanctions were not warranted where defendant preserved an

opinions interpreting Rule 37(e) have generated a number of helpful guidelines and trends. Such developments should be instructive for organizations as they look to streamline document retention policies with litigation requirements. Part Three will explore some of the principal developments that have occurred over the past three years and their pertinence to records management.

A. RECORDS MANAGEMENT STRATEGY MUST CONSIDER ACCOUNTABILITY TO THIRD PARTIES

One of the principal advances in Safe Harbor jurisprudence is that records management policies must now consider an organization's accountability to third parties.¹¹¹ This is not a novel concept.¹¹² It was previously considered in connection with disputes over preservation and production of paper documents.¹¹³ However, the extension of this doctrine to electronic data in *Phillip M. Adams & Associates, L.L.C. v. Dell, Inc.* was a significant development.¹¹⁴

In *Phillip M. Adams*, the court issued sanctions in a patent infringement action for the defendants' spoliation of source code, along with related documents and communications, after a preservation duty attached.¹¹⁵ As part of its holding, the court refused the defendants' request to invoke the Safe Harbor given their failure to operate their computer systems in good faith.¹¹⁶

In reaching this decision, the court zeroed in on the unreasonably narrow scope of the defendants' retention

alternative source of the sought after evidence); *Columbia Pictures Indus. v. Bunnell*, No. CV 06-1093FMCJJCX, 2007 WL 2080419 (C.D. Cal. May 29, 2007) (declining to order sanctions since defendant was not on notice that it should retain the requested server log data), *aff'd*, 245 F.R.D. 443 (C.D. Cal. 2007).

111. *Phillip M. Adams & Assoc., L.L.C. v. Dell, Inc.*, 621 F. Supp. 2d 1173, 1193 (D. Utah 2009).

112. *Lewy v. Remington Arms*, 836 F.2d 1104, 1113 (8th Cir. 1988); *Kozlowski v. Sears, Roebuck & Co.*, 73 F.R.D. 73, 76 (D. Mass. 1976).

113. *See, e.g., Lewy*, 836 F.2d at 1112 (explaining that a reasonable retention policy would keep records of customer complaints longer than other records); *Kozlowski*, 73 F.R.D. at 76-77 (holding that defendant's policy of indexing customer complaints was so byzantine and obstructionist that it precluded the retrieval of relevant documents).

114. Adam Cohen, *Angst Over Data Retention Ruling May Be Misplaced: 'Adams' Actually Was in Line with Legal Precedent and Evolving Best Practices at U.S. Corporations*, 31 NAT'L L.J. 51 (2009).

115. *Phillip M. Adams*, 621 F. Supp. 2d at 1191, 1195.

116. *Id.* at 1192.

practices.¹¹⁷ For example, the server hosting the defendants' e-mail was programmed to automatically delete all mail not manually archived by employees.¹¹⁸ Such an arbitrary policy—entirely reliant on the discretion of individual employees—apparently suited the defendants' business model given the limited storage capacity on their servers.¹¹⁹ Such a narrowly tailored policy was unreasonable:

A court—and more importantly, a litigant—is not required to simply accept whatever information management practices a party may have. *A practice may be unreasonable, given responsibilities to third parties.* While a party may design its information management practices to suit its business purposes, *one of those business purposes must be accountability to third parties.*¹²⁰

The defendants' parochial retention practices did not account for the duties they owed to third parties in connection with litigation.¹²¹ This practice ultimately negated any possibility that the Safe Harbor could apply.¹²²

Phillip M. Adams is a watershed case for records management. Organizations that fail to implement reasonable retention policies or that narrowly customize them to limit expense or exposure to liability may run afoul of this decision. By focusing only on reducing operating expenses, companies may cause the opposite result to occur. Organizations may exponentially increase their bottom line by failing to factor in legal considerations to third parties.

B. THE GOOD, THE BAD, AND THE UGLY—EXAMPLES OF REASONABLE AND UNREASONABLE RECORDS MANAGEMENT POLICIES

The difference between a reasonable and unreasonable document retention policy can make all the difference for an organization when it comes to maximizing revenues and minimizing operation expenses.¹²³ As evidenced by the judiciary's application of Rule 37(e), that distinction is equally applicable in legal proceedings. In litigation, sanctions are less

117. *Id.* at 1193.

118. *Id.* at 1181–82, 1192.

119. *Id.* at 1181–82.

120. *Id.* at 1193 (emphasis added).

121. *Id.* at 1192–94.

122. *Id.*

123. See PUBLIC HEARING, *supra* note 8, at 369.

frequently imposed on organizations that develop *and* follow a reasonable policy. In those instances involving a “bad” policy, or where there is no policy at all, data destruction typically prevents application of the Safe Harbor. The cases of *Gipetti v. United Parcel Service, Inc.*,¹²⁴ *Connor v. Sun Trust Bank*,¹²⁵ and *Keithley v. Home Store.com, Inc.*¹²⁶ exemplify these trends in post-Rule 37(e) case law.

1. The Good—*Gipetti v. United Parcel Service, Inc.*

One of the general hallmarks of an effective records management policy is that it addresses the particular needs of an organization while balancing them against litigation imperatives.¹²⁷ This point is well illustrated in *Gipetti v. United Parcel Service, Inc.*¹²⁸ In *Gipetti*, the court refused to sanction defendant United Parcel Service (“UPS”) for allowing copies of electronic tachograph records to be overwritten pursuant to its document retention policy.¹²⁹ Plaintiff, a terminated delivery truck driver,¹³⁰ argued that UPS should be sanctioned for allowing destruction of the tachograph records.¹³¹ Plaintiff asserted that the records, which track a vehicle’s speed and movements, would have established his age discrimination claim by showing that he drove his delivery route at the same rate as other, younger drivers.¹³²

The court rejected the sanctions request due in significant part to the good faith operation of UPS’s computer servers.¹³³ Developed several years before the instant lawsuit, UPS’s “nationwide practice” was to purge tachograph records after thirty-seven days to reduce a growing stockpile of data.¹³⁴ Another factor favoring UPS was its decision to modify the

124. *Gipetti v. United Parcel Serv., Inc.*, No. C07-00812 RMW (HRL), 2008 WL 3264483 (N.D. Cal. Aug. 6, 2008).

125. *Connor v. Sun Trust Bank*, 546 F. Supp. 2d 1360 (N.D. Cal. 2008).

126. *Keithley v. Home Store.com, Inc.*, No. C-03-04447 SI (EDL), 2008 WL 3833384 (N.D. Cal. Aug. 12, 2008).

127. See 7 MOORE’S FEDERAL PRACTICE, § 37A.56[1] (3d ed. 2009).

128. See *Gipetti*, 2008 WL 3264483, at *2.

129. *Id.* at *4.

130. *Id.* at *1. Plaintiff was discharged for “sleeping on the job” and “stealing time” from UPS. *Id.*

131. *Id.*

132. *Id.*

133. *Id.* at *4–5.

134. *Id.* at *2.

operation of its servers after a preservation duty was triggered such that records still in its possession could be produced.¹³⁵ In any event, the records were held to have little if any relevance to the plaintiff's claims.¹³⁶ What information, if any, the plaintiff needed from the records could be gleaned from time cards produced by UPS.¹³⁷

Gipetti provides a favorable benchmark against which organizations can analyze their retention practices. The reasonableness of the policy at issue was measured by its good faith business purpose, the length of time it had been in place, that it was actually followed,¹³⁸ and that the destruction of records occurred before a preservation duty attached.¹³⁹ The policy was also effective since it eliminated one source of information while maintaining another, equally viable source that could be used in litigation.¹⁴⁰ Finally, promptly modifying the policy to retain the requested records after the preservation duty was triggered eliminated any doubt regarding UPS's good faith under Rule 37(e).¹⁴¹

2. The Bad—*Connor v. Sun Trust Bank*

In contrast to *Gipetti* stands the problematic retention policy in *Connor v. Sun Trust Bank*.¹⁴² Pursuant to that retention policy, the defendant bank's server purged all e-mail more than thirty days old that had not been manually archived outside the company's e-mail system.¹⁴³ That policy, coupled with a companion practice of overwriting back-up tapes after ten days, ensured that any e-mail that a bank employee neglected to archive would be automatically deleted after forty days.¹⁴⁴

Such retention practices proved inadequate in *Connor*. A

135. *Id.* at *1.

136. *Id.* at *4.

137. *Id.*

138. *See Doe v. Norwalk Cmty. Coll.*, 248 F.R.D. 372, 378 (D. Conn. 2007) (issuing sanctions for, among other reasons, the defendant's failure to follow its document retention policies).

139. *Gipetti*, 2008 WL 3264483, at *2–4.

140. *Id.* at *4.

141. *Id.* at *2.

142. *Connor v. Sun Trust Bank*, 546 F. Supp. 2d 1360, 1367 (N.D. Cal. 2008).

143. *Id.*

144. *Id.*

negative inference instruction was imposed on the bank for failing to preserve a key e-mail relating to the plaintiff's Family and Medical Leave Act claim.¹⁴⁵ Through its general counsel, the bank issued a timely litigation hold and instructed its employees most likely to have data relevant to the lawsuit to preserve that information.¹⁴⁶ Nevertheless, the bank employee responsible for discharging plaintiff did not preserve any e-mails during a crucial six-week period, including the key e-mail at issue.¹⁴⁷ Though it was never established whether the e-mail was intentionally deleted or simply wiped out by the bank's e-mail server, this fact was irrelevant.¹⁴⁸ The e-mail was deleted in contravention of the company's preservation instructions.¹⁴⁹ Worse, it created an inference that other potentially relevant e-mails were also deleted.¹⁵⁰

The *Connor* holding is instructive on multiple fronts. Like the defendants in *Phillip M. Adams*,¹⁵¹ the bank unreasonably relied on its employees to determine what e-mails should or should not have been kept.¹⁵² The drawback to such an approach is that employees may neglect to archive (or consciously discard) their e-mails or other data.¹⁵³ That is precisely what occurred with the bank employee who terminated plaintiff.¹⁵⁴ A reasonable policy would have addressed this issue by retaining e-mails, back-up tapes or both for a longer period of time.

Regardless, the bank should have modified its e-mail and back-up tape retention policies as part of its litigation hold.¹⁵⁵ Had it done so, the deleted e-mails likely would not have slipped through the cracks.¹⁵⁶ By failing to do so, the bank

145. *Id.* at 1376–77.

146. *Id.*

147. *Id.*

148. *Id.*

149. *Id.* at 1367–68.

150. *Id.* at 1376.

151. *Phillip M. Adams & Assoc., L.L.C. v. Dell, Inc.*, 621 F. Supp. 2d 1173 (D. Utah 2009).

152. *Connor*, 546 F. Supp. 2d at 1367–68.

153. *Id.* at 1368.

154. *Id.* (noting that the employee in question fell behind in archiving her e-mails).

155. FED. R. CIV. P. 37 advisory committee's note (2006 Amendment).

156. *See Gippetti v. United Parcel Serv., Inc.*, No. C07-00812 RMW (HRL), 2008 WL 3264483, at *1 (N.D. Cal. Aug. 6, 2008).

could not establish that the routine operation of its server was in good faith.¹⁵⁷

3. The Ugly—*Keithley v. Home Store.com*

Standing apart from the “good” and “bad” examples of records management are those “ugly” situations where organizations fail to even implement a document retention policy.¹⁵⁸ This neglect can be disastrous in litigation and generally leaves organizations outside the protections of the Safe Harbor.¹⁵⁹ The *Keithley v. Home Store.com, Inc.* decision exemplifies this scenario.¹⁶⁰

In *Keithley*, the court leveled monetary and evidentiary sanctions against the defendants for their destruction of relevant source code and related evidence.¹⁶¹ The evidence destruction was tracked back to the defendants’ failure to implement a document retention policy or even issue a litigation hold.¹⁶² Such conduct, which was per se “reckless” and “intentional,” placed the defendants far beyond the Safe Harbor’s refuge.¹⁶³

Surprisingly enough, *Keithley* is not an isolated occurrence.¹⁶⁴ In the recent decision of *Technical Sales Associates, Inc. v. Ohio Star Forge Co.*, the defendant did not have an e-mail retention policy, never implemented a litigation hold, and intentionally destroyed categories of evidence.¹⁶⁵ The

157. Though Rule 37(e) is not specifically mentioned in the opinion, the analysis is paradigmatic for understanding the application of the Safe Harbor. See also *United Med. Supply Co. v. United States*, 77 Fed. Cl. 257, 274 (2007) (sanctioning defendant for allowing materials to be destroyed by its “antiquated” retention policies and reasoning that policies involving contract materials should, at a minimum, require retention of such materials during the applicable statute of limitations).

158. *Keithley v. Home Store.com, Inc.*, No. C-03-04447 SI (EDL), 2008 WL 3833384 (N.D. Cal. Aug. 12, 2008).

159. *Technical Sales Assoc., Inc. v. Ohio Star Forge Co.*, Nos. 07-11745, 08-13365, 2009 WL 728520, at *6–8 (E.D. Mich. Mar. 19, 2009).

160. *Keithley*, 2008 WL 3833384, at *6, *16.

161. *Id.* at *18, *20 (noting that defendants’ misconduct was “among the most egregious this Court has seen”).

162. *Id.* at *6, *16.

163. *Id.* at *16 (finding that defendants’ false statements and eleventh hour productions also factored into the court’s holding).

164. *Technical Sales*, 2009 WL 728520, at *6–8.

165. *Id.*

2010]

37(e) SAFE HARBOR

339

Safe Harbor was therefore not applicable.¹⁶⁶

4. Reasonable Retention Policies Can Effectively Address Organizational Needs in Relation to Litigation Requirements

The simple lesson from the Safe Harbor case law is that there is no magic formula for a reasonable and effective retention policy. Instead, it must take into account an organization's business needs, which include particularized legal demands.¹⁶⁷ That is how a thirty-seven day retention practice in *Gipetti* was held to be reasonable¹⁶⁸ while a combined forty day policy in *Connor* was not.¹⁶⁹ In those instances where a policy was inadequate, such as in *Connor*, it was because the organization did not properly assess the impact of litigation on its business.¹⁷⁰ Simply put, a policy must be reasonable under the circumstances.

C. MODIFYING RECORDS MANAGEMENT POLICIES: TIMING AND SCOPE ARE EVERYTHING

Timing is everything when it comes to knowing when to modify a document retention policy. But timing is not all; an understanding of the breadth of what needs to be preserved is also required. By correctly assessing when a preservation duty is triggered and then reasonably limiting the appropriate scope of material that is included as part of that preservation duty, litigants can establish the reasonableness of their conduct in litigation. At the same time, organizations can keep the wheels turning on their servers such that superfluous data continue to be overwritten. Most cases addressing Rule 37(e) have in some form or another touched on the issue of modifying or suspending a litigant's records management policy. Of those cases, the following spotlight the nuances that parties may need to address when considering whether to modify such a policy.

166. *Id.*

167. Phillip M. Adams & Assoc., L.L.C. v. Dell, Inc., 621 F. Supp. 2d 1173, 1193 (D. Utah 2009).

168. *Gipetti v. United Parcel Serv., Inc.*, No. C07-00812 RMW (HRL), 2008 WL 3264483, at *1-4 (N.D. Cal. Aug. 6, 2008).

169. *Connor v. Sun Trust Bank*, 546 F. Supp. 2d 1360, 1376-77 (N.D. Cal. 2008).

170. *See Connor*, 546 F. Supp. 2d at 1368; *see also* *United Med. Supply Co. v. United States*, 77 Fed. Cl. 257, 274 (2007).

1. Whether and What Aspects of a Retention Policy Require Modification

The first inquiry a litigant must consider is whether any aspect of its document management practices requires modification. As a rule, parties need not interrupt a policy if they do not know or are not reasonably aware that data encompassed by that policy should be preserved.¹⁷¹ The *Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey* decision is instructive on this issue.¹⁷²

In *Healthcare Advocates*, the court refused to sanction the defendant for allowing its computers to automatically delete internet cache files that the plaintiff argued were relevant to its claims.¹⁷³ Despite ongoing litigation, no preservation duty for the files attached such that it would have been reasonable for the defendant to have retained the files.¹⁷⁴ In addition, the defendant preserved other data in lieu of the cache files that had equal relevance to the plaintiff's claims.¹⁷⁵ Nor was there any business purpose for keeping the files.¹⁷⁶ Accordingly, the defendant had no reason to modify its policy of allowing the files to be automatically deleted.¹⁷⁷

A more subtle distinction appears when an organization knows a preservation duty has been triggered, yet chooses to allow a retention policy to continue uninterrupted.¹⁷⁸ For instance, the defendant in *Escobar v. City of Houston* did not modify a records management policy that caused e-mail and

171. *Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey*, 497 F. Supp. 2d 627, 640–41 (E.D. Pa. 2007).

172. *Id.*

173. *Id.* at 641.

174. *Id.* at 640–41; *see also* *Mohrmeyer v. Wal-Mart Stores East*, No. 09-69-WOB, slip op. at 3 (E.D. Ky. Nov. 20, 2009) (applying Rule 37(e) to hold that sanctions were not justified for the defendant's destruction of a paper record).

175. *Id.* at 641.

176. *Id.* at 639 (noting that the defendant had no marketing or advertising purpose for the disputed information).

177. This holding is consistent with the results of other cases decided under Rule 37(e). *See, e.g.*, *Columbia Pictures Indus. v. Bunnell*, No. CV 06-1093FMCJCX, 2007 WL 2080419, at *13–14 (C.D. Cal. May 29, 2007), *aff'd*, 245 F.R.D. 443 (C.D. Cal. 2007); *Convolve, Inc. v. Compaq Computer Corp.*, 223 F.R.D. 162, 177 (S.D.N.Y. 2004) (holding that under the prior draft version of Rule 37(e), defendant should not be sanctioned for failing to retain data automatically purged by the ordinary operation of a computer system).

178. *Escobar v. City of Houston*, No. 04-1945, 2007 WL 2900581 (S.D. Tex. Sept. 29, 2007).

other electronic communications to be deleted after ninety days.¹⁷⁹ Knowing that the police officers involved in a shooting that led to the plaintiff's wrongful death suit did not use e-mail, the defendant did not stop a server from deleting e-mail contemporaneous with the shooting.¹⁸⁰ Instead, the defendant preserved other records that it believed would be more relevant to the plaintiff's claim.¹⁸¹ As that conduct was found to be reasonable, plaintiff's sanctions request was denied.¹⁸²

In contrast to *Escobar*, courts typically refuse to apply Rule 37(e)'s Safe Harbor when a party allows a retention policy to destroy the only sources of relevant data. For example, in *Cache La Poudre Feeds, LLC v. Land O'Lakes, Inc.*, monetary sanctions were appropriate to address the defendants' failure to preserve archival back-up tapes.¹⁸³ The tapes contained the only source of data formerly found on the computers of the defendants' employees.¹⁸⁴ Similarly, a court issued monetary and evidentiary sanctions in *Doe v. Norwalk Community College* to address the loss of key data when back-up tapes were allowed to be overwritten.¹⁸⁵ And in *Pandora Jewelry, LLC v. Chamilia, LLC*, monetary sanctions were ordered as a result of the defendant's failure to prevent relevant e-mails from being deleted after ninety days.¹⁸⁶

2. Harmonizing Retention Practices and Litigation Imperatives Requires an Effective Management Team

Just as the reasonableness of a records management practice depends on a given set of facts, so too there is no bright line approach regarding what policies need to be modified to ensure that relevant data is retained. As previously discussed, it is unnecessary and unwise to suspend all aspects of all

179. *Id.* at *18–19.

180. *Id.* at *18.

181. *Id.* at *19.

182. *Id.*

183. *Cache La Poudre Feeds, LLC v. Land O'Lakes, Inc.*, 244 F.R.D. 614, 637 (D. Colo. 2007).

184. *Id.*

185. *Doe v. Norwalk Cmty. Coll.*, 248 F.R.D. 372, 378, 381 (D. Conn. 2007).

186. *Pandora Jewelry, LLC v. Chamilia, LLC*, No. CCB-06-3041, 2008 WL 4533902, at *8–9 (D. Md. Sept. 30, 2008); *see also* *Major Tours, Inc. v. Colorel*, No. 05-3091 (JBS/JS), slip op. at 4 (D.N.J. Aug. 4, 2009), 2009 WL 2413631 (finding that no effort was made to keep e-mails that were deleted after a preservation duty arose).

retention protocols.¹⁸⁷ Litigants will simply have to choose how much or little information they will keep to comply with a preservation obligation.¹⁸⁸ Doing nothing, however, is not an option.¹⁸⁹ Taking action to preserve data may allow an organization to use the Safe Harbor to avoid issue, evidence or terminating sanctions.¹⁹⁰ Organizations must ultimately evaluate their respective circumstances and move forward in a reasonable fashion. Drawing upon the advice of seasoned professionals, including legal counsel, will likely be critical to the success of those efforts.¹⁹¹

IV. SUGGESTED PRACTICES FOR ADDRESSING LITIGATION REQUIREMENTS IN CONNECTION WITH RECORDS MANAGEMENT PROTOCOLS

The developing body of Rule 37(e) jurisprudence provides guidance for litigants to implement effective records management protocols. This Part contains suggested practices for addressing litigation requirements in connection with an organization's retention policies.

A. TIMELY IMPLEMENT AN EFFECTIVE RETENTION POLICY

Before anything else can happen, a party must design and

187. *Cache La Poudre Feeds*, 244 F.R.D. at 623–24; *Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey*, 497 F. Supp. 2d 627, 641 (E.D. Pa. 2007) (holding it was unreasonable for Plaintiff to expect Defendants to completely remove computers from further operation to protect against data from being lost); *Turner v. Resort Condo. Int'l, LLC*, No. 1:03-cv-2025-DFH-WTL, 2006 WL 1990379, at *6 (S.D. Ind. Jul. 13, 2006) (holding that a pre-litigation demand letter that requested preservation of all company electronic data was unreasonably overbroad and did not trigger a duty to preserve all such material).

188. *Cache La Poudre Feeds*, 244 F.R.D. at 623.

189. *See Oklahoma, ex rel. Edmondson v. Tyson Foods, Inc.*, No. 05-CV-329-GKF-SAJ, 2007 WL 1498973, at *6 (N.D. Okla. May 17, 2007) (urging the parties to use the Federal Rule of Civil Procedure 26(f) conference to address issues relating to electronically stored information and warning them to “be very cautious in relying upon any ‘safe harbor’ doctrine as described in new Rule 37[e]”); cases cited *supra* Part III.C.1.

190. *See Cache La Poudre Feeds*, 244 F.R.D. at 635–36. *But see Connor v. Sun Trust Bank*, 546 F. Supp. 2d 1360 (N.D. Cal. 2008) (holding that adverse inference instruction was appropriate sanction even though defendant took some reasonable steps to preserve certain evidence).

191. *See Connor*, 546 F. Supp. 2d at 1367 n.2 (recognizing counsel's efforts to preserve relevant data); *Cache La Poudre Feeds*, 244 F.R.D. at 629–30 (noting steps counsel could have taken to prevent data from being lost).

implement a records retention policy.¹⁹² Without such a policy, an organization may be exposed to a host of problems.¹⁹³ Its servers could be adversely affected by an unnecessary build-up of e-mail, spam and viruses.¹⁹⁴ What is more, a company's failure to have such a policy in place has been held to be grossly negligent when relevant data is lost.¹⁹⁵ Organizations that fail to implement such policies will likely increase the cost of their operations.¹⁹⁶

B. PREPARE FOR LAWSUITS IN ADVANCE OF ACTUAL LITIGATION

Litigation will happen—or at least organizations should act like it will.¹⁹⁷ Parties can prepare an internal process for how they will address issues relating to document retention before any additional lawsuits are filed.¹⁹⁸ This should undoubtedly include whether and when a retention practice should be modified.¹⁹⁹ It could also include designating a litigation response team among company personnel.²⁰⁰ In addition, criteria should be prepared to assess the likelihood of future litigation and the company's anticipated response.²⁰¹

C. CLOSELY FOLLOW RECORDS MANAGEMENT PRACTICES

Once in place, a document retention policy should be followed in the ordinary course of business. The reasonableness and effectiveness of a policy will likely be evaluated by how faithful an organization has been to the designated

192. Allman, *supra* note 54, at 16.

193. See PUBLIC HEARING, *supra* note 8, at 369.

194. *Id.*

195. Doe v. Norwalk Cmty. Coll., 248 F.R.D. 372, 379–80 (D. Conn. 2007).

196. This accords with one of the law's sacred maxims: "The law helps those who help themselves, generally aids the vigilant, but rarely the sleeping, and never the acquiescent." Hannan v. Dusch, 153 S.E. 824, 831 (Va. 1930).

197. See 2007 SEDONA PRINCIPLES, *supra* note 105, at 30; SEDONA CONFERENCE COMMENTARY ON LEGAL HOLDS, *supra* note 105, at 8.

198. See Shira A. Scheindlin & Jonathan M. Redgrave, *Special Masters and E-Discovery: The Intersection of Two Recent Revisions to the Federal Rules of Civil Procedure*, 30 CARDOZO L. REV. 347, 369 (2008); 2007 SEDONA PRINCIPLES, *supra* note 105, at 30.

199. *Cf.* Scheindlin & Redgrave, *supra* note 198, at 369 (raising the questions Rule 37(e) poses regarding what actions parties need to take to protect themselves from sanctions).

200. *Id.*

201. *Id.*

procedure.²⁰² A company that does not follow its retention practices closely may find it difficult to invoke the Safe Harbor and stave off discovery sanctions.²⁰³ Indeed, the defendants in *Doe v. Norwalk Community College* could not find shelter in the Safe Harbor due in part to their failure to follow their own retention policies.²⁰⁴

D. DO NOT EXCLUSIVELY RELY ON THE SAFE HARBOR FOR PROTECTION

Despite the protection the Safe Harbor may afford, parties should be realistic about the nature of its application. If a retention practice is not reasonable, is not effective, has not been followed, or is otherwise questionable, a litigant should not expect to be bailed out by Rule 37(e).²⁰⁵ To avoid that scenario, an organization can follow, among other things, the guidelines delineated by pertinent case law in Part Three regarding the aspects of a reasonable retention policy.²⁰⁶

V. CONCLUSION

The law governing records management practices under Rule 37(e) is beginning to take shape. Valuable insight and much needed guidance are being provided to litigants about how to manage electronic data in conjunction with litigation demands. As the Safe Harbor is further construed and interpreted, case law will evolve and better guide litigants in their efforts to preserve data when required, while also reducing operating expenses. This ongoing development of the Safe Harbor should help fulfill the vision of making litigation requirements, business practices, and best practices one and the same.²⁰⁷

202. See *Gipetti v. United Parcel Serv., Inc.*, No. C07-00812 RMW (HRL), 2008 WL 3264483, at *2–3 (N.D. Cal. Aug. 6, 2008).

203. *Doe v. Norwalk Cmty. Coll.*, 248 F.R.D. 372, 378 (D. Conn. 2007).

204. *Id.* (holding that retention practices were not “routine” within the meaning of Rule 37(e)).

205. See *supra* Part III.

206. *Id.*

207. PUBLIC HEARING, *supra* note 8, at 381.