

Throwing Out the (Electronic) Trash: True Deletion Would Soothe E-Discovery Woes

Andrew Moerke Mason*

Electronic discovery (e-discovery) consumes time, money, and resources like few other aspects of modern-day litigation. Deleted data, metadata, backup data, and other intangible forms of information make e-discovery more complex and contentious than traditional discovery.¹ Computer users generate and retain electronic documents with ease, leading to significantly greater amounts of data than in a paper-only world.² E-discovery's volume and complexity increase litigation costs and complicate discovery disputes between parties, draining both party and judicial resources.

More vexing than other areas of e-discovery, e-discovery of deleted data demands expensive forensic techniques, dampens business productivity, and holds no guarantee of yielding evidence. Parties anguish over whether deleted files on a computer hard drive could contain information critical to a

© 2006 Andrew Moerke Mason.

* J.D. expected 2007, University of Minnesota Law School; B.S. 1999, University of California, Berkeley. The author thanks Professor Brad Clary; editors Elizabeth Dilks, Dave Leishman, and Sarah Bunce for invaluable feedback on structure, content, and clarity; the board and staff of the Minnesota Journal of Law, Science & Technology for their assistance; and Deborah Anne Hudleston, for love and support.

1. See ADVISORY COMM. ON THE FEDERAL RULES OF CIVIL PROCEDURE, REPORT OF THE CIVIL RULES ADVISORY COMMITTEE, *in* JUDICIAL CONFERENCE COMM. ON RULES OF PRACTICE AND PROCEDURE, REPORT OF THE JUDICIAL CONFERENCE COMMITTEE ON RULES OF PRACTICE AND PROCEDURE app. C at C-42 (2005) [hereinafter 2005 ADVISORY COMMITTEE REPORT], available at <http://www.uscourts.gov/rules/Reports/ST09-2005.pdf> (discussing various types of inaccessible electronic information).

2. See Sarah A. L. Phillips, Comment, *Discoverability of Electronic Data Under the Proposed Amendments to the Federal Rules of Civil Procedure: How Effective Are Proposed Protections for "Not Reasonably Accessible" Data?*, 83 N.C. L. REV. 984, 987-91 (2005).

claim or defense or undermine an entire litigation strategy.³ Judges must determine whether to order production of deleted files and who should bear the costs.⁴ When granted, production orders often require use of costly extraction methods.⁵ Ultimately, recovered files may contain relevant information or they may contain nothing. Yet even when relevant, information from deleted files may be inadmissible.⁶

True deletion proposes to ensure that deletion of a computer hard drive file creates complete and permanent destruction of that file—making it irretrievable.⁷ While currently not a part of major operating systems, compelling reasons for true deletion exist and could lead to its adoption.⁸ If implemented, how would true deletion affect the current e-discovery process?

This Article discusses true deletion's potential effect on e-discovery in civil litigation.⁹ Section I outlines the development of e-discovery in U.S. courts and the courts' current approach to discovery of deleted data. Section II provides a brief overview of true deletion and examines how true deletion would impact e-discovery and how the legal field could react to implementation of true deletion. This Article concludes that

3. See, e.g., *Antioch Co. v. Scrapbook Borders, Inc.*, 210 F.R.D. 645, 649-54 (D. Minn. 2002) (discussing party's concern over destruction of deleted data and resultant forensic copy of opposing party's hard drive to recover relevant deleted files before they were overwritten); *Trigon Ins. Co. v. United States*, 204 F.R.D. 277, 281-90 (E.D. Va. 2001) (ordering adverse inferences on credibility of experts after fragments of deleted files were recovered from litigation consultant's hard drive).

4. See *Antioch*, 210 F.R.D. at 651-52 (discussing who should bear costs in discovery of deleted data).

5. See *id.* at 651; Phillips, *supra* note 2, at 993-94 (describing complicated process for retrieving data from hard drives and noting the productivity loss businesses incur when deleted data is retrieved from hard drives).

6. See Leah Voigt Romano, *Developments in the Law: Electronic Discovery – VI. Electronic Evidence and the Federal Rules*, 38 LOY. L.A. L. REV. 1745, 1775-1800 (2005).

7. See Simson L. Garfinkel, *Design Principles and Patterns for Computer Systems That Are Simultaneously Secure and Usable*, 133-42 (May 16, 2005) (unpublished Ph.D. dissertation, Massachusetts Institute of Technology) (on file with author), available at <http://www.simson.net/thesis> (discussing a technologically feasible implementation of such a system).

8. See *id.*

9. Other areas potentially affected by true deletion include computer privacy and security, and the ability of law enforcement to gather evidence and prosecute criminals.

true deletion would increase efficiency and reduce the costs of e-discovery and that implementation of a deletion history file and a deletion hold certificate would ameliorate the risk of increased spoliation.

I. DELETED DATA AND ITS PLACE IN E-DISCOVERY LAW

A. DELETED DATA IS DISCOVERABLE

Data “deleted” from a computer hard drive is not destroyed.¹⁰ When a user “deletes” a file, two things occur: (1) the file becomes invisible to the operating system; and (2) the space occupied by the file is freed up for use, allowing the operating system to overwrite that space with new information.¹¹ Unless the operating system requires use of this space, overwriting does not occur—and “deleted” data remains—for a considerable time.¹² During this time the data remains invisible to the common user, yet accessible through arduous and often expensive means.¹³ Only upon overwriting does recovery of data become practically impossible.¹⁴

In e-discovery case law, cost and burden of production of data, and not the use of data, determine “accessibility.”¹⁵ Though viewed as among the *most* inaccessible types of electronic data,¹⁶ deleted data remains discoverable.¹⁷

10. See *Zubulake v. UBS Warburg, LLC*, 217 F.R.D. 309, 313 n.19 (S.D.N.Y. 2003) (quoting Shira A. Scheindlin & Jeffrey Rabkin, *Electronic Discovery in Federal Civil Litigation: Is Rule 34 Up to the Task?*, 41 B.C. L. REV. 327, 337 (2000)) (describing the reasons for which “many files are recoverable long after they have been deleted”).

11. See *id.*

12. See *id.*

13. Microsoft TechNet, Frequently Asked Questions: New Security Tool for EFS, <http://www.microsoft.com/technet/security/tools/cipherfaq.msp> (last visited Feb. 13, 2006). The accessibility of “deleted” data has been bemoaned for over five years. See James M. Rosenbaum, *In Defense of the DELETE Key*, 3 GREEN BAG 2d 393 (2000) (noting privacy concerns that arise because the computer “lies when it says delete”).

14. See Daniel Feenberg, Nat’l Bureau of Econ. Research, *Can Intelligence Agencies Read Overwritten Data? A Response to Gutmann*, July 21, 2003, last revised May 14, 2004, <http://www.nber.org/sys-admin/overwritten-data-guttman.html>.

15. See Phillips, *supra* note 2, at 1004-05.

16. See *Zubulake*, 217 F.R.D. at 319-20; 2005 ADVISORY COMMITTEE REPORT, *supra* note 1, at C-42 (listing deleted data as “difficult-to-access” in the Introduction to Proposed Rule 26(b)(2)).

17. See *Antioch Co. v. Scrapbook Borders, Inc.*, 210 F.R.D. 645, 652-53 (D. Minn. 2002) (citing *Playboy Enters. v. Welles*, 60 F. Supp. 2d 1050, 1054 (S.D.

Production and preservation orders can even encompass files “deleted” *before* the prospect of litigation,¹⁸ forcing a party to preserve—and prepare to exhume—trash made useless long ago.

Out of concern for privilege and confidentiality, parties almost always enlist special masters or forensic experts when producing deleted files.¹⁹ The forensics expert receives the hard drives and extracts the deleted files, giving copies of those files to the producing party.²⁰ On occasion, the presiding judge also receives copies of the files.²¹ The producing party reviews the files, providing to the requesting party only those documents relevant to the discovery order.²² In determining *whether* to order discovery of inaccessible information and *who pays* the cost of production for such discovery, courts balance concerns of undue burden and protection of privilege with concerns regarding spoliation and failure to produce requested materials.²³

1. Case Law Moves from “Producer Pays” to Accessibility and Relevance

In traditional paper discovery, the producing party typically pays the costs of discovery.²⁴ This seems inherently fair: production costs exist, but review of the produced materials is time-consuming and costly in a manner commensurate with the amount of material.

Cal. 1999)) (outlining test for recovery of deleted computer files); *Simon Prop. Group v. mySimon, Inc.*, 194 F.R.D. 639, 641-43 (S.D. Ind. 2000) (ordering appointment of expert to create “mirror image” copies of defendant’s hard drives and provide list of deleted files to defendant for review).

18. *See, e.g.*, *Antioch*, 210 F.R.D. at 650–51 (ordering pre-discovery preservation of computer hard drive to prevent destruction of deleted files, many of which were conceivably generated before the prospect of litigation).

19. *See id.* at 653-54.

20. *See id.*

21. *See id.*

22. *See id.*; *see also* *mySimon*, 194 F.R.D. at 641-42.

23. *See* *Antioch*, 210 F.R.D. at 653-54 (combining the approaches used in *Playboy* and *mySimon*); *see also* Scott M. Gawlicki, *e-Discovery Grows Up*, CORP. LEGAL TIMES, Feb. 2005, available at http://www.insidecounsel.com/issues/insidecounsel/15_159/features/186-1.html (noting the key e-discovery issues are data preservation, scope of e-discovery, cost sharing, and privilege waiver).

24. *See* *Oppenheimer Fund, Inc. v. Sanders*, 437 U.S. 340, 358 (1978) (stating that “the presumption is that the responding party must bear the expense of complying with discovery requests”).

E-discovery of deleted data disrupts this balance of the burdens borne by parties.²⁵ Production proves a much heavier draw on resources—the process cannot ordinarily²⁶ be automated because of concerns regarding privilege.²⁷ The price of e-discovery production rises even higher if you factor in productivity losses—caused by forensic operations which render computers unusable.²⁸ While production costs multiply, automated searching mechanisms make document review of electronic information ever easier.²⁹ Courts do shift e-discovery costs to the requesting party on a case-by-case basis, but some commentators advocate little or no cost-shifting.³⁰ Though now

25. See *Multitechnology Servs. v. Verizon Sw.*, No. 4:02-CV-702-Y, 2004 U.S. Dist. LEXIS 12957 (N.D. Tex. July 12, 2004), at *5-6 (requiring parties to shoulder the burden of discovery costs evenly, recoverable by the prevailing party at conclusion); *Antioch*, 210 F.R.D. at 651 (noting that the requesting party stated that it would pay recovery costs even before court had issued any sort of order for recovery of deleted files); see also Phillips, *supra* note 2 at 995-96.

26. With proper information management systems, production may be less costly. See Theodore O. Rogers, Jr. & Thomas I. Barnett, *Adapting Paper-Based Rules to Electronic Discovery*, N.Y. L.J., July 19, 2004, at 4 (noting that “a defensible plan to preserve potentially relevant data [allows parties to demonstrate they have ensured] . . . the retention of relevant data” and to argue against sweeping discovery requests or preservation orders).

27. See Georgene Vairo, *Foreword: Developments in Civil Litigation Electronic Discovery*, 38 LOY. L.A. L. REV. 1529, 1535 (2005).

28. See Jessica Lynn Repa, Comment, *Adjudicating Beyond the Scope of Ordinary Business: Why the Inaccessibility Test in Zubulake Unduly Stifles Cost-Shifting During Electronic Discovery*, 54 AM. U. L. REV. 257, 270 (2004) (discussing “the added cost of productivity loss from computer downtime during electronic discovery”); A.L. Brown, *The Manageable Challenge of Electronic Discovery*, May 31, 2005, http://www.rkmc.com/The_Manageable_Challenge_of_Electronic_Discovery.htm (emphasizing the huge monetary costs that can be created by e-discovery, both in the manpower required for production and the lost productivity companies experience when data is being accessed from their systems); cf. *Antioch*, 210 F.R.D. at 653 (directing that forensic experts in charge of recovering deleted data “avoid unnecessarily disrupting the normal activities or business operations of the Defendants”).

29. See Repa, *supra* note 28, at 269.

30. Compare *McPeck v. Ashcroft*, 202 F.R.D. 31 (D.D.C. 2001) (shifting costs of production of inaccessible information based on relevance of a sampling of that information), and Phillips, *supra* note 2, at 996-97 (discussing how courts have rejected a cost-based approach, which would charge requesting parties with the full cost of e-discovery, and instead have moved toward various balancing approaches, in which the requesting party may bear a *portion* of the costs), with Daniel B. Garrie & Matthew J. Armstrong, *Electronic Discovery and the Challenge Posed by the Sarbanes-Oxley Act*, 2005 UCLA J.L. & Tech. 2 (arguing that shifting costs of production will only discourage corporations from developing more effective and efficient

not uncommon, cost-shifting still only alleviates actual costs of production and rarely accounts for productivity losses suffered by the producing party due to lost use of computer systems.³¹

In 2002, the United States District Court for the Southern District of New York devised an eight-factor test to achieve balancing of e-discovery costs in *Rowe Entertainment, Inc. v. William Morris Agency, Inc.*³² The court in *Rowe* noted, “Just as a party would not be required to sort through its trash to resurrect discarded paper documents, so it should not be obligated to pay the cost of retrieving deleted emails.”³³ Shortly thereafter, in *Zubulake v. UBS Warburg, LLC*,³⁴ the same court modified the *Rowe* test. For “relatively inaccessible” information, the court outlined seven factors to determine cost-shifting:

- (1) The extent to which the request is specifically tailored to discover relevant information;
- (2) The availability of such information from other sources;
- (3) The total cost of production, compared to the amount in controversy;
- (4) The total cost of production, compared to the resources available to each party;
- (5) The relative ability of each party to control costs and its incentive to do so;
- (6) The importance of the issues at stake in the litigation; and
- (7) The relative benefits to the parties of obtaining the information.³⁵

Zubulake weighs the factors in roughly the order listed³⁶ and cites the limitations in Rule 26(b)(2) of the Federal Rules of Civil Procedure as the source of the factors.³⁷ The normal

e-storage systems).

31. See *Repa*, *supra* note 28 (discussing productivity losses); see also *Antioch*, 210 F.R.D. at 653 (attempting to mitigate business interruptions suffered by the producing party).

32. 205 F.R.D. 421 (S.D.N.Y. 2002). The test weighed the following eight factors in determining whether costs should be shifted:

- (1) the specificity of the discovery requests;
- (2) the likelihood of discovering critical information;
- (3) the availability of such information from other sources;
- (4) the purposes for which the responding party maintains the requested data;
- (5) the relative benefits to the parties of obtaining the information;
- (6) the total cost associated with production;
- (7) the relative ability of each party to control costs and its incentive to do so; and
- (8) the resources available to each party.

Id. at 429.

33. *Id.* at 431.

34. 217 F.R.D. 309 (S.D.N.Y. 2003).

35. *Id.* at 322.

36. See *id.* at 322-23.

37. See *id.* at 316-17 (noting the “proportionality test” created by Fed. R. Civ. P. 26(b)(2) and the ability to shift costs to avoid “undue burden or

presumption of “producer pays” applies to data kept in an “accessible format.”³⁸ Among e-discovery case law, the *Zubulake* test currently holds the most influence.³⁹

2. Legal Commentators Respond to E-Discovery

Calling for a clear, early, focused, and good faith discussion of e-discovery issues, an open think tank of leading jurists, lawyers, experts, and academics created the Sedona Principles.⁴⁰ These fourteen principles rely on balancing cost, burden, and need under Rule 26(b) of the Federal Rules of Civil Procedure, and only consider sanctions upon intentional or reckless failure to preserve or produce.⁴¹ Of most relevance to this Article, Sedona Principle Nine directs that “absent a showing of special need and relevance a responding party should not be required to preserve, review, or produce *deleted*, shadowed, fragmented, or residual data or documents.”⁴²

The American Bar Association also addressed the e-discovery question in its 2004 civil discovery standards by outlining sixteen factors to consider during e-discovery disputes.⁴³ Many of these factors echo those used in *Rowe* and *Zubulake*.⁴⁴

In the early stages of litigation, communication between parties and an understanding of electronic information systems facilitate preservation of relevant information.⁴⁵ Some suggest

expense” under Fed. R. Civ. P. 26(c)).

38. *See id.* at 316-18.

39. *See Repa, supra* note 28, at 260 (stating that “federal courts increasingly rely on *Zubulake* as a guide for determining cost allocation during electronic discovery”).

40. *See* SEDONA CONFERENCE WORKING GROUP ON BEST PRACTICES FOR ELEC. DOCUMENT RETENTION & PROD., THE SEDONA PRINCIPLES: BEST PRACTICES, RECOMMENDATIONS & PRINCIPLES FOR ADDRESSING ELECTRONIC DOCUMENT PRODUCTION (Jonathon M. Redgrave et al. eds., 2004), available at <http://www.thesedonaconference.org/content/miscFiles/SedonaPrinciples200401.pdf>.

41. *See id.* at i.

42. *Id.* (emphasis added).

43. *See* AMERICAN BAR ASS'N, AMENDMENTS TO CIVIL DISCOVERY STANDARDS 5-7 (2004), <http://www.abanet.org/litigation/documents/hod/ABA%20Final%20Revised%202004%20Amendments%20Civil%20Discovery%20Standards.doc>.

44. *See Phillips, supra* note 2, at 1003.

45. *See* Robert D. Brownstone, *Collaborative Navigation of the Stormy e-Discovery Seas*, 10 RICH. J.L. & TECH. 53 (2004), <http://law.richmond.edu/jolt/v10i5/article53.pdf> (discussing the need to clearly understand both your adversary's and your client's information management

it would be wise to require immediate deposition of information and technology managers to ensure rapid enactment of proper information management policies.⁴⁶ Because technology will always outpace the rules developed to manage it, only clear communication and negotiation grounded in a solid education regarding new and emerging technologies can adequately address the problems of e-discovery.⁴⁷ The need for case-specific rules, regular communication, and open negotiation regarding e-discovery, however, proves burdensome to the court system.⁴⁸

3. Discovery of Deleted Data Poses Problems for the Judiciary

The uncertain and intangible nature of deleted data causes more frequent reliance on judges to resolve e-discovery disputes involving such data.⁴⁹ Though judges have no greater insight into deleted data than the parties involved in litigation, they must labor over whether to order recovery of such data and shift costs.⁵⁰ The analysis involves multiple, time-consuming steps,⁵¹ from ordering samples of data to determining relevance

systems); Gawlicki, *supra* note 23 (noting that solutions to e-discovery problems require work on the part of litigants and clear communication to the judge and other parties).

46. See *id.* ¶ 42 (noting a federal magistrate judge's statement that the first deposition taken in cases involving e-discovery should be that of the opposing system administrator).

47. See generally Jason Krause, *The Paperless Chase: Litigators and Courts Wrestle with Database Discovery*, 91 A.B.A. J., Apr. 2005, at 48.

48. See *Repa*, *supra* note 28, at 282–83 (noting the caseload of federal judges and the increased burden brought on by e-discovery disputes).

49. See *Antioch Co. v. Scrapbook Borders, Inc.*, 210 F.R.D. 645, 654 (D. Minn. 2002) (ordering production of deleted files through use of a neutral expert in computer forensics); *Simon Prop. Group v. mySimon, Inc.*, 194 F.R.D. 639, 641 (S.D. Ind. 2000) (ordering the appointment of an expert to create “mirror copies” of defendant's hard drives and provide a list of deleted files to defendant for review); Phillips, *supra* note 2, at 996-99 (analyzing the approaches developed in *McPeck*, *Rowe*, and *Zubulake*, all of which require a detailed case-by-case analysis).

50. See Phillips, *supra* note 2, at 996-99 (discussing various approaches taken by courts to determine the scope of appropriate recovery and which party should bear the cost of such discovery).

51. See *Zubulake v. UBS Warburg, LLC*, 217 F.R.D. 309, 321-23 (S.D.N.Y. 2003) (urging a slight change in the factors outlined in *Rowe*); *Rowe Entertainment, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421, 428-33 (S.D.N.Y. 2002) (involving an extensive multi-step analysis including consideration of relevance, cost-shifting, production, specificity, likelihood of success and benefit to each party, in addition to other factors).

and weighing cost-benefit factors.⁵² For trial court judges who already have overwhelming caseloads, elimination of this time-consuming process could only be welcome.

4. Deleted Data Will Continue to Prove Problematic

The predicted increase in computer-generated information such as emails, Word files, presentations, and documents⁵³—precisely the kind of data found on computer hard drives—means the prevalence of deleted data will only increase. Moreover, deleted data's inaccessible and potentially privileged nature will require the continued use of complex court proceedings and expensive third-party services involved in recovery operations. Shifting the discovery costs associated with data recovery alleviates concerns of unfair burden associated with the costs of production,⁵⁴ but a disparity in the relative sophistication of parties already exists⁵⁵ and could grow if parties create systems that allow for complete deletion of data.⁵⁶ Should this happen, parties with greater resources that could take advantage of such systems would gain a certain immunity, leaving less sophisticated adversaries at a loss in relation to discovery requests involving deleted data.

52. See *McPeck v. Ashcroft*, 212 F.R.D. 33, 34 (D.D.C. 2003) (including a discussion on relevance in the court's approach to determining whether to compel discovery of electronic data).

53. See Tim Stammers, *Safe and Sound: How Long a Company Stores Data, and How Quickly It Must Delete It, Forms a Key Plank of Several Compliance-Related Laws and Regulations*, COMPUTERBUSINESSREVIEWONLINE, <http://www.cbonline.com/content/COMP/magazine/Articles/Storage/SafeandSound.asp> (last visited Mar. 14, 2006).

54. See *Playboy Enters., Inc. v. Welles*, 60 F. Supp. 2d 1050, 1053 (S.D. Cal. 1999) (noting the need for "the producing party [to] be protected against undue burden and expense and/or invasion of privileged matter").

55. See FULBRIGHT AND JAWORSKI, L.L.P., SECOND ANNUAL LITIGATION TRENDS SURVEY FINDINGS 22-23 (2005), available at <http://www.fulbright.com/mediaroom/files/FJ0536-US-V13.pdf> (compiling statistics indicating that larger companies are usually better prepared for litigation involving discovery of electronic information).

56. File management systems essentially achieving true deletion are already available. See Randal C. Burns, *Managing the Lifetime of Versions in Digital Archives*, Presentation at the Digital Government (dg.o) DIGARCH Pls Meeting (May 17, 2005), <http://diggov.org/library/library/dgo2005/digarch/burns.ppt> (discussing several existing systems that allow for true deletion of electronic data).

B. PROPOSED FEDERAL RULES OF CIVIL PROCEDURE ADDRESS
E-DISCOVERY ISSUES

If approved by Congress, proposed amendments to the Federal Rules of Civil Procedure, including provisions relating to e-discovery, become effective December 1, 2006.⁵⁷ While Proposed Rules 16, 26, 33, 34, 37, and 45 all relate to e-discovery, Proposed Rules 26(b)(2) and 37(f) relate most directly to e-discovery of deleted data.⁵⁸

The proposed amendment to Rule 26(b)(2) follows the approach taken in *Zubulake*, defining data “not reasonably accessible”—including deleted data—as presumptively undiscoverable.⁵⁹ Nonetheless, the responding party must identify all sources containing inaccessible information “potentially responsive” to the request for discovery.⁶⁰ To then compel discovery of such “inaccessible information,” the requesting party must show good cause.⁶¹ Harkening to *Zubulake*, the proposed rule directs courts to follow the limitations in Rule 26(b)(2)(C) as a guide to evaluating “good cause.”⁶² Courts should consider “the burden and cost of locating, restoring, and retrieving potentially responsive information” when determining “not reasonably accessible” under proposed Rule 26(b)(2).⁶³

Proposed Rule 37(f) prevents courts from imposing sanctions “on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic operating system.”⁶⁴ This safe harbor provision reflects the needed balance between information preservation and continuation of business operations.⁶⁵ Specifically, information storage systems that automate overwriting of information do not give rise to sanctions unless deliberately

57. See U.S. Courts Federal Rulemaking, Supreme Court Action: Rules and Amendments Approved 4/12/06, <http://www.uscourts.gov/rules/index.html#supreme0406>.

58. See generally 2005 ADVISORY COMMITTEE REPORT, *supra* note 1, at C-18 to C-109.

59. See Phillips, *supra* note 2, at 1010 (arguing that the Rule should further distinguish among backup data, deleted data, and legacy data).

60. See 2005 ADVISORY COMMITTEE REPORT, *supra* note 1, at C-47 to C-48.

61. *Id.* at C-45 to C-46.

62. *See id.*

63. *Id.* at C-43.

64. *Id.* at C-86.

65. *See id.* at C-83, C-86 to C-88.

designed to destroy litigation-related material.⁶⁶ Nonetheless, the Committee emphasizes preservation whenever possible and notes that failure to take good-faith measures to preserve could remove a party from the sanctity of the safe harbor.⁶⁷

Trade publications, academic writing, and public commentary⁶⁸ all criticized the proposed amendments for lack of clarity. Much of the criticism centered on the vagueness of phrases such as “not reasonably accessible” and “good cause” in Proposed Rule 26, and “reasonable” preservation of data in Rule 37.⁶⁹ There is also fear that the safe harbor created by Proposed Rule 37 encourages parties to devise information management systems that delete information relevant to litigation, despite the language to the contrary in the committee note.⁷⁰ The Rules Committee directly addressed all these concerns in the final draft of the Proposed Rules.⁷¹

II. THE E-DISCOVERY PROCESS WOULD BENEFIT FROM TRUE DELETION

Rule 1 of the Federal Rules of Civil Procedure calls for a “just, speedy, and inexpensive” litigation process. Yet e-discovery of deleted data is anything but speedy and inexpensive.⁷² What if deleted data ceased to linger, and

66. See 2005 ADVISORY COMMITTEE REPORT, *supra* note 1, at C-84, C-87.

67. See *id.* at C-84 to C-85.

68. There was a public comment period from August 10, 2004 to February 15, 2005. See Informational Memorandum, Preston Gates Ellis, L.L.P., Public Comment Period Begins for Federal Civil Rules Proposals Addressing Electronic Discovery Issues (Aug. 20, 2004), available at http://www.prestongates.com/images/pubs/FRCP_CommentPeriod.pdf. During this time, three public hearings were held on the proposed amendments. See 2005 ADVISORY COMMITTEE REPORT, *supra* note 1, at 1.

69. See Phillips, *supra* note 2, at 1010-14 (discussing the definitions of “not reasonably accessible” and “good cause” under Proposed Rule 26(b)(2) and arguing for stronger language in either the proposed rule or the corresponding committee note); David Chaumette & Linda Kish, *Questions Surround Proposed E-Discovery Rules*, TEX. LAW., April 5, 2005, <http://www.law.com/jsp/ltn/PubArticleFriendlyLTN.jsp?id=1112618114470> (noting the loose definition of “reasonable” preservation could create a glut of preservation requests, but conceding that too precise of a definition would become inapplicable).

70. See Richard Acello, *E-Mail to Lawyers: E-Discovery Rules on the Way*, ABA JOURNAL REPORT, Oct. 7, 2005, <http://www.abanet.org/journal/ereport/oc7rules.html>.

71. See 2005 ADVISORY COMMITTEE REPORT, *supra* note 1, at C-42 to C-45, C-84 to C-86.

72. See, e.g., *id.* at C-43 (noting that cases do arise where a producing

therefore ceased to be discoverable?

True deletion is just as its name indicates: when a user deletes a computer hard drive file, all information in that file would be permanently irretrievable. The current “false delete” is most easily explained as an oversight of early computer designers.⁷³ “True deletion” is technologically possible and could be universally implemented.⁷⁴ Security and privacy advocates seek to implement true deletion in all operating systems, including Windows and Macintosh.⁷⁵ One proposed implementation of true deletion adds a “shredder” step to the current deletion process.⁷⁶ Upon deletion, files move to the recycle bin or trash.⁷⁷ With a shredder step, when the recycle bin or trash is emptied, the operating system would send the file to the shredder.⁷⁸ Then, at the instruction of the user, or at scheduled intervals, the shredder would overwrite all versions of the file in question.⁷⁹

From a business perspective, “companies almost universally consider it desirable to delete data the instant that it becomes legal to rub it out,” to avoid being caught with the “wrong” data.⁸⁰ File management systems that write over deleted files instead of simply de-allocating hard drive space already exist.⁸¹ Consequently, common business practices all but mandate complete destruction of deleted files.

party cannot determine which data may be available without first conducting an expensive and time-consuming search); Tracey L. Boyd, Note, *The Information Black Hole: Managing the Issues Arising from the Increase in Electronic Data Discovery in Litigation*, 7 VAND. J. ENT. L. & PRAC. 323, 325 (2005) (discussing costly use of forensics experts to produce electronically stored data); Rena Durrant, *Developments in the Law: Electronic Discovery – VII. Spoliation of Discoverable Electronic Evidence*, 38 LOY. L.A. L. REV. 1803, 1813 (2005) (noting that forensics experts can be quite expensive and that their results are not necessarily guaranteed); Voigt Romano, *supra* note 6 (discussing admissibility issues specific to electronic information).

73. See Garfinkel, *supra* note 7, at 106.

74. See *id.* at 133–37.

75. See generally *id.*

76. See *id.* at 134–37.

77. See *id.* at 136.

78. See *id.*

79. See Garfinkel, *supra* note 7, at 136.

80. Stammers, *supra* note 53.

81. See Burns, *supra* note 56.

A. TRUE DELETION AND A DECREASED BURDEN OF E-DISCOVERY

If implemented, true deletion would eliminate the risk that deleted files remain on a user's computer hard drive indefinitely, potentially subject to litigation e-discovery. Reduction in e-discovery disputes brought before judges and magistrates would result from the elimination of this ponderous prospect of hidden files *potentially* relevant to litigation. And implementation of true deletion in all major operating systems would minimize disparities favoring parties sophisticated enough to recognize and effectively deal with deletion's currently misrepresentative nature. As the Judicial Conference "recognizes that all electronic information systems are designed to recycle, overwrite, and change information in routine operation,"⁸² true deletion would not interfere with the goals of the proposed rules. In fact, the Committee understands the clear need for this type of routine destruction of data, as evidenced by Rule 37's safe harbor provision.

With deleted information made unavailable by true deletion, parties would surely seek information from other sources—including backup data. These requests for data from backup sources—considered "inaccessible" due to costs and burdens⁸³—could merely shift the cost and burden of e-discovery from one area to another. Two forces mitigate this potential shift of burden. First, discovery of information on backup tapes already poses a burden,⁸⁴ often in conjunction with requests for information from deleted files.⁸⁵ Second, more intelligent backup systems continue to decrease the cost of recovering backup information.⁸⁶ The diminishing difference

82. See JUDICIAL CONFERENCE COMM. ON RULES OF PRACTICE AND PROCEDURE, *supra* note 1 at 33.

83. See *Zubulake v. UBS Warburg, L.L.C.*, 217 F.R.D. 309, 318-20 (S.D.N.Y. 2003).

84. See *McPeck v. Ashcroft*, 202 F.R.D. 31 (D.D.C. 2001) (addressing issues surrounding high cost of recovering data from backup tape drives).

85. See, e.g., *Tilberg v. Next Mgmt. Co.*, No. 04-Civ-7373, 2005 WL 2759860 (S.D.N.Y. Oct. 24, 2005); *Landmark Legal Found. v. EPA*, 272 F. Supp. 2d 70 (D.D.C. 2003).

86. See Oliver Kaven, *Performance Tests: Tape Backup*, PCMAG.COM, Mar. 11, 2003, <http://www.pcmag.com/article2/0,1759,889896,00.asp> (noting that backup systems now possess catalog and file location information, making for smoother recovery); John Woelbern, *Does Tape Backup Have a Future? – SAIT*, STORAGESEARCH.COM, May 5, 2003, <http://www.storagesearch.com/sonyart1.html> (discussing technology for backup tape systems that provides high-speed access to any file on tape); Amit Zinman, *Tape Backup Alternatives*, MSEXCHANGE.ORG, Apr. 7, 2005,

between the cost of accessing day-to-day data and the cost of accessing backup data⁸⁷ could soon make certain backup data “accessible.” In this scenario, true deletion would shift e-discovery deleted data—a data type currently unknown and uncontrollable—to backup data—one becoming ever more accessible.

B. TRUE DELETION AND SPOILIATION

True deletion poses the very realistic concern of increased spoliation of relevant information. Even without true deletion, parties attempt to eliminate critical electronic evidence.⁸⁸ The ease with which a user could completely and permanently destroy electronic files would increase upon implementation of true deletion—no special software or operations would be needed.⁸⁹ So, true deletion’s greatest benefit might create its most serious problem.

The court in *Rowe Entertainment v. William Morris Agency* noted that “a party would not be required to sort through its trash to resurrect discarded paper documents.”⁹⁰ More realistically, eradication of the hypothetical paper trash in *Rowe* would occur long before a request for production. Parties regularly destroy paper documents—via shredding, document destruction services, or other means.⁹¹ This activity is widely

http://www.msexchange.org/pages/article_p.asp?id=822 (noting alternatives to backup tapes that allow for faster recovery of backup data).

87. Phillips, *supra* note 2, at 1005.

88. See, e.g., *United States v. Gordon*, 393 F.3d 1044, 1049 (9th Cir. 2004) (discussing defendant’s use of “evidence eliminator” software to overwrite deleted files after being put on notice that he was being investigated for embezzlement), *cert. denied*, 126 S. Ct. 472 (2005); *Anderson v. Crossroads Capital Partners*, Civil No. 01-2000, 2004 U.S. Dist. LEXIS 1867, at *7-8 (D. Minn. Feb. 10, 2004) (discussing plaintiff’s use of “cyberscrub” software to permanently remove files from her hard drive), *claim dismissed*, 2004 U.S. Dist. LEXIS 3820 (D. Minn. Mar. 10, 2004).

89. See Garfinkel, *supra* note 7, at 133–37.

90. 205 F.R.D. 421, 431 (S.D.N.Y. 2002).

91. See J. Nealy-Brown, *Paper Shredding Business Piles up*, ST. PETERSBURG TIMES, Feb. 1, 2002, at 1E, available at http://www.sptimes.com/2002/02/01/news_pf/Business/Paper_shredding_busin.shtml (stating that in 2002 there were 500 to 600 companies receiving their main source of revenue from shredding); Nat’l Ass’n for Info. Destruction, Interesting Facts, <http://www.naidonline.org/facts.html> (last visited Mar. 16, 2006) (detailing that every business possesses information that should be destroyed and that records ought to be destroyed on a regular basis); Shred-it, <http://www.shredit.com> (last visited Mar. 16, 2006) (stating that over 150,000

accepted as a satisfactory means of information management. Still, destruction of paper documents sometimes poses problems for litigation.⁹² In cases where parties destroy documents critical to litigation, courts grant orders for sanctions or adverse inferences.⁹³ The prospect of criminal prosecution is also a deterrent to destruction of documents critical to litigation.⁹⁴

Viewed as the electronic parallel to routine destruction of paper documents, true deletion would ensure that electronic data was fully irretrievable upon deletion. The downside is that—as with paper shredders—parties could use true deletion to maliciously destroy relevant information. The judiciary would likely respond with the same system of sanctions and adverse inferences applied in cases involving shredding of paper documents. Courts already adapt traditional spoliation methods to “shredding” of relevant electronic information.

Used with increasing prevalence, data-wiping software overwrites computer hard drives in an effort to remove all traces of deleted files.⁹⁵ Good faith use of such software prevents breaches of security or intrusions of privacy.⁹⁶ However, parties to litigation occasionally use data-wiping software maliciously to thwart discovery.⁹⁷ True deletion would essentially incorporate wiping software’s functionality into routine computer operations.⁹⁸ Wiping software generally overwrites all files on the hard drive, but forensic experts can

customers use Shred-it’s services to destroy confidential information).

92. See Chris William Sanchirico, *Evidence Tampering*, 53 DUKE L.J. 1215, 1217–18 (2004) (discussing Oliver North’s destruction of critical evidence and Arthur Andersen’s shredding of documents relating to the SEC inquiry into Enron activities).

93. See *id.* at 1261–86.

94. See *id.* at 1248–61.

95. See generally Thomas J. Fitzgerald, *Deleted but Not Gone: Programs Help Protect Confidential Data by Making Disks and Drives Unreadable*, N.Y. TIMES, Nov. 3, 2005, at C9 (discussing various software and services available for destruction of electronic data).

96. Andrew Brandt, *Do Passwords Provide True Protection? Don’t Count on It*, PC WORLD, May, 2005, available at <http://www.pcworld.com/howto/article/0,aid,119978,00.asp>; Fitzgerald, *supra* note 95.

97. See, e.g., *United States v. Gordon*, 393 F.3d 1044, 1049 (9th Cir. 2004), *cert. denied*, 126 S. Ct. 472 (2005); *Anderson v. Crossroads Capital Partners*, Civil No. 01-2000, 2004 U.S. Dist. LEXIS 1867, at *7-8 (D. Minn. Feb. 10, 2004), *claim dismissed*, 2004 U.S. Dist. LEXIS 3820 (D. Minn. Mar. 10, 2004).

98. See Garfinkel, *supra* note 7, at 133–37.

often recreate a history of what files were deleted and when,⁹⁹ establishing that spoliation of relevant information occurred.¹⁰⁰

Universal true deletion would normalize destruction of deleted files, creating a more controlled—and less clandestine—wiping of computer hard drives. Implementation of “deletion history” and “deletion hold” mechanisms—two safeguards proposed below—would allow parties to maintain and review a record of when file deletion occurred without reverting to costly forensic experts.

C. APPROPRIATE SAFEGUARDS CAN MITIGATE, OR EVEN PREVENT, INCREASED SPOILIATION

While true deletion creates potential spoliation problems, concern could be greatly mitigated by implementing proper safeguards. This Article proposes and examines two potential safeguards: (1) creation of a deletion history file, and (2) a litigation hold function built into the operating system. Both of these safeguards work harmoniously with the Proposed Rule 37(f), which “provides protection from sanctions only for the ‘good faith’ routine operation of an electronic information system.”¹⁰¹ Further, the safeguards encourage early communication between parties regarding electronic discovery.

1. A Deletion History

I suggest the use of a deletion history, a record similar to the record of deleted files currently created when forensic analysis is performed on computer hard drives. Made undeletable, yet easily accessible to those with a password, the history would normally remain private to the user of the computer. Upon litigation, parties could quickly and easily see when certain files were deleted, allowing for deeper inquiry into any file deleted after a party should have had knowledge of

99. Alex Salkever, *Hot on the E-Trail of Evidence at Enron*, BUSINESSWEEKONLINE, Jan. 29, 2002, http://www.businessweek.com/print/bwdaily/dnflash/jan2002/nf20020129_3701.htm?chan=db (noting that Windows-generated files holding deletion history can often be located even after data-wiping software has been used); *see also* Gordon, 393 F.3d at 1049 (9th Cir. 2004).

100. *See, e.g.*, Gordon, 393 F.3d at 1049 (noting how forensic analysis confirmed that defendant had used “evidence eliminator” to overwrite files many times and how this confirmation helped establish spoliation).

101. *See* 2005 ADVISORY COMMITTEE REPORT, *supra* note 1, at C-85.

pending litigation. Ideally, the deletion history would play a key role in information management, and parties would quickly become educated as to the deletion history's importance.

Review of the deletion history would occur at early pre-discovery meetings and form the first step of analysis when spoliation was suspected. For any files deleted after notice, a rebuttable presumption that those files contained adverse information would attach. Burdens of proof and persuasion would shift to the party who deleted files to show that those files contained no relevant information. For example, review of deletion history files at the Rule 16(b) pretrial conference could help establish the schedule for discovery of electronic information.¹⁰² Parties would supply deletion history files, set the e-discovery schedule for the related computers, and agree on times at which good faith file deletion could resume.

Implementation of true deletion and a deletion history would force companies and individuals to better maintain the data on their computer hard drives. Any party would think twice before deleting a file after notice of litigation—if a file were deleted, explanation of its deletion may be ordered. Some parties might be uncomfortable with the idea of a deletion history, but a private deletion history looks benign compared to the prospect of an expert extracting long forgotten files from a computer hard drive. As covered above, current “deletion” technology misrepresents what information computer hard drives retain.

The lack of anything more than a file name gives the deletion history little value as hard evidence, yet it could contribute to circumstantial evidence regarding existence of relevant information. Individuals may be deposed to establish the former contents of a known deleted file. Fear of deposition may cause some parties to appreciate the importance of the deletion history and maintain careful practice while on notice of litigation. Other parties may see depositions as an insignificant threat and delete files at will, attempting to overcome the rebuttable presumption by simply denying that the file contained relevant information. In either case, the deletion history approach leaves the spoliation problem unresolved in at least some, if not many, cases.

102. The proposed amendments focus on discussion of electronic information during the Rule 16(b) conference. See 2005 ADVISORY COMMITTEE REPORT, *supra* note 1, at C-25 to C-28.

2. A “Deletion Hold” Mechanism

One pitfall of the deletion history—not truly knowing whether deletion of a file was inadvertent or malicious—could be addressed by a “deletion hold” mechanism. An extension of “litigation hold” procedures used in litigation discovery generally, “deletion hold” would prevent destruction of all files on a computer hard drive. Users could place a computer into a password-protected “deletion hold,” effectively disabling the true deletion of any files. In the true deletion scheme discussed above, files would still be sent to the trash bin and shredder, but no shredding would occur until the “deletion hold” was lifted. Computer use could occur without fear of having to answer for a file accidentally deleted. Judges would likely grant motions to take a computer out of hold mode only upon satisfactory production of all relevant information—giving great weight to the opposing party’s consent. Taking a computer out of deletion hold mode before completion of litigation or a judicial order would create a rebuttable presumption that relevant information was destroyed.

Properly implemented, deletion hold would create one datestamp when activated and one datestamp when deactivated. A “hold certificate” would validate deletion records, allaying concerns of falsified deletion hold records.¹⁰³ At the Rule 16(b) conference, parties would designate specific computers for deletion hold. As an extra measure of precaution, counsel could place the stipulated computers in deletion hold and maintain the deletion hold password, checking malicious action by parties.

3. Effective Implementation

While a deletion history and deletion hold mechanism would help prevent spoliation, these safeguards could also increase disputes over destroyed data. Courts use sanctions and adverse inferences as checks on destruction of information.¹⁰⁴ But adverse inferences and “sanctions for the destruction of evidence . . . [require] holding secondary

103. See Krause, *supra* note 47 (discussing notarization of electronic databases for current e-discovery purposes).

104. See, e.g., *Metropolitan Opera Ass’n v. Local 100, Hotel Employees and Restaurant Employees International Union*, 212 F.R.D. 178, 220-30 (S.D.N.Y. 2003) (ordering severe sanctions for discovery abuses by the defendant); see also Sanchirico, *supra* note 92, 1261-86.

hearings to determine whether evidence was in fact destroyed, and if so, its likely content, the destroyer's state of mind, and the extent to which the destruction prejudiced the other side."¹⁰⁵ True deletion could create a significant increase in secondary hearings. This would mean true deletion simply shifted the problems currently posed by deleted data to another area of the discovery process. Strict use of deletion hold mechanisms could check the growth of such hearings, and would rely on harsh fines for failure to enact or maintain a deletion hold. Once a judge ordered a deletion hold, failure to produce certification of such a hold would generate more than a rebuttable presumption.

Spoliation would still occur despite the protection and deterrence provided by a deletion history and a deletion hold mechanism. Parties would inevitably attempt, and even succeed at, overcoming the barriers these two safeguards present. But the safeguards could check the spoliation created by true deletion and over time development of more effective safeguards would occur. Judges' strict enforcement of deletion holds could check any increase in evidentiary hearings on destruction of evidence.

CONCLUSION

Electronic discovery is burdensome to both parties and the legal system. While first intuition guides a legal solution to these problems—either in the form of a statute, procedural rule, or common law doctrine—technology may aid in solving some of the problems. Doing away with e-discovery's most frustrating area, true deletion would create a more efficient and fair system of discovery. Implementation would reduce e-discovery costs, minimize business interruptions, normalize how parties deal with deleted data, and allow judges to focus on other areas of litigation. Concerns with spoliation could be addressed by a focused implementation and the judicial system's strict utilization of agreed-upon safeguards, such as certified deletion history and deletion hold files.

105. Sanchirico, *supra* note 92, at 1223–24.