NOTE

A Solution to the Spoliation Chaos: Rule 37(e)'s Unfulfilled Potential to Bring Uniformity to Electronic Spoliation Disputes

*Alexander B. Hastings**

INTRODUCTION

A gunshot rang out through northwest Houston as Police Officer Arthur Carbonneau shot to death Eli Escobar, Jr., an unarmed, fourteen-year-old boy.[1] Moments before the boy's death, witnesses report that he yelled out, "Mama, come and get me! Mama!"[2] Escobar was playing video games at a friend's house when Carbonneau, investigating a possible assault, interrupted the boys for questioning and ultimately discharged his firearm and shot the boy in the head.[3]

* J.D., expected May 2011, The George Washington University Law School; B.A., 2008, University of Dallas. I thank Brian Thavarajah and Tim Frey for their comments during the drafting of this Note, as well as Gloria Maier and *The George Washington Law Review* staff for outstanding editorial work. Also, I thank my parents, Michael and Kathleen Hastings, and my sister, Stephanie, for their enduring support.

1 Escobar v. City of Houston, No. 04-1945, 2007 WL 2900581, at *1 (S.D. Tex. Sept. 29, 2007). Although the underlying claim is unique, this case serves as an example of the contentious electronic discovery spoliation disputes that may arise in various situations among different types of organizations. *Id.* at *17–19.

2 Lise Olsen, *HPD Officer Who Shot Boy Failed Firearms Test*, HOUS. CHRON., Oct. 15, 2007, at A1.

3 *See Escobar*, 2007 WL 2900581, at *1; Elissa Rivas, *Memorial Held for Teen Killed by HPD Officer*, KTRK-TV (Oct. 21, 2008), http://abclocal.go.com/ktrk/story?section=news/local&id=6517970.

Although a separate criminal proceeding resulted in Carbonneau's conviction for negligent homicide, the incident left a tragic void in the Escobar family.[4]

Following the shooting, the Escobars brought a civil action against the City of Houston and the Houston Police Department ("HPD") seeking damages for the wrongful death of their son.[5] The Escobars sought discovery of HPD's electronic communications during the twenty-four hours after the shooting.[6] Although the Escobars requested the material within sixty days after the incident, and despite HPD's policy to retain electronic materials for ninety days, HPD deleted these electronic materials without providing them to the Escobars.[7] Believing the deleted communications were crucial to proving their civil case against the HPD, the Escobars moved for discovery sanctions against the department.[8]

Similar to many organizations—including large corporations, government agencies, and small businesses—HPD faced several challenges in preserving electronic data. In this instance, HPD responded to the motion for sanctions by relying on Federal Rule of Civil Procedure 37(e)'s safe harbor provision. This Rule prevents courts from issuing sanctions when responsive information is lost in good faith during the routine operation of electronic information systems.[9]

Despite the fact that the electronic communications were deleted after the Escobars had notified HPD of their claim, the court accepted HPD's Rule 37(e) defense.[10] The court explained that sanctions would not be imposed because the electronic communications were deleted in the routine operation of HPD's electronic system and there existed no indication that HPD acted with bad faith.[11] This finding is striking in light of HPD's document retention policy, which required the retention of electronic records for at least ninety days after their creation.[12] In the end, HPD reached a civil settlement with the Escobar family.[13] This settlement, however, does not excuse the court's approach to Rule 37(e)'s safe harbor provision. As discussed below,

---

4 *See Escobar*, 2007 WL 2900581, at *4–5.

5 *See id.* at *5; Olsen, *supra* note 2.

6 *Escobar*, 2007 WL 2900581, at *17.

7 *See id.* at *17–18.

8 *See id.* at *17.

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

10 *Escobar*, 2007 WL 2900581, at *17–18.

11 *Id.* at *18.

12 *See id.* at *17.

13 Rivas, *supra* note 3.

the *Escobar* decision illustrates just one of many unfortunate instances in which courts have failed to give effect to the intentions of those who supported the adoption of Rule 37(e)'s safe harbor protection.

As illustrated by this situation, the need to address electronic discovery and the questions that surround this issue becomes more pressing with each passing day. For instance, in 2009, a court in every federal circuit addressed the issue of electronic discovery.[14] Moreover, the number of disputes regarding these matters nearly doubled in 2009 compared to 2008.[15] These disputes consume precious judicial resources and can result in sanctions for the parties involved. In 2009, courts imposed sanctions related to electronic discovery in over seventy percent of the instances in which such sanctions were sought.[16] Moreover, the issue of electronic spoliation becomes even more worrisome for practitioners as courts increasingly sanction attorneys who represent a spoliating party.[17] Litigants cannot ignore electronic discovery concerns. As technology increasingly penetrates our society, disputes over electronic discovery will become more complex.

The Judicial Conference Committee on Rules of Practice and Procedure ("Judicial Conference"), which consists of federal judges who create policy affecting the administration of federal courts,[18] recently sought to develop a partial solution to the chaos surrounding electronic discovery. To this end, the Judicial Conference proposed Rule 37(e) to alleviate the worries of parties who fear that they will be subject to sanctions despite their best efforts to maintain electronic information.[19] The Rule provides that "[a]bsent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result

---

14 Gibson, Dunn & Crutcher LLP, *2009 Year-End Electronic Discovery and Information Law Update*, GIBSON DUNN (Jan. 15, 2010), http://www.gibsondunn.com/publications/Pages/2009YearEndElectronicDiscoveryUpdate.aspx.

15 *See id.*

16 *See id.*

17 *See, e.g.*, Swofford v. Eslinger, 671 F. Supp. 2d 1274, 1288–89 (M.D. Fla. 2009) (imposing attorney's fees and costs on the defendant's in-house counsel); Green v. McClendon, 262 F.R.D. 284, 291–92 (S.D.N.Y. 2009) (imposing attorney's fees and costs on the defendant's attorney).

18 *See Judicial Conference of the United States*, USCOURTS.GOV, http://www.uscourts.gov/FederalCourts/JudicialConference.aspx (last visited Jan. 13, 2011).

19 *See* COMM. ON RULES OF PRACTICE & PROCEDURE, JUDICIAL CONFERENCE OF THE U.S., REPORT OF THE JUDICIAL CONFERENCE 23–24, 33 (2005) [hereinafter REPORT OF THE JUDICIAL CONFERENCE], *available at* http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Reports/ST09-2005.pdf.

of the routine, good-faith operation of an electronic information system."[20]

This Rule possesses great promise to calm the storm that surrounds electronic discovery. But for the Rule to have its full effect, courts must move away from applying it in an apparently ad hoc fashion and strive for a more unified interpretation of the Rule's good-faith exception to discovery sanctions.[21]

This Note presents a two-part solution—the Uniform Safe Harbor Standard—that evaluates whether to impose sanctions in light of Rule 37(e)'s safe harbor provision. Specifically, when evaluating a claim for sanctions for destruction of material that occurred before the filing of a complaint, the court should accept a Rule 37(e) defense unless the moving party demonstrates that the opposing party deleted electronic information with the intent to conceal evidence or with a willful blindness to the fact that responsive information would be lost. Once a complaint has been filed, however, the court should accept a Rule 37(e) defense only if the party that destroyed electronic material postcomplaint demonstrates that it acted reasonably in reference to its discovery obligation. The Uniform Safe Harbor Standard introduced in this Note demonstrates that by shifting the burden of proof and the required level of culpability based on the status of the litigation, the court may create a consistent interpretation of Rule 37(e)'s safe harbor defense. In turn, this consistency would provide companies with guideposts to structure their document retention policies and litigation holds.

Before arriving at this solution, Part I of this Note begins by discussing electronic discovery generally and providing the necessary background to appreciate the challenges that arise in this emerging area of the law. After discussing background principles, this Note turns to a consideration of Rule 37(e) itself. Part II addresses the rationale behind the Rule's adoption, as well as the Rule's drafting history and text. After introducing the Rule, Part III examines its current interpretation. This discussion demonstrates instances in which it appears that courts failed to apply the Rule when it was intended to be applied, as well as situations in which courts implemented the Rule beyond its intended scope. Part IV provides a detailed description of the Uniform Safe Harbor Standard for interpreting Rule 37(e). In addition, this Part applies the Note's interpre-

---

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

21 *Cf.* Gibson, Dunn & Crutcher LLP, *supra* note 14 (discussing the various judicial approaches to discovery sanctions).

tation to various cases to demonstrate that this approach would create desirable and uniform results.

I. Background of Electronic Discovery

Before turning to the issue of interpreting Rule 37(e), it is important to discuss electronic discovery generally and to understand the challenges facing those who practice law in this field. This Part attempts to lay the foundation by addressing many of the principal concerns involved in the management of electronic information. Specifically, this Part first addresses document retention policies and litigation holds; it then turns to an explanation of spoliation and the potential sanctions that confront parties who lose responsive electronic information.

Any discussion of electronic discovery should incorporate the analysis of discovery obligations developed by Judge Scheindlin of the Southern District of New York. Judge Scheindlin initially embarked on a detailed description of a party's discovery obligations during the *Zubulake v. UBS Warburg LLC* litigation.[22] Taken as a whole, five of the *Zubulake* opinions represent a place in the jurisprudence of electronic discovery similar to the foundational nature that *Chevron U.S.A. Inc. v. Natural Resources Defense Council, Inc.*[23] holds in administrative law. Following the *Zubulake* litigation, Judge Scheindlin further elaborated on a party's discovery obligations in *Pension Committee of University of Montreal Pension Plan v. Banc of America Securities, LLC*.[24]

In establishing the foundational requirements of electronic discovery, Judge Scheindlin's opinions explore the duty to preserve and the resulting spoliation sanctions when a party breaches this duty.[25] Her analysis of these topics has been incorporated in the discussion below.

---

22 *See* Zubulake v. UBS Warburg LLC (*Zubulake VI*), 382 F. Supp. 2d 536 (S.D.N.Y. 2005); Zubulake v. UBS Warburg LLC (*Zubulake V*), 229 F.R.D. 422 (S.D.N.Y. 2004); Zubulake v. UBS Warburg LLC (*Zubulake IV*), 220 F.R.D. 212 (S.D.N.Y. 2003); Zubulake v. UBS Warburg LLC (*Zubulake III*), 216 F.R.D. 280 (S.D.N.Y. 2003); Zubulake v. UBS Warburg LLC (*Zubulake I*), 217 F.R.D. 309 (S.D.N.Y. 2003).

23 Chevron U.S.A. Inc. v. Natural Res. Def. Council, Inc., 467 U.S. 837 (1984).

24 Pension Comm. of Univ. of Montreal Pension Plan v. Banc of Am. Sec., LLC, 685 F. Supp. 2d 456 (S.D.N.Y. 2010).

25 *See Zubulake V*, 229 F.R.D. at 436–38.

A. Electronic Discovery: Document Retention Policies and Litigation Holds

Discovery rules allow companies to delete outdated and unresponsive data in accordance with reasonable document retention polices. Nevertheless, companies must carefully construct document retention policies because practices that delete responsive electronic material may result in harsh sanctions.[26] This Section attempts to provide a description of the delicate balance between document retention and deletion by considering the basic requirements of electronic discovery, namely, document retention policies and litigation holds.

1. Document Retention Policies

Document retention policies are becoming increasingly important with the dawn of electronic discovery. Somewhat counterintuitively, these policies set forth a company's plan through which it destroys paper documents and electronic information.[27] The Supreme Court recognized the need for document retention polices in *Arthur Andersen, LLP v. United States*.[28] The Court explained that companies routinely use document retention policies and may direct their employees to destroy records in accordance with such policies.[29]

Document retention policies existed well before electronic discovery, but the purpose behind these policies has evolved. Originally, document retention polices aimed to eliminate documents for the sake of security, to ensure such documents did not land in the wrong hands.[30] With the growth of electronic systems, companies must delete information not only for security's sake, but also because retaining excessive amounts of electronic information is both highly unproductive and practically impossible.

Retaining large amounts of unnecessary information proves cost prohibitive and impractical for several reasons. First, retaining excessive information requires large amounts of storage space.[31] Second, retaining large amounts of data saddles parties with the high cost of reviewing such data during litigation.[32] Specifically, as one commenta-

---

26 Gibson, Dunn & Crutcher LLP, *supra* note 14.

27 Arthur Andersen LLP v. United States, 544 U.S. 696, 704 (2005).

28 *Id.*

29 *See id.*

30 *See id.*

31 Martin H. Redish, *Electronic Discovery and the Litigation Matrix*, 51 DUKE L.J. 561, 590 (2001) (explaining that companies may retain thousands of backup tapes, each of which may contain enough information to equal up to 1500 boxes of paper documents).

32 COMM. ON RULES OF PRACTICE & PROCEDURE, JUDICIAL CONFERENCE OF THE U.S.,

tor notes, document retention policies that aim to retain vast levels of information are inefficient because they result in the need to review excessive amounts of irrelevant and duplicative information.[33]

With ninety-nine percent of responsive documents currently stored electronically,[34] it should come as no surprise that the average price of performing electronic discovery during the litigation of a single matter has reached over $1.5 million,[35] with the review costing around $2000 for each gigabyte of information.[36] These figures become overwhelming when combined with the realization that ninety percent of U.S. corporations are engaged in litigation[37] and a company with over $1 billion in revenue can expect over 140 active lawsuits at any given time.[38]

To illustrate more vividly the astronomical costs associated with document retention policies that take a "save everything" approach to electronic information, the legal department of DuPont, an American chemical company, studied a single document production request.[39] The response to this request took over three years and involved the review of over 75 million documents.[40] In the end, DuPont concluded that more than fifty percent of the documents reviewed should have been destroyed in accordance with a reasonable document retention policy.[41] The unnecessary work of reviewing the documents kept beyond their retention period resulted in an additional cost of over $12 million.[42] Combining this example with the hundreds of lawsuits managed by corporations at any given time demonstrates the importance

---

EXCERPT FROM THE REPORT OF THE JUDICIAL CONFERENCE 4–5 (2005), *available at* http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/supct1105/Excerpt_STReport_CV.pdf.

33 Gal Davidovitch, Comment, *Why Rule 37(e) Does Not Create a New Safe Harbor for Electronic Evidence Spoliation*, 38 SETON HALL L. REV. 1131, 1133 (2008) (noting that "Rule 37[e] responds to a distinctive and necessary feature of computer systems—the recycling, overwriting, and alteration of electronically stored information that attends normal use"); *see also* Pension Comm. of Univ. of Montreal Pension Plan v. Banc of Am. Sec., LLC, 685 F. Supp. 2d 456, 461 (S.D.N.Y. 2010) (noting the "vast amount of electronic information" created by companies).

34 *See E-Discovery Solution Offering*, MIKE 2.0, http://mike2.openmethodology.org/wiki/EDiscovery_Solution_Offering (last visited Jan. 9, 2011).

35 *Id.*

36 *See* BRIAN DIRKING, ORACLE, LOWERING E-DISCOVERY COST THROUGH ENTERPRISE RECORDS AND RETENTION MANAGEMENT 4 (2007), www.oracle.com/technetwork/middleware/content-management/records-retention-whitepaper-130956.pdf.

37 *E-Discovery Solution Offering*, *supra* note 34.

38 DIRKING, *supra* note 36, at 3.

39 *Id.* at 4.

40 *Id.*

41 *See id.*

42 *Id.*

of creating and following document retention polices that allow for the reasonable destruction of data.

Third, in addition to being cost prohibitive, the dynamic nature of electronic information means that indefinite storage of electronic information would require constant maintenance. Specifically, separating electronic information from the system that created it would likely render it incomprehensible.[43] Therefore, indefinite storage requires companies to maintain the electronic systems that created their information. Maintaining systems that read the various forms of electronic information produced by a company, however, can become extremely expensive and burdensome.[44] Moreover, electronic information cannot simply sit in a box in storage, as can paper documents, but instead must be routinely refreshed to maintain the integrity of the data.[45] Therefore, document retention policies serve a crucial role in electronic discovery by ensuring that discovery does not become too costly or impractical. As discussed in the next Subsection, however, the costs of retention must be incurred when the potential for litigation gives rise to a duty to preserve.

2. The Duty to Preserve and Litigation Holds

Recognizing a litigant's duty to preserve remains central to a proper understanding of electronic discovery. A party's planned destruction of electronic material in accordance with its document retention policy must cease and a litigation hold must be implemented when a duty to preserve arises. This duty to preserve may be imposed when a party is served with a lawsuit,[46] receives a document production request,[47] is given notice of a potential claim,[48] or can reasonably expect that litigation may arise.[49]

---

43 *See* Davidovitch, *supra* note 33, at 1133.

44 *Id.* at 1134.

45 George Parapadakis, *8 Things You Need to Know About Information Risk*, DIGITAL LANDFILL (June 22, 2009, 6:30 AM), http://aiim.typepad.com/aiim_blog/2009/06/8-things-you-need-to-know-about-information-risk.html (explaining that "long-term preservation, media refresh and format refresh, need to be considered proactively").

46 *See* Kronisch v. United States, 150 F.3d 112, 126–27 (2d Cir. 1998).

47 Trigon Ins. Co. v. United States, 204 F.R.D. 277, 287 (E.D. Va. 2001).

48 *See Kronisch*, 150 F.3d at 126.

49 *See, e.g.*, Jordan F. Miller Corp. v. Mid-Continent Aircraft Serv., Inc., No. 97-5089, 1998 WL 68879, at *5 (10th Cir. Feb. 20, 1998) (holding that the duty to preserve arises when a party "knows or should know [information] is relevant to imminent or ongoing litigation"); *Zubulake IV*, 220 F.R.D. 212, 218 (S.D.N.Y. 2003) (holding that when a party "reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a 'litigation hold' to ensure the preservation of relevant documents").

This concept becomes especially important in electronic discovery jurisprudence because courts will rely on the threshold question of whether a duty to preserve has arisen to determine whether sanctions should even be considered.[50] Judge Scheindlin, in *Zubulake*, explained the duty to preserve in the electronic discovery context. In her opinion, she recognizes that the duty to preserve invokes two considerations: the time when the duty arises and the scope of the duty.[51] As to the first consideration, the duty does not arise merely based on the possibility of litigation.[52] Instead, the duty arises at the point in time when a party has a concrete belief that litigation might arise.[53] Furthermore, even when foreseeable litigation triggers the duty, the party does not need to preserve all of its electronic information.[54] Instead, Judge Scheindlin explains that a party must refrain from "destroy[ing] unique, relevant evidence that might be useful to an adversary."[55] In sum, a party reasonably anticipating litigation must not destroy relevant or potentially responsive material.[56]

Notably, attorneys carry a heavy responsibility to ensure that their clients comply with the duty to preserve.[57] The role of an attorney when the duty to preserve arises includes more than merely informing their client of a litigation hold; they must take an active role in ensuring their client complies with the duty to preserve.[58] This compliance includes halting the intentional deletion of material per-

---

50 *See* Fujitsu Ltd. v. Fed. Express Corp., 247 F.3d 423, 436 (2d Cir. 2001) (noting that "[t]he obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation").

51 *See Zubulake IV*, 220 F.R.D. at 216 (stating that "the duty to preserve involves two related inquiries: *when* does the duty to preserve attach, and *what* evidence must be preserved?").

52 *See id.* at 217.

53 *See id.* (indicating that a duty to preserve is not triggered "[m]erely because one or two employees contemplate the possibility that a fellow employee might sue," but instead arises only when there is a widespread belief among the relevant individuals that there exists a strong possibility the employee will file a complaint).

54 *See id.* at 217–18.

55 *See id.* at 217.

56 *See id.* at 217–18.

57 Brian C. Dalrymple & Daniel Harshman, *Electronic Discovery: What You Need to Know and What It May Cost if You Don't*, NIXON PEABODY (Oct. 27, 2004), http://www.nixonpeabody.com/publications_detail3.asp?Type=P&PAID=66&ID=771; *see also Zubulake V*, 229 F.R.D. 422, 432 (S.D.N.Y. 2004) ("Proper communication between a party and her lawyer will ensure (1) that all relevant information (or at least all sources of relevant information) is discovered, (2) that relevant information is retained on a continuing basis[,] and (3) that relevant non-privileged material is produced to the opposing party.").

58 Dalrymple & Harshman, *supra* note 57.

formed by electronic systems.[59] Moreover, the attorney must ensure that parties affirmatively confirm that the normal operations of computer systems will not destroy potentially responsive electronic material.[60]

The duty to preserve may be best illustrated by way of an example. Consider the case of *103 Investors I, L.P. v. Square D Co.*,[61] in which a building owner brought suit against an electrical-parts manufacturer following a fire. The building owner asserted that a failure to warn about the proper care of an electrical busway caused the fire.[62] The building owner, however, had disposed of large portions of the manufacturer's busway that were damaged in the fire.[63] Unfortunately for the building owner, the discarded parts of the busway were those that would have contained a warning label, if one had been present.[64] As such, the court sanctioned the building owner for the destruction of the busway because it served as evidence relevant to ongoing litigation.[65]

Although it falls outside the electronic discovery context, *103 Investors I* represents a straightforward case of a violation of the duty to preserve because the litigation had already commenced. In circumstances such as this case, one can easily see that both parties had notice of litigation.[66] More difficult situations arise when a party claims that the spoliating party violated the duty to preserve because it should have reasonably anticipated litigation.[67]

The debate regarding when the duty to preserve arises falls outside the scope of this Note. For purposes of the following discussion, one should recognize that the potential for sanctions and a Rule 37(e) defense only apply after a party's duty to preserve arises.[68] In situations in which no duty to preserve has arisen, there is no requirement that a party deviate from its normal document retention policy,

---

59 *See* Convolve, Inc. v. Compaq Computer Corp., 223 F.R.D. 162, 176 (S.D.N.Y. 2004).

60 *Id.* at 176–77.

61 103 Investors I, L.P. v. Square D Co., 470 F.3d 985, 987 (10th Cir. 2006).

62 *See id.* A busway consists of four aluminum bars that run the vertical length of a building and serve to distribute electricity throughout the building. *Id.*

63 *Id.* at 988.

64 *See id.*

65 *See id.* at 988–89.

66 *See id.* at 987.

67 *See, e.g.*, Fujitsu Ltd. v. Fed. Express Corp., 247 F.3d 423, 436 (2d Cir. 2001) (resolving a conflict between parties that debated whether a duty to preserve has arisen); *see also* SHIRA A. SCHEINDLIN ET AL., ELECTRONIC DISCOVERY AND DIGITAL EVIDENCE: CASES AND MATERIALS 402–03 (2009).

68 *See Fujitsu Ltd.*, 247 F.3d at 436.

and as such, the party will not be subject to sanctions.[69] Accordingly, this Note will assume that a duty to preserve has arisen and will focus on the scope of the parties' responsibilities to preserve information.

B. The Consequences of Spoliation: Why Rule 37(e) Matters

Once a duty to preserve arises, the parties have an obligation to institute a litigation hold.[70] As discussed above, the litigation hold represents a party's need to preserve responsive material and avoid the spoliation of material by stopping the normal operation of document retention policies.[71] Spoliation occurs when a party destroys or materially alters information relevant to "pending or reasonably foreseeable litigation."[72] Setting aside the availability of Rule 37(e) protections, a party can be sanctioned in various ways as a result of its spoliation of electronic information.[73]

1. The Purpose and Source of Spoliation Sanctions

Courts provide a twofold rationale for issuing sanctions. By sanctioning a party, the court aims both to punish the spoliator and remedy the potential prejudice caused by the inaccessibility of the lost information.[74] No firm precedent exists regarding what sanctions must be applied in certain circumstances. Instead, the decision regarding the appropriate sanction rests in the "sound discretion of the trial judge, and is assessed on a case-by-case basis."[75]

The power of courts to sanction parties comes from two separate sources. First, courts possess the inherent power to sanction parties in carrying out their judicial duties.[76] The inherent power of the courts to sanction arises from the understanding that without certain powers, courts are unable to accomplish their judicial tasks and maintain re-

---

69 *See id.* (requiring the defendant to show that the plaintiff had a duty to preserve damaged freight containers before entering into any discussion of possible spoliation sanctions).

70 *See* Jordan F. Miller Corp. v. Mid-Continent Aircraft Serv., Inc., No. 97-5089, 1998 WL 68879, at *5 (10th Cir. Feb. 20, 1998).

71 *See* Disability Rights Council v. Wash. Metro. Transit Auth., 242 F.R.D. 139, 146 (D.D.C. 2007) (demonstrating that Rule 37(e) requires a party to halt normal document destruction procedures through a litigation hold at the onset of litigation).

72 *See* Pension Comm. of Univ. of Montreal Pension Plan v. Banc of Am. Sec., LLC, 685 F. Supp. 2d 456, 465 (S.D.N.Y. 2010); *see also Zubulake IV*, 220 F.R.D. 212, 216 (S.D.N.Y. 2003).

73 Andrew Hebl, *Spoliation of Electronically Stored Information, Good Faith, and Rule 37(e)*, 29 N. ILL. U. L. REV. 79, 86 (2008).

74 *See* Davidovitch, *supra* note 33, at 1142.

75 Fujitsu Ltd. v. Fed. Express Corp., 247 F.3d 423, 436 (2d Cir. 2001) (citation omitted).

76 Chambers v. NASCO, Inc., 501 U.S. 32, 44–45 (1991).

spect and public support for the judicial system.[77] The Supreme Court recognizes that that inherent power must be preserved, and that such powers cannot be disturbed by the Federal Rules of Civil Procedure.[78] Notably, a safe harbor provision that protects litigants from spoliation sanctions based on a court's inherent powers does not exist.[79]

In addition to a court's inherent powers, it may also issue sanctions under Rule 37 when the party "fails to obey [a court] order to provide or permit discovery."[80] In particular, sanctions for the spoliation of electronic discovery arise when a party's destruction of responsive material renders it unable to fulfill discovery obligations, including complying with a court order or disclosing information.[81]

2. Types of Sanctions Imposed on a Spoliating Party

The importance of a Uniform Safe Harbor Standard becomes apparent when one recognizes the gravity of the sanctions that may be imposed on a party responsible for the spoliation of information. The seriousness of potential sanctions appeared in the *Zubulake* controversy when the court imposed an adverse inference against the defendant.[82] The adverse inference, or spoliation instruction, allows or requires the jury to infer that spoliated materials would be unfavorable to the party responsible for the spoliation.[83] After Judge Scheindlin resolved questions related to the accessibility of the backup tapes and cost shifting, the parties entered a fierce debate regarding the defendant's destruction of responsive e-mails that were located on the backup tapes.[84] Because these tapes were crucial to her employment discrimination claim, the plaintiff requested that the court impose an adverse inference against the defendant.[85] Recognizing that the defendant failed to properly preserve and produce the e-mails,

---

77 *See id.* at 43.

78 *See id.* at 46.

79 *See* Davidovitch, *supra* note 33, at 1143–44; *see also* Pension Comm. of Univ. of Montreal Pension Plan v. Banc of Am. Sec., LLC, 685 F. Supp. 2d 456, 465–66 (S.D.N.Y. 2010).

80 *See* Kopitar v. Nationwide Mut. Ins. Co., 266 F.R.D. 493, 495 (E.D. Cal. 2010) (internal quotation marks and citations omitted); *see also* Davidovitch, *supra* note 33, at 1144.

81 FED. R. CIV. P. 37(b)–(d), (f); *see also, e.g.*, Richard Green (Fine Paintings) v. McCledon, 262 F.R.D. 284, 288, 292 (S.D.N.Y. 2009) (holding that Rule 37 would permit issuance of sanctions against a party that destroyed relevant electronic data prior to the filing of a lawsuit because that party's spoliation rendered it unable to comply with the court's discovery order).

82 *Zubulake V*, 229 F.R.D. 422, 439–40 (S.D.N.Y. 2004).

83 *See* Hebl, *supra* note 73, at 86.

84 *Zubulake V*, 229 F.R.D. at 426–30.

85 *See id.* at 439.

Judge Scheindlin instructed the jury to infer that any e-mail that the defendant failed to produce would be unfavorable to the defense.[86]

In addition to an adverse inference, a party can be subject to monetary sanctions or a default judgment.[87] Generally, the more egregious the loss of information—such as the intentional deletion of material—the greater the sanction that will be imposed.[88] Courts determine the appropriate sanction in each case based on the prejudice that the spoliation causes to the nonspoliating party and the spoliating party's mens rea.[89] Similar to the conflict regarding the proper mens rea for the good-faith standard of Rule 37(e), there does not exist a clear consensus regarding the required level of mens rea to impose each sanction.[90] For purposes of the discussion below, however, one should realize that a conflict exists and the spoliating party's mens rea plays an important role throughout the consideration of whether discovery sanctions will be imposed. Therefore, these serious sanctions reveal the importance of developing a Uniform Safe Harbor Standard

---

86 *See id.* at 439–40.

87 *See* Hebl, *supra* note 73, at 86; *see, e.g.*, Pension Comm. of Univ. of Montreal Pension Plan v. Banc of Am. Sec., LLC, 685 F. Supp. 2d 456, 469–70 (S.D.N.Y. 2010) (explaining that the gravity of the sanction depends on a party's intent and the level of prejudice caused by the spoliation).

88 *Compare In re* Krause, 367 B.R. 740, 770 (D. Kan. 2007) (suggesting that a willful and intentional destruction of evidence will likely result in an adverse-inference instruction), *and* Gibson, Dunn & Crutcher LLP, *supra* note 14 (same), *with* United Med. Supply Co. v. United States, 77 Fed. Cl. 257, 275–76 (2007) (imposing monetary sanctions and not an adverse inference because the defendant's conduct was reckless, rather than intentional).

89 *See* Hebl, *supra* note 73, at 84; *see, e.g.*, *Pension Comm. of Univ. of Montreal Pension Plan*, 685 F. Supp. 2d at 469.

90 *See United Med. Supply Co.*, 77 Fed. Cl. at 266–67; Hebl, *supra* note 73, at 87–88 (noting that some courts require intentional or reckless conduct, whereas others have accepted negligent conduct). The federal circuits have different approaches to the required level of culpability. SCHEINDLIN ET AL., *supra* note 67, at 387–88 (discussing the differing mens rea requirements for each level). For instance, a "distinct minority" of circuits require a showing of "bad faith" before issuing any sanctions. *United Med. Supply Co.*, 77 Fed. Cl. at 266; *see also* S.C. Johnson & Son v. Louisville & Nashville R.R., 695 F.2d 253, 258–59 (7th Cir. 1982); Vick v. Tex. Emp't Comm'n, 514 F.2d 734, 737 (5th Cir. 1975). Other courts may still require "bad faith" for some sanctions, such as default judgments and adverse inferences, but not for others. *See* 103 Investors I, L.P. v. Square D Co., 470 F.3d 985, 988–89 (10th Cir. 2006); Harlan v. Lewis, 982 F.2d 1255, 1260 (8th Cir. 1993). Still others require no showing of purposeful conduct before issuing any of the sanctions, but instead require merely a showing of fault. *See* Sacramona v. Bridgestone/Firestone, Inc., 106 F.3d 444, 447 (1st Cir. 1997); Vodusek v. Bayliner Marine Corp., 71 F.3d 148, 156–57 (4th Cir. 1995). To make the conflict surrounding the proper level of mens rea even more confusing, the terms do not always mean the same thing. For instance, a reference to "bad faith" has been interpreted to encompass things such as intentional conduct, recklessness, or gross negligence. *See United Med. Supply Co.*, 77 Fed. Cl. at 266–67.

to provide consistency for parties seeking to satisfy their discovery obligations.

II. RULE 37(E): A POTENTIAL SOLUTION

To arrive at a proper understanding of the good-faith exception of Rule 37(e), it is important to evaluate the history of the Rule's development and the text of the Rule. As the discussion above illustrates, Rule 37(e) arose during a time of great uncertainty in the realm of electronic discovery.[91] The Judicial Conference recognized the need for rules addressing electronic discovery.[92] To this end, it introduced a series of new rules, including Rule 37(e).[93] An examination of the history of the Rule, particularly the need for its adoption and its text, facilitates a better understanding of the purpose of the Rule's safe harbor provision.

A. The Development of Rule 37(e)

Rule 37(e) aims to cure the volatility that exists concerning sanctions for electronic discovery. In particular, a solution had to be developed that answered the problems unique to computer systems, including their propensity to automatically alter and delete electronic information.[94] For instance, computer systems routinely alter and overwrite data as more recent information becomes available.[95] There are countless examples in which the routine operation of computer systems results in the deletion of electronic material. For instance, nearly all companies enable their software to delete e-mails that have been sent or received after a certain time.[96] Moreover, most backup systems recycle the backup media at predetermined intervals despite the fact that such recycling deletes electronically stored information from the backup media.[97] This dynamic nature of electronic information, inter alia, required the adoption of this new Rule, which offers

---

91 *See supra* p. 849.

92 *See* REPORT OF THE JUDICIAL CONFERENCE, *supra* note 19, at 22–23.

93 *See id.* at 25.

94 *See id.* at 22–23.

95 *See id.* at 23.

96 *See* GEORGE L. PAUL & BRUCE H. NEARON, THE DISCOVERY REVOLUTION: E-DISCOVERY AMENDMENTS TO THE FEDERAL RULES OF CIVIL PROCEDURE 24 (2006); *see also* CONTOURAL, INC., HOW LONG SHOULD EMAIL BE SAVED? 3–4 (2007), http://eval.veritas.com/mktginfo/enterprise/white_papers/ent-whitepaper_how_long_should_email_be_saved.en-us.pdf (discussing the practical need to delete e-mails after a certain point, which can range from one to fifty years).

97 *See* PAUL & NEARON, *supra* note 96, at 25.

protection for information lost in the routine, good-faith operation of computer systems.

Nevertheless, while Rule 37(e) should provide protection for instances in which electronic discovery tends to act differently than traditional paper discovery, courts must still determine the specific situation in which Rule 37(e) applies. In particular, courts must establish the required level of mens rea that will allow a party to claim that it lost information in the "routine, good-faith operation" of its computer systems.[98] As discussed in the next Section, this reference to "good faith" came as a compromise between those who advocated two different levels of mens rea. Therefore, determining the required level of mens rea remains challenging.

B. Rule 37(e): What Does the Text Say?

To arrive at a better understanding of when a party should be entitled to shelter under Rule 37(e)'s safe harbor, one must turn to the text of the Rule. This Section analyzes the important parts of Rule 37(e) to evaluate the ways in which they affect a party's ability to claim protection under this Rule.[99]

Turning first to the Rule's requirement that the party lose the information during the "routine operation" of its electronic information systems, little debate exists regarding whether an individual's actions may fall within this provision.[100] The routine operation of a computer system includes more than simply a "periodic or habitual" operation of an electronic system.[101] In particular, the Judicial Conference suggests that to be routine, the operation must be "designed, programmed, and implemented to meet the party's technical and business needs."[102] To this end, the court must examine the electronic system as a whole and determine whether the system operated to

---

98 *See* FED. R. CIV. P. 37(e).

99 Notably absent from this Section is a discussion of the Rule's reference to "exceptional circumstances." Although this Note focuses on the good-faith standard contained in the Rule, it is appropriate to mention that the text's reference to "exceptional circumstances" has served as a source of significant debate. In some situations, a court will recognize that certain "exceptional circumstances" will bar a party from seeking protection under Rule 37(e), thereby keeping the court from even evaluating whether good faith existed. *See* REPORT OF THE JUDICIAL CONFERENCE, *supra* note 19, app. at C-88. While the question of what qualifies as an "exceptional circumstance" falls outside the scope of this Note, it should be noted that in certain situations, especially where the loss of electronic information results in extreme prejudice, a party will be barred from seeking safe harbor, regardless whether that party acted in "good faith." *See id.*

100 *See* Davidovitch, *supra* note 33, at 1137.

101 *See id.* at 1136.

102 *See* REPORT OF THE JUDICIAL CONFERENCE, *supra* note 19, app. at C-87.

generally serve the technical and business needs of the party.[103] As such, the court will evaluate the computer system as a whole and not consider how the system operated in the specific instance that resulted in the loss of responsive information.[104]

The central debate surrounding the text of Rule 37(e) lies in the requirement that the information be lost in "good faith." On the surface, the good-faith clause ensures that a party does not take advantage of the routine operation of its computer systems to destroy responsive electronic information.[105] By itself, however, the good-faith clause does not reveal the levels of mens rea at which a party may still claim protection under the safe harbor provision. Considering the drafting history of the Rule reveals that the Judicial Conference intended the good-faith standard to serve as a middle ground between the alternatives of a strict intentional or narrow reasonableness standard.[106]

The drafting history of the Rule, which indicates that the Judicial Conference originally proposed two versions, demonstrates the intended fluctuation in the standard. The initial proposal stated that a party would be entitled to safe harbor protection to the extent that its actions qualify as reasonable.[107] In other words, the Judicial Conference initially did not intend to protect intentional, reckless, or negligent conduct. This proposed version of the Rule contained an important footnote, however, that made reference to a variation of the Rule using an intentional or reckless standard.[108]

During the comment period, many individuals expressed concern over the narrowness of the first proposed Rule and the broad scope of the version proposed in the footnote.[109] The proposed versions of the Rule would either allow parties virtually no protection unless their conduct qualified as reasonable or would provide too much protection

---

103 *See* Davidovitch, *supra* note 33, at 1136.

104 *See id.* The consideration of "routine operation" does not center on whether the electronic system acted in a routine manner in the particular circumstance before the court, but instead whether the electronic system lost information due to its regular process designed to meet the technical and business needs of the company. *See id.*

105 REPORT OF THE JUDICIAL CONFERENCE, *supra* note 19, app. at C-87.

106 *See* LEE H. ROSENTHAL, ADVISORY COMM. ON THE FED. RULES OF CIVIL PROCEDURE, JUDICIAL CONFERENCE OF THE U.S., REPORT OF THE CIVIL RULES JUDICIAL CONFERENCE 83–86 (2005), *available at* http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Reports/CV5-2005.pdf.

107 REPORT OF THE JUDICIAL CONFERENCE, *supra* note 19, app. at C-88.

108 *See* ROSENTHAL, *supra* note 106, at 84.

109 *See id.*

and allow sanctions for only the most egregious intentional conduct.[110] The consensus, however, appeared to favor a more narrow approach to the Rule where safe harbor would be provided only in the instances in which a party's conduct could be considered reasonable.[111]

After receiving these comments, the Judicial Conference recognized that a reasonableness standard would offer "'no meaningful protection, but rather [would] protect against conduct unlikely to be sanctioned in the first place.'"[112] Accordingly, instead of choosing either proposed Rule, the Judicial Conference settled on the good-faith standard, which it identified as being an intermediate approach.[113]

Therefore, the Rule adopted consisted of a compromise between the reasonableness and intentional standards by referring to "good faith." The hesitancy of the Judicial Conference to fully adopt an intentional or reasonableness standard demonstrates that the good-faith standard should not be read as a firm standard, but rather should be interpreted as a malleable approach to mens rea.

The Uniform Safe Harbor Standard proposed by this Note carries this compromise one step further and, by varying the mens rea requirement based on the point in time during the litigation when the destruction occurred, proposes an even more refined compromise between those who advocated different levels of mens rea. As demonstrated by the next Part, this solution is necessary because of the inconsistent interpretations of Rule 37(e)'s reference to "good faith."

III. CURRENT INTERPRETATIONS OF RULE 37(E)

Before turning to the proposed Uniform Safe Harbor Standard, this Part considers the ways in which courts have interpreted Rule 37(e) in practice. An examination of the caselaw makes apparent that, overall, courts have erred on the side of caution and have narrowly interpreted the protections of Rule 37(e).[114] Nevertheless, the varying interpretations of the Rule prevent parties from developing "routine" computer systems that appropriately maintain and delete electronic information.[115] In reaching this conclusion, the discussion below evaluates several situations based on actual cases. This Part

110 *See* Hebl, *supra* note 73, at 93–94.

111 *See id.*

112 *Id.* at 95 (quoting ROSENTHAL, *supra* note 106, at 84).

113 *See id.*

114 *See, e.g.*, Maria Perez Crist, *Preserving the Duty to Preserve: The Increasing Vulnerability of Electronic Information*, 58 S.C. L. REV. 7, 48–50 (2006) (discussing the concern of courts that parties will rely on Rule 37(e) to subvert their discovery obligations).

115 *See id.* at 52–53.

first considers those circumstances in which almost everyone will agree that the courts appropriately declined to grant a party protection under the safe harbor provision. Second, this Part discusses situations in which a party should have been granted safe harbor under Rule 37(e) but was denied such protection by the court. These examples illustrate that courts almost always place the burden on the spoliator to show that conduct qualifies as good faith, rather than on the moving party to demonstrate a lack of good faith.[116]

This analysis, however, should not leave the reader with the impression that courts never accept a Rule 37(e) defense. In fact, on some occasions, courts have gone to the other extreme and applied Rule 37(e) when the circumstances do not seem to support exempting a party from sanctions. The tragic case of *Escobar v. City of Houston*,[117] discussed above, provides one such example.[118]

A. The Correct Application of Rule 37(e) by Courts

Although courts may differ as to the proper level of mens rea encompassed by the good-faith exception, almost everyone can agree that parties do not deserve to avoid sanctions through safe harbor protection in certain situations.[119] For example, in *In re Krause*,[120] a party's discovery obligations required it to turn over two desktop computers to the opposing party.[121] Shortly before providing access to the computers, however, the spoliating party employed a piece of software called "GhostSurf" to delete all the electronic information from the computers.[122] When the opposing party moved for sanctions, the spoliating party sought protection under Rule 37(e)'s safe harbor provision.[123] Although the court placed the burden of proof on the party seeking sanctions, it found that the defendant "willfully and in-

116 *See, e.g.*, Phillip M. Adams & Assocs. v. Dell, Inc., 621 F. Supp. 2d 1173, 1192 (D. Utah 2009) (holding that the spoliator's expert failed to show that the document retention policies were reasonable, thereby leading the court to conclude that there existed insufficient evidence to find "good-faith" conduct).

117 Escobar v. City of Houston, No. 04-1945, 2007 WL 2900581, at *1 (S.D. Tex. Sept. 29, 2007).

118 *See supra* notes 1–13 and accompanying text.

119 *See, e.g.*, Kucala Enters. v. Auto Wax Co., No. 02-C-1403, 2003 WL 21230605, at *8 (N.D. Ill. May 27, 2003) (declining to accept a Rule 37(e) defense when the party deleted electronic information through the use of "Evidence Eliminator" software).

120 *In re* Krause, 367 B.R. 740 (D. Kan. 2007).

121 *See id.* at 748.

122 *See id.*

123 *See id.* at 767.

tentionally destroyed electronically stored evidence" and issued sanctions, denying the party's request for Rule 37(e) protection.[124]

B. The Failure to Apply Rule 37(e) when Appropriate

Despite the most obvious situations in which a party should not be granted Rule 37(e) protections, several times courts have either ignored Rule 37(e) or applied such a narrow definition of "good faith" that they inappropriately imposed sanctions on parties. *United States v. Maxxam, Inc.*,[125] serves as an excellent example of a situation in which Rule 37(e) should have been applied. In that case, the plaintiff brought a qui tam action under the False Claims Act alleging fraud in the development of a sustained yield plan submitted to the California Department of Forestry and Fire Protection that discussed the effect of harvesting lumber.[126]

The defendant contracted with a third party that used a software system to create the model plans.[127] This third-party contractor created hundreds of these plans per year and routinely deleted them because it never found a need to retain copies of the old plans.[128] The plaintiff moved for sanctions when the defendant could not produce copies of the old plans during discovery.[129] The court failed to recognize that the defendant's contractor had no indication that the plans would ever be required for litigation. Instead, the court ignored the protections available through Rule 37(e) and declined to impose sanctions based on the plaintiff's inability to prove that the data existed at the time the duty to preserve arose.[130] Although sanctions were not imposed, the court practically ignored Rule 37(e), instead of explicitly recognizing its relevance in this situation.

In addition to ignoring the Rule, as in *Maxxam*, courts have improperly imposed sanctions by reading the good-faith exception too narrowly. For instance, in *Nucor Corp. v. Bell*,[131] the court sanctioned a party in the form of an adverse inference when one of the party's

---

124 *See id.*

125 United States v. Maxxam, Inc., No. C-06-07497, 2009 WL 817264 (N.D. Cal. Mar. 27, 2009).

126 *See id.* at *1.

127 *See id.* at *3.

128 *See id.*

129 *See id.* at *1.

130 *See id.* at *1, *11–12 (discussing the lack of intentional conduct and the ordinary business practices that resulted in the destruction of evidence without making reference to the legal protections potentially available under Rule 37(e)).

131 *See* Nucor Corp. v. Bell, 251 F.R.D. 191 (D.S.C. 2008).

employees continued to use a laptop computer in the normal course of business.[132] The continued use of this computer resulted in the automatic deletion of responsive material, unbeknownst to the spoliating party.[133] Rather than considering whether the company's decision not to stop using its computer systems resulted in unreasonable conduct, the court made an apparently ad hoc decision that sanctions were warranted[134]—an approach that is, unfortunately, frequently used to make reasonableness determinations in electronic discovery.

In contrast, the central nature of the reasonableness determination in this Note's Uniform Safe Harbor Standard will lead courts to rely on a developed body of caselaw that would help to determine consistently whether a company's treatment of electronic information qualifies as reasonable.

The most egregious example of a court's failure to use Rule 37(e) lies in a recent patent infringement case in which the defendant did not produce responsive e-mails.[135] As is often the case with electronic discovery, the plaintiff demonstrated that unproduced e-mails existed based on its having received copies of such e-mails from a third party.[136] The question remained, what happened to the unproduced e-mails? As it turns out, unlike the *Zubulake* case, the defendant had not consciously failed to produce responsive material.[137] Instead, the operation of the defendant's electronic systems resulted in the loss of the material.[138]

The plaintiff moved for sanctions based on the defendant's inability to produce these e-mails.[139] Although the e-mails were lost well before (1) the defendant had any indication that the e-mails would be relevant in future litigation and (2) any complaint had been filed, the plaintiff asked the court to infer, based on the missing e-mails, that the defendant destroyed the responsive material.[140] In response, the defendant recognized the loss of the e-mails and sought Rule 37(e) protections, claiming that the e-mails were deleted during the normal

---

132 *See id.* at 197–98, 203–04.

133 *Id.*

134 *Id.* Interestingly, the court dismissed the defendant's Rule 37(e) defense in a footnote by merely stating that the safe harbor provision did not apply because the defendant acted in bad faith. *See id.* at 196 n.3.

135 Phillip M. Adams & Assocs. v. Dell, Inc., 621 F. Supp. 2d 1173, 1191–92 (D. Utah 2009).

136 *See id.* at 1178–79.

137 *See id.* at 1180–81.

138 *See id.* at 1181–82.

139 *See id.* at 1176.

140 *See id.*

operation of its electronic information systems.[141] While the plaintiff did not inform the defendant of the likelihood of litigation until 2005, the court concluded that in 1999 the defendant should have been retaining e-mails.[142] The court made this determination despite the inability of electronic storage systems to retain every piece of information and the defendant's reasonable practice of deleting e-mails after a certain time unless they were deemed to be potentially responsive to future litigation.[143]

This case strikes at the heart of the problem because the plaintiffs failed even to acknowledge Rule 37(e)'s protections and argued that the defendant had to be sanctioned if the electronic information had been lost, regardless of the reason.[144] In addition, the defendant deleted the e-mails over five years before the filing of the complaint and well before it could have reasonably anticipated litigation.[145] Furthermore, the court relied on inferences and flatly rejected a seemingly reasonable document retention policy.[146] The court did not apply a set standard; instead, it merely relied on its vague impression that the defendant's conduct did not occur in good faith.[147]

These examples illustrate the chaos that surrounds the implementation of Rule 37(e). The need for a Uniform Safe Harbor Standard becomes apparent in light of the failure of these courts to apply the Rule to parties who deserve its protection and the application of its protection to undeserving parties.

IV. The Uniform Safe Harbor Standard: Bringing Order to Spoliation Chaos

In light of the confusion currently surrounding a party's ability to receive safe harbor from sanctions, this Note proposes that courts embrace a Uniform Safe Harbor Standard. To this end, courts should adopt a unified and consistent basis for Rule 37 sanctions. Further,

---

141 *See id.* at 1191.

142 *See id.* at 1190–91 (noting that the defendants, ASUS, should have been "sensitized to the issue" in 1999 because one of its competitors, Toshiba, had just entered a class action settlement that involved the same type of issues presently before the court).

143 *See id.* at 1181–82.

144 *See generally id.* (lacking any mention of the plaintiff's response to the defendant's Rule 37(e) defense).

145 *See id.* at 1190–91.

146 *See id.* at 1189–92.

147 *See id.* at 1192. The court indicates that "ASUS does know how to protect data it regards as important," but does not explain why ASUS's document retention policy that resulted in the deletion of the e-mails in controversy does not qualify as acting in "good faith." *See id.*

courts should extend this safe harbor protection to parties potentially subject to sanctions under the court's inherent powers.[148]

This Part sets forth a proposed framework for establishing a consistent safe harbor from spoliation sanctions. The solution is then applied to several of the cases discussed above, thereby demonstrating the clear and unified results that would flow from the adoption of the Uniform Safe Harbor Standard. Lastly, the discussion addresses potential concerns that may arise with the implementation of the Uniform Safe Harbor Standard.

A. The Uniform Safe Harbor Standard

The Uniform Safe Harbor Standard involves both shifting the burden of proof and considering a different level of mens rea based on the point in time during the litigation when the spoliation occurs. Courts should not be faulted for not developing a consistent approach to this Rule. Instead, confusion is completely understandable considering the Rule's relatively recent adoption, its vague reference to "good faith," and the unlikelihood of Rule 37(e) discovery decisions being reviewed by appellate courts. As such, the proposal below serves as a unified approach to the good-faith standard that may offer litigants protection from sanctions derived from Rule 37 or a court's inherent powers.

1. Precomplaint Spoliation Claims

Turning to the proposal, when the spoliation occurs before the filing of a complaint but after a duty to preserve arises, the spoliating party should be granted safe harbor unless the party moving for sanctions can prove that the deletion of electronic information occurred with the intent to conceal responsive electronic information. In this situation, where a complaint has not been filed, the burden of proof rests on the party moving for sanctions. As discussed above, courts routinely place the burden on the moving party to show that the spoli-

---

148 Courts have started to provide safe harbor from sanctions derived from their inherent powers. *See, e.g.*, Rimkus Consulting Grp. v. Cammarata, 688 F. Supp. 2d 598, 611 (S.D. Tex. 2010). In *Rimkus*, in the end, the court recognized that any sanctions would be based on the court's inherent powers because the alleged spoliation occurred before the filing of the lawsuit or the issuance of any discovery orders. *See id.* at 612. Nevertheless, the court evaluated sanctions through the lens of Rule 37(e) and determined that the spoliating party would not be granted safe harbor because the loss of the information did not occur in "good faith." *See id.* at 642. Therefore, while recognizing that Rule 37(e) only applies in the context of sanctions based on Rule 37, the court entertained the possibility of a safe harbor from sanctions similar to Rule 37(e), imposed pursuant to the court's inherent authority. *See id.*

ator intentionally deleted electronic material.[149] Placing the burden on the moving party in the precomplaint context should therefore not be controversial. Further, the level of proof should track the normal preponderance of the evidence standard applied to other burdens in the discovery context.[150]

Therefore, before a complaint has been filed, the spoliating party can claim protection for the loss of responsive electronic information in several instances. The only limitation ensures that the party did not intentionally destroy the material with a purpose to conceal it or act in a willfully blind manner to the fact that its electronic information system would likely destroy responsive electronic information. This interpretation of "good faith" would allow a party to seek safe harbor protection for negligent conduct that resulted in the loss of electronic information before a complaint has been filed.

There are several advantages to adopting this broad interpretation of "good faith" in situations where spoliation occurs precomplaint. First, it provides a potential litigant an incentive to file a complaint in a timely fashion in order to protect responsive information from the negligent actions of the other party. Notably, encouraging parties to file their complaints would not result in an increased number of frivolous lawsuits because rules of the court would prevent such conduct.[151] Also, parties would not be induced to file premature complaints, because the availability of spoliation sanctions represents just one of several considerations that must be evaluated when a party prepares to file.

Furthermore, the broad interpretation of "good faith," combined with the shifting burden of proof, discourages a party with a weak case from waiting to file until after the spoliation has occurred. Without

---

149 *See, e.g.*, Nucor v. Bell, 251 F.R.D. 191, 200 (D.S.C. 2008) (placing the burden on the party moving for sanctions and finding that the party failed to show that the spoliator had intentionally wiped data from a hard drive). It should be noted that the burden of proof associated with demonstrating the spoliating party's mens rea should not be confused with the separate burden carried by the party seeking sanctions to prove that the now-destroyed material once existed and contained responsive information. *See, e.g.*, Pension Comm. of Univ. of Montreal Pension Plan v. Banc of Am. Sec., LLC, 685 F. Supp. 2d 456, 466–67 (S.D.N.Y. 2010) (explaining that a party seeking sanctions must demonstrate that the data alleged to have been deleted existed and is material to the party's claim or defense).

150 *See, e.g.*, *In re* Krause, 367 B.R. 740, 764 (D. Kan. 2007) (requiring that the party seeking sanctions carry her burden by a preponderance of the evidence in demonstrating that the allegedly destroyed material once existed and contained responsive information).

151 *See, e.g.*, FED. R. CIV. P. 11(b)(2) (requiring that "the claims, defenses, and other legal contentions [be] warranted by existing law or by a nonfrivolous argument for extending, modifying, or reversing existing law or for establishing new law").

shifting the burden of proof as an incentive, a party with a weaker claim may be inclined to delay filing a complaint with the hope that spoliation will eventually occur. Then, after spoliation occurs, the party could file and seek sanctions. In addition to monetary sanctions, a party may request an adverse inference in its favor, thereby making it more likely to prevail despite having a less meritorious claim.

2. Postcomplaint Spoliation Claims

After the filing of a complaint, however, a new standard of mens rea must apply, and the burden for proving that mens rea should shift. Specifically, following the filing of a complaint, a party can seek safe harbor under a good-faith standard only if it persuades the court of the reasonableness of its actions that resulted in the destruction of responsive electronic material. Once the complaint has been filed, the court should shift the burden of proof to the party allegedly responsible for losing responsive electronic information. The spoliating party would be subject to sanctions for intentional, reckless, and negligent conduct that resulted in the loss of information. In order to avoid sanctions, that party must show that it did not act with the intention to conceal evidence and that its management of electronic information qualifies as reasonable.

3. Summary and Comparison of Proposed Provision

This chart further illustrates the solution proposed by this Note:

Table. The Uniform Safe Harbor Standard

Rule 37(e) Protections	Precomplaint	Postcomplaint
Burden of Proof	Protection for conduct, unless party moving for sanctions demonstrates the other party intentionally deleted material	No protection, unless party responsible for spoliation demonstrates the reasonableness of its conduct
Required Level of Mens Rea	Protection for conduct, except intentional or reckless destruction of responsive material	No protection, unless conduct qualifies as reasonable

Although the Judicial Conference could revise Rule 37(e) or offer clarification of its proper interpretation, the Uniform Safe Harbor Standard's best chance of bringing calm to the spoliation chaos lies with the courts. A uniform and consistent interpretation of safe harbor protections should come from the courts because they can apply this consistent approach to both Rule 37(e) and their decisions to impose discovery sanctions under their inherent powers. Further, courts

are best suited to establish a body of common law governing the standards for reasonable conduct in the maintenance of electronic data.

Admittedly, difficulty would arise when implementing this proposal because of uncertainty about conduct that results in spoliation but still qualifies as reasonable. Nevertheless, the courts may rely on currently existing standards to determine if a party's conduct is reasonable.[152] For example, after a complaint has been filed, a company's obligation to preserve electronic information does not end by merely imposing a litigation hold.[153] Instead, the company must continually ensure that the litigation hold remains adequate to preserve information and that personnel abide by the requirements of the hold.[154] Moreover, the continued use of desktop computers or file servers may be unreasonable if the company anticipates that their use could potentially result in the loss of responsive electronic information.

Although it would take time to establish a body of law for determining which conduct qualifies as reasonable, any potential confusion that would occur in developing a reasonableness standard in the context of this proposal would certainly not be any worse than the currently confusing and inconsistent interpretations of Rule 37(e). Moreover, once the standard of reasonableness begins to take form, it will serve as an invaluable reference for responsible companies to know their obligations in the retention of electronic information.

In sum, the Uniform Safe Harbor Standard proposes that the courts interpret the safe harbor provision so that it always applies in situations where a party acts reasonably and never applies in circumstances where a party's intentional conduct or willful blindness results in the deletion of information. In addition, depending on the point in time during the litigation, a party's negligent conduct that results in the loss of electronic information could be protected. This solution seems appropriate in light of the disagreement in the drafting of Rule 37(e).[155] By varying the mens rea based on the point in time during the litigation when the spoliation occurred, this approach ensures that

---

152 *See, e.g.*, Cache La Poudre Feeds v. Land O'Lakes, Inc., 244 F.R.D. 614, 637 (D. Colo. 2007) (imposing sanctions for unreasonable conduct where the defendant imposed a litigation hold shortly after litigation commenced, identified key employees, and took measures to ensure information related to those individuals was preserved, but did not regularly follow up to ensure the responsive data was properly protected).

153 *See id.* at 630.

154 *See id.* at 629–30.

155 *See supra* Part II.B.

the good faith standard becomes the "intermediate standard" that was intended by the Judiciary Committee.[156]

B. Application of the Note's Approach to Actual Cases

In order to better understand the uniformity that would be created by the Uniform Safe Harbor Standard, this Section applies the proposal to the cases discussed above to demonstrate the current approach of courts. First, consider again *In re Krause*, where a party used the "GhostSurf" software to clear the contents of its computers.[157] Similar to the actual outcome, applying the Uniform Safe Harbor Standard would not prevent the court from imposing discovery sanctions. This same result would be achieved in several ways. First, the party moving for sanctions would likely have no difficulty demonstrating that the spoliator acted with intent to destroy responsive material. The party could simply point to the spoliating party's use of software specifically designed to render files unreadable. Moreover, because the destruction occurred in this case after the complaint was filed,[158] the spoliating party could only seek safe harbor protection by proving the reasonableness of its actions. The continued use of the "GhostSurf" software would not warrant Rule 37(e) protection because of the inherently unreasonable nature of using document-destruction software during litigation.

The circumstances of *In re Krause* seem straightforward because most would agree that individuals who install software designed specifically to delete compromising information should not have the opportunity to seek safe harbor. Other cases discussed above, however, reached results that differ from what would occur by implementing the Uniform Safe Harbor Standard. Consider, for instance, the circumstances in *Maxxam*,[159] where the plaintiff sought spoliation sanctions when the defendant's contractor deleted responsive sustained yield plans in the normal operation of its business.[160] When the deletion occurred, no indication existed that litigation would arise and no complaint had been filed in the case.[161]

Under the Uniform Safe Harbor Approach, the party moving for sanctions can prevail only if it carries its burden of showing that the

---

156 *See* ROSENTHAL, *supra* note 106, at 84–85.

157 *In re* Krause, 367 B.R. 740, 748 (D. Kan. 2007).

158 *Id.* at 747–48.

159 United States v. Maxxam, Inc., No. C-06-07497, 2009 WL 817264 (N.D. Cal. Mar. 27, 2009).

160 *See id.* at *1.

161 *See id.*

defendant acted with the intent to conceal evidence or was willfully blind to the fact that its actions would result in the deletion of evidence. Nevertheless, the moving party would not have been able to prove the necessary intentional or reckless conduct because the procedures in question were such that the third-party contractor routinely deleted the older plans based on its experience that past plans had never been required for any purpose.[162] Moreover, even assuming a complaint had been filed at the time the plans were deleted, the Uniform Safe Harbor Standard would arguably still not impose sanctions. Specifically, the actions of the defendant's contractor, which resulted in the automatic deletion of older revisions of the sustained yield plans, seem completely reasonable in light of the minimal value these plans could have in litigation.

Finally, lest the reader believe the Uniform Safe Harbor Standard adopts too broad an interpretation of "good faith," courts have accepted a Rule 37(e) defense in situations where this Note's Uniform Safe Harbor Standard would not offer protection. The most notable example involves the shooting death of the young boy in *Escobar*.[163]

Applying the Uniform Safe Harbor Standard, the court in *Escobar* should likely have imposed sanctions on the police department for deleting electronic communications that were made within twenty-four hours of the incident giving rise to the suit.[164] In *Escobar*, the spoliation occurred before the complaint was filed, and thus the moving party would have carried the burden of proof and the spoliator would have been able to seek Rule 37(e) safe harbor protection so long as the destruction did not occur intentionally. By ignoring plaintiffs' notice of the need for responsive information and deleting the electronic communications that took place in the twenty-four hours following the controversial shooting death of a fourteen-year-old boy, the plaintiffs likely could have satisfied their burden of proving that the police department intentionally deleted the communications to conceal responsive material.[165] Further, if HPD failed to initiate a litigation hold after it had been served with notice of the plaintiff's lawsuit, and if the potentially responsive electronic communications had thus been deleted pursuant to the ninety-day document retention policy, the plaintiffs could have satisfied their burden by showing that

---

162 *See id.* at *3.

163 *See supra* notes 1–13 and accompanying text.

164 *See* Escobar v. City of Houston, No. 04-1945, 2007 WL 2900581, at *17 (S.D. Tex. Sept. 29, 2007).

165 *See id.* at *1, *17–18.

HPD was willfully blind in its failure to adequately initiate a litigation hold.[166]

C. *Potential Counterarguments*

Two potential arguments may be raised against the Uniform Safe Harbor Standard. First, commentators have suggested that the adoption of a single level of mens rea would create a greater level of uniformity.[167] Thus, it may appear that the Uniform Safe Harbor Standard does not achieve uniformity because it varies the requisite level of mens rea based on the point in time during litigation when the spoliation occurred. Second, the Uniform Safe Harbor Standard's approach appears to be too lenient on spoliating parties because it allows safe harbor for negligent conduct in some circumstances. It could be argued that denying sanctions for negligent conduct precomplaint will cause companies to liberally and irresponsibly delete electronic material. This Section demonstrates how the Uniform Safe Harbor Standard accounts for each of these concerns.

1. *Achieving Optimal Uniformity by Varying the Mens Rea*

Several commentators present differing interpretations of Rule 37(e)'s good-faith standard.[168] Each of these approaches, however, advocates for a fixed level of mens rea, rather than an approach—such as that of the Uniform Safe Harbor Standard—that varies the level of mens rea based on a point in time.[169] It does not follow, however, that reliance on one level of mens rea across the board creates a more uniform or desirable result. Instead, so long as courts maintain uniformity in an approach, it will not matter if the mens rea varies based on whether a complaint has been filed.

Moreover, varying the mens rea creates the desirable result of avoiding the pitfalls that accompany an approach that protects all conduct (unless intentional) or, alternatively, that requires the conduct to be reasonable to be protected. For example, reading Rule 37(e)'s

166 *See id.* at *17.

167 *See, e.g.*, Hebl, *supra* note 73, at 96–97, 107–10 (discussing the inconsistent applications of Rule 37(e) and suggesting that courts should consistently apply a reckless or intentional conduct standard when interpreting this Rule).

168 *Compare id.* at 96–97 (arguing that the "good-faith" standard is the "absence of bad faith," which is "a state of mind more culpable than negligence . . . [that] does in fact mean intentional or reckless conduct"), *with* Davidovitch, *supra* note 33, at 1138–39 (explaining that the standard of "good faith" is very similar to a "negligence standard" that does not allow a party safe harbor protection unless the conduct is reasonable).

169 *See* Hebl, *supra* note 73, at 96–97; Davidovitch, *supra* note 33, at 1138–39.

good-faith reference solely as a reasonableness standard would provide protection only if a party's spoliation could be considered reasonable.[170] This reading would result in too high a bar for parties in the maintenance of their electronic systems. As the Judicial Conference points out, protecting only reasonable conduct would protect nothing at all because sanctions are rarely even considered when a party acts reasonably.[171]

By contrast, interpreting "good faith" to be anything but intentional or reckless conduct would create the undesirable result of protecting parties from sanctions whenever they acted negligently. Therefore, those who advocate for only one level of mens rea may achieve uniformity, but they would do so at the cost of producing undesirable results in which Rule 37(e)'s protections become overly broad or too narrow. Instead, the Uniform Safe Harbor Standard both achieves uniformity in determining the mens rea and avoids the pitfalls that accompany interpretations that embrace only one level of mens rea.

2. Discouraging Liberal Document Retention Policies

Because the Uniform Safe Harbor Standard provides protection for a party's negligent conduct in some situations, it may appear that companies would be inclined to adopt liberal document retention policies that delete unreasonable amounts of data. This Note's solution, however, would not encourage liberal deletion of electronic material. In applying the Uniform Safe Harbor Standard, the court should not consider whether a document retention policy qualifies as reasonable. Instead, the court should focus on whether a party's precomplaint conduct reveals that the party acted recklessly or with the intent to destroy potentially responsive electronic material. The Uniform Safe Harbor Standard does not provide protection for a party that establishes an unreasonably liberal document retention policy because establishing such a policy demonstrates intent to destroy material and therefore lies outside of the scope of Rule 37(e)'s protections. This intent to destroy material through a liberal document retention policy would become even more apparent when a company adopts such a policy in light of potential litigation. This type of behavior would not warrant safe harbor protection under the Uniform Safe Harbor Standard.

---

170 *See* Davidovitch, *supra* note 33, at 1138–39.

171 *See id.* at 1138.

Therefore, the Uniform Safe Harbor Standard addresses many of the concerns surrounding a satisfactory interpretation of Rule 37(e). In particular, varying the mens rea based on the point in time during litigation when the spoliation occurred would actually create greater uniformity. Moreover, the Uniform Safe Harbor Standard would prevent, rather than encourage, parties from creating liberal document retention policies.

Conclusion

The chaos currently surrounding the interpretation of Rule 37(e) calls for courts to adopt a clear and consistent approach to providing parties safe harbor from sanctions that originate from Rule 37 or the inherent powers of courts. The Uniform Safe Harbor Standard presents a consistent approach that aims to provide litigants with clear expectations.

Rather than applying a single meaning to the good-faith provision of Rule 37(e), the Uniform Safe Harbor Standard varies the level of mens rea and the burden of proof based on the point in time during litigation when the spoliation occurred. In particular, when the loss of electronic information occurs prior to the filing of a complaint, the party requesting sanctions carries the burden of demonstrating that the spoliating party deleted the information either with the intent to conceal evidence or in a state of willful blindness. Once a complaint has been filed, however, the burden shifts to the spoliating party, which can avoid sanctions only if it demonstrates the reasonableness of its actions that resulted in the loss of responsive material. This approach should not only be implemented by courts when interpreting Rule 37(e), but should also be applied to limit the inherent power of courts to sanction parties.

In light of the current confusion regarding safe harbor protections, courts must act to ensure that Rule 37(e) does not deny justice to families like the Escobars, who struggle with the death of a loved one that came at the hands of a negligent police officer. Moreover, courts must provide clear standards to companies that have the best intentions of producing evidence but must contend with the challenges that accompany maintaining a plethora of electronic information. Enough time has passed since the adoption of Rule 37(e); federal courts must move away from an apparently ad hoc application of this Rule and strive for uniformity in the issuance of sanctions.