Winter 2010

Time for an Upgrade: Amending the Federal Rules of Evidence to Address the Challenges of Electronically Stored Information in Civil Litigation

Jonathan L. Moore
University of Richmond

ARTICLES

TIME FOR AN UPGRADE: AMENDING THE FEDERAL RULES OF EVIDENCE TO ADDRESS THE CHALLENGES OF ELECTRONICALLY STORED INFORMATION IN CIVIL LITIGATION

Jonathan L. Moore*

ABSTRACT: In recent years, electronically stored information (ESI) has begun to play an increasingly important role in civil litigation. Although the e-discovery amendments to the Federal Rules of Civil Procedure in 2006 provided guidelines for the discovery of this information, no accompanying changes were made to the Federal Rules of Evidence to govern the admissibility of this information at trial.

This article outlines the vastly different ways courts have addressed this problem in three areas: authentication, hearsay, and the best evidence rule. After discussing the various approaches courts take in these areas, this article proposes specific amendments to the Federal Rules of Evidence that would provide guidance to courts and litigants as to the admissibility of electronically stored information at trial.

CITATION: Jonathan L. Moore, Time for an Upgrade: Amending the Federal Rules of Evidence to Address the Challenges of Electronically Stored Information in Civil Litigation, 50 Jurimetrics J. 147–193 (2010).

America has undergone a radical transformation with the rise of computer technology, firmly placing modern society into the "Digital Age."[1] As a result, there has been a dramatic increase in the amount of digital information created each day.[2] This information can be stored in "mainframe computers, network servers, personal computers, hand-held devices, automobiles, [and even]

*Associate, Bowman and Brooke LLP, Richmond, Virginia. J.D., 2009, University of Richmond School of Law, *summa cum laude*. The author would like to thank Professor James Gibson for his helpful comments and suggestions on this article.

1. MICHAEL R. ARKFELD, ARKFELD ON ELECTRONIC DISCOVERY AND EVIDENCE § 1.1 (2d ed. 2009) (summarizing the rise of the "Digital Age").

2. *See, e.g.*, 2 GEORGE E. DIX ET AL., MCCORMICK ON EVIDENCE § 227, at 72 (Kenneth S. Broun ed., 6th ed. 2006) (noting that "the recording, communication, and preservation of digital information pervade society"); *see also infra* notes 20–25 and accompanying text.

household appliances."[3] The changes brought by this technology pervade all aspects of modern life, "chang[ing] almost everything about our relationship with information: how we create it, how much of it we create, how it is stored, who sees it, [and] how and when we dispose of it."[4]

In light of its proliferation, it should come as no surprise that digital information has begun to play a greater role in litigation.[5] Indeed, the value of electronic information has been demonstrated historically in such famous instances as President Clinton's relationship with Monica Lewinsky,[6] the Iran-Contra scandal,[7] and the Rodney King beatings.[8] Yet, throughout these vast technological and societal changes, the Federal Rules of Evidence have essentially remained static.[9] Accordingly, when faced with new forms of electronic evidence, federal courts have used vastly differing admissibility standards. This article's thesis is that the varying standards for admitting electronically stored information necessitate amendments to the Federal Rules of Evidence to provide clarity and uniformity.[10]

---

3. MANUAL FOR COMPLEX LITIGATION (FOURTH) § 11.446, at 78 (2004), *available at* http://www.fjc.gov/public/pdf.nsf/lookup/mcl4.pdf/$file/mcl4.pdf [hereinafter MANUAL FOR COMPLEX LITIGATION].

4. James Gibson, *A Topic Both Timely and Timeless*, 10 RICH. J.L. & TECH. 49, ¶ 2 (2004), *available at* http://law.richmond.edu/jolt/v10i5/article49.pdf.

5. *See, e.g.*, Bills v. Kennecott Corp., 108 F.R.D. 459, 462 (D. Utah 1985) ("Improvements in technology which advantage almost everyone have become commonplace and widespread, and because we live in a society which emphasizes both computer technology and litigation, the mix of computers and lawsuits is ever increasing."); 8B CHARLES ALAN WRIGHT ET AL., FEDERAL PRACTICE AND PROCEDURE § 2218 (Supp. 2007) (noting that "it has become evident that computers are central to modern life and consequently also to much civil litigation").

6. *See* Marianne Lavelle & Elise Ackerman, *Perjury and the President*, U.S. NEWS & WORLD REP., Oct. 5, 1998, at 22 (discussing how independent counsel Kenneth Starr used e-mails to bolster his findings and Monica Lewinsky's credibility). These e-mails were frequently cited in Starr's final report. *See generally* KENNETH W. STARR, U.S. OFFICE OF THE INDEP. COUNSEL, THE REPORT (1998), *available at* http://elections.donyell.net/other_reports/ken_starr.pdf.

7. *See* Martha Middleton, *A Discovery: There May Be Gold in E-Mail*, NAT'L L.J., Sept. 20, 1993, at 1, 40 (noting that Oliver North was "convicted in part because information was discovered on mainframe backup tapes that had been deleted from an electronic-mail system").

8. *See* M.A. Stapleton, *Discovery 'Paper Chase' Transforming Bit By Byte As Attorneys Target Computer Data*, CHI. DAILY L. BULL., Nov. 25, 1994, at 20 (noting the e-mail messages of an officer involved in the Rodney King beating, sent shortly after the incident, which stated "[o]ops, I haven't beaten anyone so bad in a long time").

9. *E.g.*, PAUL R. RICE, ELECTRONIC EVIDENCE: LAW AND PRACTICE 492 (2d ed. 2008) (noting that "new evidentiary problems faced in the Internet Age have been directly addressed in few, if any, of these evidence codes"); George L. Paul, *The "Authenticity Crisis" in Real Evidence*, LAW PRAC. TODAY, Mar. 2006, http://www.abanet.org/lpm/lpt/articles/tch03065.shtml ("Certainly no action has been taken by Congress to change the Federal Rules of Evidence to address the recent wave of digitization."). One notable exception is the recent passage of Federal Rule of Evidence 502, which was designed, in part, to address issues surrounding inadvertent waiver of the attorney-client privilege when producing electronically stored information. *See infra* notes 241–42 and accompanying text.

10. Although the Federal Rules of Evidence apply to both civil and criminal cases, *see* FED. R. EVID. 1101(b), this article will focus on ESI's role in civil litigation. Differences in the criminal context will be noted when relevant.

Part I describes what electronically stored information (ESI) is and some of the factors that led to its increasingly significant role in litigation. Part II outlines the various standards courts have adopted in response to the proliferation of this type of evidence, specifically in the areas of authentication, hearsay, and the best evidence rule. Finally, Part III proposes specific amendments to the Federal Rules of Evidence that would provide needed guidance to courts when determining the admissibility of electronically stored information.

I. BACKGROUND: THE GROWING ROLE OF ESI IN LITIGATION

A. What is ESI?

The term "electronically stored information" is broad and difficult to define.[11] Some commentators have resigned themselves to this fact and defined the term simply as "everything other than the traditional paper documents or microfilm."[12] Others provide a slightly narrower definition of "any information created, stored, or best utilized with computer technology of any type."[13] When the Advisory Committee amended the Federal Rules of Civil Procedure in 2006,[14] it noted that "[t]he wide variety of computer systems currently in use, and the rapidity of technological change, counsel against a limiting or precise definition."[15] While these technological changes may make a precise definition impossible, in litigation, ESI typically comes in several

11. Interestingly, one pocket guide for judges simply defines the term "ESI" as "[e]lectronically stored information," without attempting a further definition. BARBARA J. ROTHSTEIN ET AL., FED. JUDICIAL CTR., MANAGING DISCOVERY OF ELECTRONIC INFORMATION: A POCKET GUIDE FOR JUDGES 23 (2007), *available at* http://www.fjc.gov/public/pdf.nsf/lookup/eldscpkt.pdf/$file/eldscpkt.pdf.

12. MARIAN K. RIEDY ET AL., LITIGATING WITH ELECTRONICALLY STORED INFORMATION 5 (2007). Similarly, the Sedona Conference, a widely respected group of scholars, defines ESI as "[e]lectronically stored information, regardless of the media or whether it is in the original format in which it was created, as opposed to stored in hard copy (i.e. on paper)" in its Glossary. SEDONA CONF. WORKING GROUP, THE SEDONA CONFERENCE GLOSSARY: E-DISCOVERY & DIGITAL INFORMATION MANAGEMENT 20 (2d ed. 2007), *available at* http://www.thesedonaconference.org/content/miscFiles/TSCGlossary_12_07.pdf [hereinafter SEDONA CONFERENCE GLOSSARY; *see also* Zubulake v. UBS Warburg L.L.C., 217 F.R.D. 309, 318–20 (S.D.N.Y. 2003) (outlining five categories of electronic information).

13. CONF. OF CHIEF JUSTICES, GUIDELINES FOR STATE TRIAL COURTS REGARDING DISCOVERY OF ELECTRONICALLY-STORED INFORMATION 1 (2006), *available at* http://www.ncsconline.org/images/EDiscCCJGuidelinesFinal.pdf.

14. *See infra* Part I.B.

15. FED. R. CIV. P. 34 advisory committee's note.

common "evidentiary 'flavors,'"[16] such as e-mail,[17] Web sites and Internet postings,[18] and computer-generated documents and data files.[19]

These various forms of ESI have several fundamental differences from traditional forms of information that make them valuable for purposes of litigation. Initially, the sheer volume of ESI is substantially greater than with paper information.[20] In 2006 alone, the amount of digital information that was created, captured, or replicated was over 161 billion gigabytes or "[three] million times the information in all the books *ever* written."[21] Considering that one gigabyte of data is, according to conservative estimates, the equivalent of roughly 75,000 typed pages,[22] this amount of data would be the equivalent of over twelve *quadrillion* pages of information. If printed, it would be enough paper to fill the 110-story Sears Tower in Chicago (now known as the Willis

16. Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 538 (D. Md. 2007); *see also* 2 DIX ET AL., *supra* note 2, § 227, at 72 (noting that e-mails, Internet postings, and computer-generated documents and data files are the most commonly used forms of "e-evidence").

17. "E-mail" means "[a]n electronic means for communicating information under specified conditions, generally in the form of text messages, through systems that will send, store, process, and receive information and in which messages are held in storage until the addressee accesses them." SEDONA CONFERENCE GLOSSARY, *supra* note 12, at 18; *see also* Reno v. ACLU, 521 U.S. 844, 851 (1997) ("E-mail enables an individual to send an electronic message—generally akin to a note or letter—to another individual or to a group of addressees. The message is generally stored electronically, sometimes waiting for the recipient to check her 'mailbox' and sometimes making its receipt known through some type of prompt.").

18. The "Internet" has been defined as "[a] worldwide network of networks that all use the TCP/IP communications protocol and share a common address space. It supports services such as e-mail, the World Wide Web, file transfer (FTP), and Internet Relay Chat (IRC). Also known as 'the net,' 'the information superhighway,' and 'cyberspace.'" SEDONA CONFERENCE GLOSSARY, *supra* note 12, at 28; *see also Reno*, 521 U.S. at 852 ("In concrete terms, the Web consists of a vast number of documents stored in different computers all over the world. Some of these documents are simply files containing information. However, more elaborate documents, commonly known as Web 'pages,' are also prevalent. Each has its own address—'rather like a telephone number.' Web pages frequently contain information and sometimes allow the viewer to communicate with the page's (or 'site's') author. They generally also contain 'links' to other documents created by that site's author or to other (generally) related sites." (citation omitted)).

19. "Data" is "[a]ny information stored on a computer." SEDONA CONFERENCE GLOSSARY, *supra* note 12, at 12. A "file" is "[a] collection of data or information stored under a specified name on a disc." *Id.* at 21. Finally, a "document" is "[a] collection of pages or files produced manually or by a software application, constituting a logical single communication of information, but consisting of more than a single stand-alone record." *Id.* at 16.

20. *See, e.g.*, ARKFELD, *supra* note 1, § 1.2(G).

21. JOHN F. GANTZ ET AL., INT'L DATA CORP., THE EXPANDING DIGITAL UNIVERSE: A FORECAST OF WORLDWIDE INFORMATION GROWTH THROUGH 2010, at 1 (2007), *available at* http://www.emc.com/collateral/analyst-reports/expanding-digital-idc-white-paper.pdf (emphasis added).

22. RALPH C. LOSEY, E-DISCOVERY: CURRENT TRENDS AND CASES app. at 291 (2008). Notably, however, "[e]stimating 'pages' per gigabyte is more an art than a science," since "[t]he number of pages per gigabyte will vary significantly based on the types of files at issue." Gil Keteltas & John Rosenthal, *Discovery of Electronic Evidence*, *in* RICE, *supra* note 9, at 5 n.7. For example, one source lists a gigabyte as the equivalent of 500,000 pages, *see* MANUAL FOR COMPLEX LITIGATION, *supra* note 3, § 11.446, while another listed a gigabyte as only 250,000 pages, United States v. Triumph Capital Group, Inc., 211 F.R.D. 31, 46 (D. Conn. 2002) ("The hard drive actually contained approximately 1 GB, or 250,000 pages of data . . . ."). If the larger estimate of 500,000 pages per gigabyte is used, the equivalent number of pages for all information in 2006 would be 80.5 quadrillion.

Tower) 644 million times.[23] Further, ninety-two percent of this electronic information is stored on magnetic media and never reduced to paper form.[24] This vastly expanded pool of evidentiary sources is valuable for purposes of litigation, particularly in light of its potentially informal nature.[25]

In addition to this flood of information, there is a significant amount of redundancy, as data may be located in multiple places in multiple forms.[26] For example, a user may originally save a document on a computer and then backup that document to an external source or e-mail a copy to another user.[27] In addition to intentional copying, a computer automatically creates "replicant" data, also known as "archival" data, without any action by the user to backup files in case there is a computer malfunction or power loss.[28] This automatic backup procedure may result in multiple copies of an electronic file that a user cannot erase and often is not even aware exists.[29]

Similarly, the existence of multiple copies of information makes permanently deleting any electronic file difficult.[30] Even if a user has not made any copies intentionally, a computer will retain residual data relating to the file, which is recoverable even if an attempt is made to delete it.[31] Further, when a user "deletes" a file, the computer simply makes the space occupied by that file available for subsequent use.[32] Therefore, unless the computer overwrites

---

23. One terabyte of data is the equivalent of one thousand gigabytes, *see* GANTZ ET AL., *supra* note 21, at 2, so converting the 161 billion gigabytes of information in 2006 to terabytes equals 161 million terabytes. A single terabyte of information, if printed, would fill the Sears Tower four times. Jason Krause, *What a Concept!: New Computer Search Methods Promise Better E-Discovery Results*, A.B.A. J., Aug. 2003, at 60, 60. Thus, multiplying 161 million terabytes by four provides the fact that, if printed, the amount of information in 2006 would fill the Sears Tower 644 million times.

24. *See* PETER LYMAN & HAL R. VARIAN, HOW MUCH INFORMATION? 1 (2003), http://www2.sims.berkeley.edu/research/projects/how-much-info-2003/printable_report.pdf. This number appears to remain relatively constant over time. *See In re* Bristol-Myers Squibb Sec. Litig., 205 F.R.D. 437, 440 n.2 (D.N.J. 2002) (quoting a study finding that 93% of information was generated in digital form).

25. *See, e.g.*, ARKFELD, *supra* note 1, § 1.2(A). For an example of a case where the informal nature of e-mails hurt the defendant, see *Strauss v. Microsoft Corp.*, No. 91 Civ. 5928 (SWK), 1995 WL 326492, at *4 (S.D.N.Y. June 1, 1995) (sexual discrimination suit based, in part, upon inappropriate e-mails sent by supervisor).

26. *See* ARKFELD, *supra* note 1, § 1.2(H).

27. *See* Shira A. Scheindlin & Jeffrey Rabkin, *Electronic Discovery in Federal Civil Litigation: Is Rule 34 Up to the Task?*, 41 B.C. L. REV. 327, 336–37 (2000); *see also* Mark D. Robins, *Evidence at the Electronic Frontier: Introducing E-mail at Trial in Commercial Litigation*, 29 RUTGERS COMPUTER & TECH. L.J. 219, 224 (2003).

28. *See, e.g.*, ARKFELD, *supra* note 1, § 3.6(B); Scheindlin & Rabkin, *supra* note 27, at 336–37.

29. *See, e.g.*, ARKFELD, *supra* note 1, § 3.6(B); Scheindlin & Rabkin, *supra* note 27, at 336–37.

30. *See, e.g.*, Christine Sgarlata Chung & David J. Byer, *The Electronic Paper Trail: Evidentiary Obstacles to Discovery and Admission of Electronic Evidence*, 4 B.U. J. SCI. & TECH. L. 5, ¶¶ 12–18 (1998).

31. *See* ARKFELD, *supra* note 1, § 3.6(B); *see also* Scheindlin & Rabkin, *supra* note 27, at 337.

32. *See* Scheindlin & Rabkin, *supra* note 27, at 337.

the "deleted" file, generally, it can be recovered.[33] Thus, electronic evidence can still be found even if a party attempts to destroy it.[34]

Electronically stored information is also much easier to manipulate than traditional forms of evidence.[35] As technology permeates society, more people have the ability to easily alter ESI—and at an increasingly lower cost.[36] As one commentator noted, manipulation is far easier, in part, because "[e]diting software exists for almost all types of digital information, whether it be business records (word processing), photographs (image editing software), or sound (digital audio workstations)."[37] E-mail is also susceptible to manipulation. In one recent case, for example, the court rejected an e-mail offered by a party because the time stamp indicated that it was sent seven months in the future.[38]

Metadata, or "data about data,"[39] is another aspect of ESI that is not present with printed information.[40] With printed copies, all of the relevant information is clearly visible.[41] In contrast, with ESI, metadata can be embedded within a file, providing information about that file, "such as the date it was created, its author, when and by whom it was edited, what edits were made, and, in the case of e-mail, the history of its transmission."[42] A computer can create this metadata automatically, or a user can provide it.[43] This information is generally not visible when a document is printed or converted to a different format.[44] Thus, metadata is important because it means that producing a printout of an electronically stored document in discovery does not necessarily convey all of the information that may be available about that document.[45]

---

33. *See id.*; *see also* RICE, *supra* note 9, at xix (noting that electronic evidence is often "hard to kill").

34. *See, e.g.*, ARKFELD, *supra* note 1, § 3.6(B); Chung & Byer, *supra* note 30, ¶ 12.

35. *See, e.g.*, ARKFELD, *supra* note 1, § 3.1(D); RICE, *supra* note 9, at 303–05; Chung & Byer, *supra* note 30, ¶¶ 22–25; Paul, *supra* note 9.

36. *See, e.g.*, Paul, *supra* note 9.

37. *Id.*

38. *See* Network Alliance Group L.L.C. v. Cable & Wireless USA, Inc., No. CIV 02-644DWFAJB, 2002 WL 1205734, at *1 & n.2 (D. Minn. May 31, 2002) (acknowledging "inconsistencies within the alleged e-mail correspondence which suggest that the correspondence is not authentic. Most notably, the 'date stamp' for one of the e-mail messages is Thursday, December 6, 2002. Obviously, December 6, 2002, has not yet arrived. Moreover, December 6, 2001, was a Thursday, but December 6, 2002, will be a Friday.").

39. Madison River Mgmt. Co. v. Bus. Mgmt. Software Corp., 387 F. Supp. 2d 521, 528 n.5 (M.D.N.C. 2005); *see also* SEDONA CONFERENCE GLOSSARY, *supra* note 12, at 33 (defining metadata, in part, as "[d]ata typically stored electronically that describes characteristics of ESI, found in different places in different forms"). *See generally* W. Lawrence Wescott II, *The Increasing Importance of Metadata in Electronic Discovery*, 14 RICH. J.L. & TECH. 10 (2008) (discussing the various types of metadata and how they are used in litigation).

40. *See, e.g.*, ARKFELD, *supra* note 1, § 3.7(A).

41. *See id.*

42. ROTHSTEIN ET AL., *supra* note 11, at 3.

43. *See* RICE, *supra* note 9, at 235; *see also* SEDONA CONFERENCE GLOSSARY, *supra* note 12, at 33 (noting that metadata "[c]an be supplied by applications, users or the file system").

44. *See* RICE, *supra* note 9, at 234.

45. *See, e.g.*, ARKFELD, *supra* note 1, §§ 1.4(C), 3.7(A).

However, metadata, like all ESI, is prone to manipulation, potentially making it an inaccurate or misleading source of information.[46] This alteration can occur intentionally or inadvertently.[47] For example, metadata can reflect that an electronic document was modified, when in fact it was only accessed or saved to a different location.[48] These various unique characteristics of ESI, such as metadata, demonstrate the significant differences between ESI and traditional printed copies of information.

B. The E-Discovery Amendments to the Federal Rules of Civil Procedure

Before 2006, the Federal Rules of Civil Procedure had not been amended to reflect the issues presented by computers since 1970.[49] Although judges and practitioners realized that "digital is different," the common view was that the existing rules could accommodate this form of evidence.[50] However, because of the problems that began to arise in connection with the growth of technology, the Rules were amended in 2006 to provide additional guidance for the discovery of electronically stored information.[51]

Although a complete discussion of these changes is beyond the scope of this article, the effect of these amendments was to regulate and expand the role of ESI in litigation.[52] Generally, these amendments resulted in the "discovery of electronically stored information stand[ing] on equal footing with [the] discovery of paper documents."[53] Recognizing the variety of computer systems in existence and the pace at which technology was changing, the Rules adopted an expansive definition of ESI to include "any type of information that is stored electronically."[54]

---

46. *See* RICE, *supra* note 9, at 234–35.

47. *See* SEDONA CONFERENCE GLOSSARY, *supra* note 12, at 33.

48. *E.g.*, Fennell v. First Step Designs, Ltd., 83 F.3d 526, 530–31 (1st Cir. 1996); *see* Sedona Conference Working Group, *The Sedona Conference Commentary on ESI Evidence & Admissibility*, 9 SEDONA CONF. J. 217, 227, 229 (2008) (noting some of the methods that can be used to manipulate metadata).

49. *E.g.*, Lee H. Rosenthal, *A Few Thoughts on Electronic Discovery After December 1, 2006*, 116 YALE L.J. POCKET PART 167, 167 (2006) ("The last time the Federal Rules of Civil Procedure were amended to acknowledge computers was 1970, when the words 'data and data compilations' were added to Rule 34.").

50. Kenneth J. Withers, *Electronically Stored Information: The December 2006 Amendments to the Federal Rules of Civil Procedure*, 4 NW. J. TECH. & INTELL. PROP. 171, 172 (2006), http://www.law.northwestern.edu/journals/njtip/v4/n2/3/J.%20Withers.pdf.

51. *Id.* at 191–94.

52. For a complete discussion of the e-discovery amendments, see generally Rosenthal, *supra* note 49 and Withers, *supra* note 50. For a discussion of the initial case law interpreting these amendments, see generally Emily Burns et al., *E-Discovery: One Year of the Amended Federal Rules of Civil Procedure*, 64 N.Y.U. ANN. SURV. AM. L. 201 (2008).

53. FED. R. CIV. P. 34 advisory committee's note.

54. *Id.* The Advisory Committee notes to Rule 34 go on to state that "[r]eferences elsewhere in the rules to 'electronically stored information' should be understood to invoke this expansive approach." *Id.*

More specifically, several amendments require parties to pay attention to the discovery of ESI early in litigation. An amendment to Rule 26(f) requires parties to discuss and develop a proposed plan for "any issues relating to disclosure or discovery of electronically stored information, including the form or forms in which it should be produced."[55] Similarly, an amendment to Rule 16 allows a court's scheduling order to address ESI.[56]

Amendments also address the production of ESI. First, changes to Rule 26(a)(1)(B) require parties to provide a copy or description of all electronically stored information that was in their control, along with any documents or physical evidence, that may be used to support claims or defenses.[57] Another amendment limits the scope of discovery required when ESI was "not reasonably accessible because of undue burden or cost."[58] This provision recognizes the various issues that may arise when attempting to locate or retrieve ESI, such as remnants of deleted files that may require substantial effort to recover.[59]

If the parties are unable to reach an agreement in the Rule 26(f) conference, an amendment to Rule 34(b) "provide[s] a default procedure for the production of electronically stored information."[60] Recognizing that ESI may exist in several forms, the rule allows a discovery request to "specify the form or forms in which electronically stored information is to be produced."[61]

If a requesting party does not specify a particular form of ESI, the responding party has two options. First, the party can produce the information in "a form or forms in which it is ordinarily maintained."[62] Alternatively, a party can produce the information in a "reasonably usable form."[63] Regardless, "a party need not produce the same electronically stored information in more than one form."[64]

---

55. FED. R. CIV. P. 26(f). As noted by the Advisory Committee, "[t]he particular issues regarding electronically stored information that deserve attention during the discovery planning stage depend on the specifics of the given case." *Id.* advisory committee's note. This amendment was important in light of the complicated preservation obligations created by the volume and dynamic nature of ESI. *Id.* Because computers may both automatically create and delete or overwrite files during the course of ordinary operation, the Advisory Committee was concerned that failure to address these issues early in litigation would result in uncertainty and increase the potential for disputes. *Id.*

56. FED. R. CIV. P. 16(b)(3)(B)(iii). The Advisory Committee's notes stated that "[t]he amendment . . . is designed to alert the court to the possible need to address the handling of discovery of electronically stored information early in the litigation." *Id.* advisory committee's note.

57. FED. R. CIV. P. 26(a)(1)(B).

58. FED. R. CIV. P. 26(b)(2)(B).

59. *See* Rosenthal, *supra* note 49, at 168–69.

60. Withers, *supra* note 50, at 203.

61. FED. R. CIV. P. 34(b). Of course, the responding party retains the ability to object to the form of ESI production sought. *See id.*

62. FED. R. CIV. P. 34(b)(2)(E)(ii). Many commentators have interpreted this provision to mean that ESI can be produced in its "native file format." *E.g.*, Withers, *supra* note 50, at 203.

63. FED. R. CIV. P. 34(b)(2)(E)(ii). This option may require a party to "'translate' information it produces into a 'reasonably usable' form." *Id.* advisory committee's note.

64. FED. R. CIV. P. 34(b)(2)(E)(iii).

Several additional amendments address miscellaneous issues presented by allowing the discovery of ESI. For example, a change to Rule 26(b)(5) addresses the potential for waiver of the attorney-client privilege by producing ESI.[65] Another provision protects a party from sanctions for the failure to provide ESI lost "as a result of the routine, good-faith operation of an electronic information system."[66] Further, a Rule 33 amendment allows interrogatories to be answered by producing electronically stored business records.[67] Overall, these "e-discovery" amendments created provisions "designed to integrate electronic evidence and materials into every stage of the litigation process."[68]

II. CURRENT ATTEMPTS TO APPLY THE FEDERAL RULES OF EVIDENCE TO ESI

Despite ensuring the discoverability of ESI, to date, no changes have been made to clarify how and when this newly discoverable evidence will be admissible at trial.[69] Accordingly, judges have been forced to resolve the evidentiary issues presented by ESI through a growing body of diverse, and often diametrically opposed, opinions.[70] This section examines how courts have applied the Federal Rules of Evidence to ESI, specifically in the areas of authentication, hearsay, and the best evidence rule.

A. Authentication

1. *General Authentication Rules*

In order for evidence to be admissible, it must be authenticated.[71] Federal Rule of Evidence 901 provides that the authentication requirement is "a condition precedent to admissibility," which is "satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims."[72]

65. FED. R. CIV. P. 26 advisory committee's note; *see* Withers, *supra* note 50, at 201–02.

66. FED. R. CIV. P. 37(f).

67. FED. R. CIV. P. 33(d).

68. Timothy J. Chorvat, *E-Discovery and Electronic Evidence in the Courtroom: A Primer for Business Lawyers*, BUS. L. TODAY, Sept.–Oct. 2007, http://www.abanet.org/buslaw/blt/2007-09-10/chorvat.shtml; *see also* PSEG Power N.Y., Inc. v. Alberici Constructors, Inc., No. 1:05-CV-657 (DNH/RFT), 2007 WL 2687670, at *1 (N.D.N.Y. Sept. 7, 2007) ("With the rapid and sweeping advent of electronic discovery, the litigation landscape has been radically altered in terms of scope, mechanism, cost, and perplexity.").

69. *See supra* note 9 and accompanying text.

70. *See* RICE, *supra* note 9, at 492. Generally, courts make preliminary rulings on the admissibility of evidence. *See* FED. R. EVID. 104.

71. FED. R. EVID. 901.

72. FED. R. EVID. 901(a).

Essentially, this requirement is a "special aspect of relevancy"—if evidence is not authentic, it has no relevance to the case.[73]

Pursuant to Rule 104(b), a judge must be satisfied that there is sufficient evidence to support a finding by the trier of fact that the evidence at issue is what its proponent claims.[74] Typically, this standard is "not a particularly high barrier to overcome."[75] Thus, for example, to authenticate a photograph, a witness may testify that it accurately represents the depicted scene, regardless of whether that witness took the photograph or was present when it was taken.[76]

Rule 901 provides a non-exhaustive list of illustrations of how the authentication requirement can be satisfied.[77] For example, testimony from a witness with knowledge that "a matter is what it is claimed to be" will suffice.[78] Any distinctive characteristics of the evidence can also be used for authentication purposes.[79] Although this provision contains several subsections targeted at specific types of evidence, such as telephone conversations, there is currently no provision specifically addressing electronically stored information.[80] Rule 902 also provides various methods that allow a piece of evidence to be self-authenticating.[81]

Notably, even if evidence is authentic, it "by no means assures admission of an item into evidence, as other bars, hearsay for example, may remain."[82] However, as one court noted, "the inability to get evidence admitted because of a failure to authenticate it almost always is a self-inflicted injury which can be avoided by thoughtful advance preparation."[83]

---

73. FED. R. EVID. 901 advisory committee's note; *see also* 31 CHARLES ALAN WRIGHT & VICTOR JAMES GOLD, FEDERAL PRACTICE AND PROCEDURE § 7102 (2000) ("Thus, Rule 901 does not have to create the authentication requirement because it is implicit in Rule 402, which makes inadmissible evidence that is irrelevant."). For example, in a prosecution for drug possession, if the prosecution attempted to introduce a bag of drugs, that evidence would not be relevant unless it could be proven that the specific bag of drugs that was being introduced was the same bag that had been found on the defendant. *See* 31 WRIGHT & GOLD, *supra*, § 7102.

74. FED. R. EVID. 104(b); *see also infra* note 347.

75. Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 542 (D. Md. 2007).

76. *E.g.*, United States v. Lawson, 494 F.3d 1046, 1052 (D.C. Cir. 2007) ("A photograph may be authenticated if a witness with knowledge of the scene testifies that it accurately depicts the scene it purports to represent."); United States v. Clayton, 643 F.2d 1071, 1074 (5th Cir. Unit B Apr. 1981) ("A witness qualifying a photograph need not be the photographer or see the picture taken; it is sufficient if he recognizes and identifies the object depicted and testifies that the photograph fairly and correctly represents it.").

77. *See* FED. R. EVID. 901(b); *see also id.* advisory committee's note ("The examples are not intended as an exclusive enumeration of allowable methods but are meant to guide and suggest, leaving room for growth and development in this area of the law.").

78. FED. R. EVID. 901(b)(1).

79. *See* FED. R. EVID. 901(b)(4).

80. FED. R. EVID. 901(b); *see* 2 DIX ET AL., *supra* note 2, § 227, at 72.

81. *See* FED. R. EVID. 902.

82. FED. R. EVID. 901 advisory committee's note; *see* 2 DIX ET AL., *supra* note 2, § 227, at 73.

83. Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 542 (D. Md. 2007). For example, in civil cases, parties can use FED. R. CIV. P. 36(a)(1)(B) to request that an opponent admit the "genuineness of documents." A party can also request, pursuant to FED. R. CIV. P. 16(c)(2)(C),

Authentication rules address several evidentiary concerns. First, they prevent fraud by requiring a party to show that its evidence is complete and unaltered.[84] Additionally, authentication prevents innocent mistakes by ensuring that evidence originates from its named source.[85] One example of this justification is when a plaintiff erroneously attributes a document to the defendant, but in fact, a different person who has the same name signed it.[86] Finally, authentication requirements prevent "jury credulity," or a jury's psychological tendency to take matters at face value and "assume the connection of a writing with a particular individual when such a connection is suggested, no matter how inconclusively, by the writing itself."[87]

Although the authentication requirement applies to electronically stored information,[88] ESI poses several unique authentication concerns. Primarily, these concerns revolve around the potential for the easier alteration or fabrication of ESI than traditional forms of physical evidence.[89] Web sites exemplify these concerns. Authors create, revise, and delete these sites on a daily basis.[90] No external checks exist to ensure that information on a site is accurate.[91] Accordingly, the ease with which a Web site can be altered makes it difficult for visitors, or a court, to determine whether they "are literally on the same page when they visit the site on different dates."[92] As Web sites demonstrate, ESI presents several unique challenges to the application of the authentication requirement.

---

that the opposing party admit that documents are authentic. Finally, if proper pretrial disclosure of documents is made using FED. R. CIV. P. 26(a)(3), an opposing party's failure to file objections within fourteen days waives most objections, unless the court excuses the waiver for good cause. *Lorraine*, 241 F.R.D. at 553.

84. *See, e.g.*, 5 CHRISTOPHER B. MUELLER & LAIRD C. KIRKPATRICK, FEDERAL EVIDENCE § 9:2 (3d ed. 2006); RICE, *supra* note 9, at 335; John William Strong, *Liberalizing the Authentication of Private Writings*, 52 CORNELL L. REV. 284, 285 (1967). Similarly, because the authentication requirement ensures the trustworthiness of evidence, it can implicate analysis in other areas, such as hearsay. *E.g.*, *Lorraine*, 241 F.R.D. at 542.

85. *See, e.g.*, 5 MUELLER & KIRKPATRICK, *supra* note 84, § 9:2; Strong, *supra* note 84, at 285–86.

86. *See* RICE, *supra* note 9, at 335; 7 JOHN HENRY WIGMORE, EVIDENCE IN TRIALS AT COMMON LAW § 2130, at 709–11 (James H. Chadbourn rev. 1978).

87. Strong, *supra* note 84, at 286–87; *see* 5 MUELLER & KIRKPATRICK, *supra* note 84, § 9:2; 7 WIGMORE, *supra* note 86, § 2129, at 704.

88. 5 JACK B. WEINSTEIN & MARGARET A. BERGER, WEINSTEIN'S FEDERAL EVIDENCE § 900.06(1)(b) (Joseph M. McLaughlin ed., 2d ed. 2008) ("The Federal Rules of Evidence, including Rule 901, apply to computer-based evidence in the same way as they do to other evidence."); *see* Am. Express Travel Related Servs. Co. v. Vee Vinhnee (*In re* Vee Vinhnee), 336 B.R. 437, 444 (B.A.P. 9th Cir. 2005) ("Authenticating a paperless electronic record, in principle, poses the same issue as for a paper record, the only difference being the format in which the record is maintained: one must demonstrate that the record that has been retrieved from the file, be it paper or electronic, is the same as the record that was originally placed into the file." (citing FED. R. EVID. 901(a))); *Lorraine*, 241 F.R.D. at 541 ("In order for ESI to be admissible, it also must be shown to be authentic.").

89. *See, e.g.*, ARKFELD, *supra* note 1, § 8.11(B).

90. *See, e.g.*, RICE, *supra* note 9, at 311.

91. *See id.* As a result, authenticating a Web site's content "often poses a difficult hurdle." *Id.*

92. Fenner v. Suthers, 194 F. Supp. 2d 1146, 1149 (D. Colo. 2002).

2. *General Approaches to Authenticating ESI*

Courts have taken widely varying approaches to the authentication of ESI. Some courts are highly skeptical and adopt a tough standard for authentication. For example, in *St. Clair v. Johnny's Oyster & Shrimp, Inc.*, the plaintiff brought claims for personal injuries he allegedly sustained while working on a boat owned by the defendant.[93] The plaintiff attempted to introduce data from the U.S. Coast Guard's Web site to refute the defendant's claim that it never owned the ship on which the plaintiff worked.[94]

The court held that the "[p]laintiff's electronic 'evidence' is totally insufficient," because "[w]hile some look to the Internet as an innovative vehicle for communication, the Court continues to warily and wearily view it largely as one large catalyst for rumor, innuendo, and misinformation."[95] The court concluded that "this so-called Web provides no way of verifying the authenticity" of the plaintiff's claims.[96] Accordingly, "[t]here is no way Plaintiff can overcome the presumption that the information he discovered on the Internet is inherently untrustworthy."[97] Further, the court noted, "any evidence procured off the Internet is adequate for almost nothing," and instead of relying upon such "voodoo information," a hard copy or other legitimate source was required.[98] Other courts agree with this sentiment and adopt similarly stringent authentication requirements for ESI.[99]

In contrast, other courts liberally construe the rules of evidence to maximize the admissibility of ESI. Under this approach, given the prevalence of technology in society, a judge will "accept things as authentic if they seem

---

93. St. Clair v. Johnny's Oyster & Shrimp, Inc., 76 F. Supp. 2d 773, 774 (S.D. Tex. 1999).

94. *Id.*

95. *See id.*

96. *Id.*

97. *Id.* The court went on to note that:

> Anyone can put anything on the Internet. No web-site is monitored for accuracy and *nothing* contained therein is under oath or even subject to independent verification absent underlying documentation. Moreover, the Court holds no illusions that hackers can adulterate the content on *any* website from *any* location at *any* time.

Id. at 775.

98. *Id.* at 775. The same judge reaffirmed these views in several subsequent, more recent, cases. *See, e.g.*, Perforaciones Maritimas Mexicanas S.A. de C.V. v. Seacor Holdings, Inc., 443 F. Supp. 2d 825, 832 (S.D. Tex. 2006); Barbour v. Head, 178 F. Supp. 2d 758, 760 n.3 (S.D. Tex. 2001).

99. *See, e.g.*, United States v. Jackson, 208 F.3d 633, 638 (7th Cir. 2000) (finding that postings on a Web site were not authenticated because they categorically lacked indications of trustworthiness); Wady v. Provident Life & Accident Ins. Co., 216 F. Supp. 2d 1060, 1064–65 (C.D. Cal. 2002); McReynolds v. Lowe's Cos., No. CV08-335-S-EJL, 2008 WL 5234047, at *7 (D. Idaho Dec. 12, 2008); Curran v. Amazon.com, Inc., Civ. Action No. 2:07-0354, 2008 WL 472433, at *14 (S.D. W. Va. Feb. 19, 2008) ("A party's website is self-serving and there is no assurance that the content is authentic. Relying on a party's website in support of its argument is akin to relying on their memoranda." (citation omitted)); *see also* Perma Research & Dev. v. Singer Co., 542 F.2d 111, 121 (2d Cir. 1976) (Van Graafeiland, J., dissenting) ("As one of the many who have received computerized bills and dunning letters for accounts long since paid, I am not prepared to accept the product of a computer as the equivalent of Holy Writ. Neither should a District Judge.").

authentic, and if no questions are raised by the opponent."[100] As stated by one court, Rule 901(a) is "general or elastic," which caused the court to overrule a party's authentication objections to various Internet documents, even though their proponent had not individually authenticated them.[101] Courts adopting this approach generally tend to admit ESI evidence and relegate authentication concerns to the jury to assess as part of determining its proper weight.[102]

3. *Approaches to ESI Authentication Under Rule 901(b)*

Courts also take widely varying approaches to the authentication of ESI under the illustrations contained in Rule 901(b).[103] First, Rule 901(b)(1) provides that evidence can be authenticated by "testimony that a matter is what it is claimed to be."[104] Different standards have developed for how technical this testimony must be for ESI, as well as who may testify. For example, for evidence from Web sites, some courts require testimony establishing that the content of the site is authentic, such as testimony from a corporate representative that the information on the site was placed there by the corporation.[105] These courts, similar to the attitude taken in *St. Clair*,[106] are concerned with the potential for hackers to slip information onto a company's Web site.[107]

Other courts have stated that testimony from individuals with knowledge of the process used to obtain ESI is sufficient for authentication purposes.

---

100. RICE, *supra* note 9, at 374.

101. Moose Creek, Inc. v. Abercrombie & Fitch Co., 331 F. Supp. 2d 1214, 1225 n.4 (C.D. Cal. 2004).

102. *See, e.g.*, United States v. Barlow, 568 F.3d 215, 220 (5th Cir. 2009) (upholding a district court's decision to admit transcripts of an online chat over the defendant's authentication objection because "[t]he ultimate responsibility for determining whether evidence is what its proponent says it is rests with the jury"); United States v. Meienberg, 263 F.3d 1177, 1181 (10th Cir. 2001) ("Any question as to the accuracy of the printouts, whether resulting from incorrect data entry or the operation of the computer program, as with inaccuracies in any other type of business records, would have affected only the weight of the printouts, not their admissibility." (quoting United States v. Catabran, 836 F.2d 453, 458 (9th Cir.1988))); United States v. Tank, 200 F.3d 627, 630 (9th Cir. 2000) (noting, in a criminal case involving chat room logs, that "[t]he government need only make a prima facie showing of authenticity" (quoting United States v. Black, 767 F.2d 1334, 1342 (9th Cir. 1985))); Olympic Ins. Co. v. H.D. Harrison, Inc., 418 F.2d 669, 670 (5th Cir. 1969) (noting that computer printouts have a "prima facie aura of reliability"); *Moose Creek, Inc.*, 331 F. Supp. 2d at 1225 n.4; Bauman v. DaimlerChrysler AG, No. C-04-00194 RMW, 2005 WL 3157472, at *4–5 (N.D. Cal. Nov. 22, 2005); Telewizja Polska USA, Inc. v. Echostar Satellite Corp., No. 02C3293, 2004 WL 2367740, at *6 (N.D. Ill. Oct. 15, 2004); RICE, *supra* note 9, at 374–75.

103. As previously noted, these illustrations are nonexclusive. *See supra* note 77 and accompanying text.

104. FED. R. EVID. 901(b)(1).

105. *See, e.g.*, Wady v. Provident Life & Accident Ins. Co., 216 F. Supp. 2d 1060, 1064 (C.D. Cal. 2002); Terbush v. United States, No. 1:02-CV-5509SMS, 2005 WL 3325954, at *5 n.4 (E.D. Cal. Dec. 7, 2005), *aff'd in part, rev'd in part on other grounds*, 516 F.3d 1125 (9th Cir. 2008) ("Information on internet sites presents special problems of authentication. A proponent should be able to show that the information was posted by the organization/s to which it is attributed."); *see also* United States v. Jackson, 208 F.3d 633, 638 (7th Cir. 2000) (requiring a party to show that a Web site posting was actually placed there by the group that operated the site).

106. St. Clair v. Johnny's Oyster & Shrimp, Inc., 76 F. Supp. 2d 773 (S.D. Tex. 1999).

107. *See, e.g.*, *Jackson*, 208 F.3d at 637–38.

When authenticating Internet evidence, this means that testimony from webmasters, or even simply individuals who viewed the site, will suffice.[108] Similarly, most courts hold that testimony from participants in online chats suffices to authenticate a transcript of the chat.[109] Many courts also adopt analogous standards for witness testimony authenticating computerized records, requiring only testimony demonstrating that the witness was present when the information was retrieved from the computer.[110] These courts rationalize this approach by stressing the low threshold required for the authentication requirement to be satisfied, as well as the opposing party's ability to introduce evidence disproving the information's authenticity.[111]

One example of this approach is *United States v. Whitaker*.[112] In *Whitaker*, the defendant was convicted of conspiracy to distribute marijuana.[113] On appeal, the defendant argued that the prosecution failed to properly authenticate, and the trial court erred by admitting, printouts of information taken from his co-conspirator's computer.[114] Specifically, the defendant argued that his co-conspirator assisted law enforcement officers in retrieving the evidence from the computer, potentially compromising the information's authenticity.[115] Because the defendant had no evidence disproving the authenticity of the printouts, the court rejected this argument and concluded the trial court properly admitted them into evidence.[116]

Similar differing standards for the proper form of testimony exist when authenticating e-mail under Rule 901(b)(1). Some courts analogize e-mails to

---

108. *See, e.g., In re* Homestore.com, Inc. Sec. Litig., 347 F. Supp. 2d 769, 782–83 (C.D. Cal. 2004) (stating that testimony from a "webmaster or someone else with personal knowledge" is sufficient for authentification purposes); Nightlight Sys., Inc. v. Nitelites Franchise Sys., Inc., Civ. Action No. 1:04-CV-2112-CAP, 2007 WL 4563875, at *6 (N.D. Ga. May 11, 2007); St. Luke's Cataract & Laser Inst., P.A. v. Sanderson, No. 8:06-CV-223-T-MSS, 2006 WL 1320242, at *2 (M.D. Fla. May 12, 2006); Telewizja Polska USA, Inc. v. Echostar Satellite Corp., No. 02C3293, 2004 WL 2367740, at *6 (N.D. Ill. Oct. 15, 2004).

109. *See, e.g.*, United States v. Barlow, 568 F.3d 215, 220 (5th Cir. 2009); United States v. Gagliardi, 506 F.3d 140, 151 (2d Cir. 2007); United States v. Tank, 200 F.3d 627, 630–31 (9th Cir. 2000); United States v. Simpson, 152 F.3d 1241, 1249–50 (10th Cir. 1998).

110. *See, e.g.*, United States v. Whitaker, 127 F.3d 595, 601–02 (7th Cir. 1997) (concluding that printouts of computer records were properly authenticated by testimony from an FBI agent describing how and when the records were retrieved); United States v. Kassimu, 188 F. App'x 264, 264 (5th Cir. 2006) (noting that a witness's familiarity with the procedure of how computerized records were generated was sufficient to authenticate them); SEC v. Berger, 244 F. Supp. 2d 180, 191–92 & n.12 (S.D.N.Y. 2001) (affidavit from witness stating that witness had retrieved documents from company's computers and that the attached documents were the same documents she retrieved was sufficient to authenticate); United States v. Scott-Emuakpor, No. 1:99-CR-138, 2000 WL 288443, at *14 (W.D. Mich. Jan. 25, 2000) (stating that the authentication requirement may be satisfied by "testimony of a witness who was present and observed the procedure by which the documents were obtained from [the d]efendant's computers").

111. *See, e.g., Telewizja Polska USA, Inc.*, 2004 WL 2367740, at *6.

112. *Whitaker*, 127 F.3d 595.

113. *Id.* at 597.

114. *Id.* at 599–600.

115. *See id.* at 602.

116. *See id.* at 601–02. In fact, the court dismissed the defendant's arguments as "wild-eyed speculation." *Id.* at 602.

regular letters and require testimony from the sender of the e-mail for authentication purposes.[117] In contrast, other courts require testimony from the recipient of the e-mail.[118] Further, some courts state that testimony from either the sender *or* the recipient will authenticate an e-mail.[119] Regardless of the testimony necessary, some courts impose an additional requirement that a party prove that the e-mail was actually received in order for it to be authenticated.[120] As these cases indicate, courts remain divided over how to apply Rule 901(b)(1) to various forms of ESI.

Another illustration in Rule 901(b) states that evidence can be authenticated by "[a]ppearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with the circumstances."[121] Many courts have used this illustration to authenticate ESI.[122] Indeed, according to one court, this illustration is "one of the most frequently used to authenticate e-mail and other electronic records."[123]

However, while courts have been willing to apply Rule 901(b)(4) to authenticate ESI, the degree of distinctiveness demanded by each court varies significantly. For example, when faced with computerized information, parties often attempt to introduce a printout.[124] With Internet sources, if this printout contains the Web site's domain name and a date, these characteristics are often sufficiently distinctive to qualify under Rule 901(b)(4).[125] Similarly, some

---

117. *See, e.g.*, United States v. Safavian, 435 F. Supp. 2d 36, 40 (D.D.C. 2006); *In re* Homestore.com, Inc. Sec. Litig., 347 F. Supp. 2d 769, 781 (C.D. Cal. 2004); Middlebrook v. Anderson, No. Civ.A. 3:04-CV-2294, 2005 WL 350578, at *4 n.7 (N.D. Tex. Feb. 11, 2005); *see also* Uncle Henry's Inc. v. Plaut Consulting Inc., 240 F. Supp. 2d 63, 71 (D. Me. 2003) (noting that "e-mails (like letters and other documents) must be properly authenticated or shown to be self-authenticating"); Hasbro, Inc. v. Clue Computing, Inc., 66 F. Supp. 2d 117, 124 (D. Mass. 1999) (noting that unless a party verifies the source of an e-mail, that e-mail has "limited value as evidence").

118. *See, e.g.*, B.S. *ex rel.* Schneider v. Bd. of Sch. Trs., Fort Wayne Cmty. Schs., 255 F. Supp. 2d 891, 893–94 (N.D. Ind. 2003).

119. *See, e.g.*, Tibbetts v. RadioShack Corp., No. 03 C 2249, 2004 WL 2203418, at *15 (N.D. Ill. Sept. 29, 2004).

120. *See, e.g.*, Recursion Software, Inc. v. Interactive Intelligence, Inc., 425 F. Supp. 2d 756, 771–72 & n.8 (N.D. Tex. 2006); Fenje v. Feld, 301 F. Supp. 2d 781, 809 (N.D. Ill. 2003); *Schneider*, 255 F. Supp. 2d at 893–94.

121. FED. R. EVID. 901(b)(4).

122. *See, e.g.*, United States v. Siddiqui, 235 F.3d 1318, 1322–23 (11th Cir. 2000) (authenticating e-mails); *Safavian*, 435 F. Supp. 2d at 40 (authenticating e-mails); Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1153–54 (C.D. Cal. 2002) (authenticating Web sites); Brown v. Wireless Networks, Inc., No. C 07-4301 EDL, 2008 WL 4937827, at *4 (N.D. Cal. Nov. 17, 2008) (authenticating e-mails); United States *ex rel.* Parikh v. Premera Blue Cross, No. C01-0476P, 2006 WL 2841998, at *6 (W.D. Wash. Sept. 29, 2006) (using this illustration to authenticate a printout of a case from Westlaw).

123. Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 546 (D. Md. 2007); *see* Sheldon M. Finkelstein & Evelyn R. Storch, *Admissibility of Electronically Stored Information: It's Still the Same Old Story*, LITIG., Spring 2008, at 13, 14.

124. *See* 5 MUELLER & KIRKPATRICK, *supra* note 84, § 9:9.

125. *See, e.g.*, *Perfect 10, Inc.*, 213 F. Supp. 2d at 1154; Premier Nutrition, Inc. v. Organic Food Bar, Inc., No. SACV 06-0827 AG (RNBx), 2008 WL 1913163, at *6 (C.D. Cal. Mar. 27, 2008); EEOC v. E.I. DuPont de Nemours & Co., No. Civ.A. 03-1605, 2004 WL 2347559, at *2 (E.D. La. Oct. 18, 2004).

courts hold that the presence of a unique e-mail address on a printout is distinctive enough to authenticate it.[126] This approach is premised on the relatively low hurdle posed by the authentication requirement, as well as practicality concerns.[127]

Again, however, other courts reach a different conclusion. For Internet sources, these courts hold that the presence of a domain name and date on a printout is insufficient for authentication purposes.[128] As the Third Circuit noted when faced with printouts from a Web site, "[a]nyone may purchase an [I]nternet address, and so, without proceeding to discovery or some other means of authentication, it is premature to assume that a webpage is owned by a company merely because its trade name appears in the uniform resource locator."[129] Thus, courts differ in applying this illustration when faced with ESI.

Another illustration that courts have applied to ESI in drastically different ways is Rule 901(b)(9), which provides a method of authenticating the results of a process or system.[130] Some courts remain wary of the potential for fraud and therefore require parties to present elaborate evidence demonstrating the integrity of a computerized storage system.[131] Other courts, however, indicate that printouts of preexisting ESI from a computer do not even fall under this illustration, and that even if they did, a modicum of circumstantial evidence would suffice to authenticate them.[132]

---

126. *See, e.g.*, *Siddiqui*, 235 F.3d at 1322–23; *Safavian*, 435 F. Supp. 2d at 40–41; Fenje v. Feld, 301 F. Supp. 2d 781, 810 (N.D. Ill. 2003); Clement v. Cal. Dep't of Corr., 220 F. Supp. 2d 1098, 1111 (N.D. Cal. 2002); *Parikh*, 2006 WL 2841998, at *7; *see also* Discover Re Managers, Inc. v. Preferred Employers Group, Inc., No. 3:05-CV-809, 2006 WL 2838901, at *7–8 (D. Conn. Sept. 29, 2006) (examining circumstantial evidence such as an e-mail address and witness testimony to hold that a party sufficiently authenticated e-mails).

127. *See, e.g.*, *Perfect 10, Inc.*, 213 F. Supp. 2d at 1154; *Premier Nutrition, Inc.*, 2008 WL 1913163, at *6.

128. *See, e.g.*, *In re* Homestore.com, Inc. Sec. Litig., 347 F. Supp. 2d 769, 782–83 (C.D. Cal. 2004) (stating that, for Internet postings, a time stamp and URL on a printout is not sufficient to authenticate); *see also* Victaulic Co. v. Tieman, 499 F.3d 227, 236 (3d Cir. 2007) (noting that the fact that a URL contains a company's name is not enough to authenticate information from that site).

129. *Victaulic Co.*, 499 F.3d at 236.

130. FED. R. EVID. 901(b)(9) (stating that authentication can occur through "[e]vidence describing a process or system used to produce a result and showing that the process or system produces an accurate result").

131. *See, e.g.*, Am. Express Travel Related Servs. Co. v. Vee Vinhnee (*In re* Vee Vinhnee), 336 B.R. 437, 446 (B.A.P. 9th Cir. 2005) (adopting an eleven-step test for determining when computerized records fall under this illustration).

132. *See, e.g.*, United States v. Meienberg, 263 F.3d 1177, 1181 (10th Cir. 2001) ("The computer printouts were not the result of a process or system used to produce a result; they were merely printouts of pre-existing records that happened to be stored on a computer. In any event, the government did offer circumstantial evidence that the computer printouts accurately depicted the approval numbers . . . ." (citation omitted)); *see also* Indianapolis Minority Contractions Ass'n, Inc. v. Wiley, No. IP94-1175-C-T-G, 1998 WL 1988826, at *7 (S.D. Ind. May 13, 1998).

Because the authentication methods listed in Rule 901(b) are not exhaustive, many courts have turned to other "outside of the box" methods of authenticating ESI.[133] One of these approaches has been to take judicial notice of specific information or facts relating to ESI.[134] For example, this mechanism could be used to establish commonly known characteristics of computers, how the Internet operates, the calculations performed by various computer programs, or other similar facts.[135]

However, trial courts have split on whether this type of judicial notice is appropriate.[136] Instead of clarifying this issue, appellate decisions have also split, as three circuits have concluded that a trial court committed error by taking judicial notice of facts from a Web site,[137] while two circuits have held

133. *See* Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 552–54 (D. Md. 2007).

134. *See* RICE, *supra* note 9, at 483–89 (discussing how courts apply judicial notice to e-commerce). Under Rule 201, a court may take judicial notice of a fact "not subject to reasonable dispute that is either (1) generally known within the territorial jurisdiction of the trial court or (2) capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned." FED. R. EVID. 201(b). A court *must* take judicial notice of facts "if requested by a party and supplied with the necessary information." FED. R. EVID. 201(d).

135. *See Lorraine*, 241 F.R.D. at 553; *see also* EDWARD J. IMWINKELRIED, EVIDENTIARY FOUNDATIONS 98 (7th ed. 2008) (noting that the proposition that "a person or entity can establish a Web site that other persons can visit" is "so well established that it is judicially noticeable").

136. *Compare* Wible v. Aetna Life Ins. Co., 375 F. Supp. 2d 956, 965–66 (C.D. Cal. 2005) (taking judicial notice of various publications on Amazon.com); Town of Southold v. Town of E. Hampton, 406 F. Supp. 2d 227, 232 n.2 (E.D.N.Y. 2005), *aff'd in part, rev'd in part, and remanded on other grounds*, 477 F.3d 38 (2d Cir. 2007) ("This Court may take judicial notice of the contents of a website assuming, as in this case, its authenticity has not been challenged and 'it is capable of accurate and ready determination.'" (quoting FED. R. EVID. 201)); *In re* Extradition of Gonzalez, 52 F. Supp. 2d 725, 731 n.12 (W.D. La. 1999) (taking judicial notice of mileage based on the MapQuest Web site), *with* Ruiz v. Gap, Inc., 540 F. Supp. 2d 1121, 1124 (N.D. Cal. 2008) (declining to take judicial notice of a study from a Web site); Nw. Bypass Group v. U.S. Army Corps of Eng'rs, 488 F. Supp. 2d 22, 25–26 (D.N.H. 2007) (declining to take judicial notice of the contents of an e-mail); Fenner v. Suthers, 194 F. Supp. 2d 1146, 1148–49 (D. Colo. 2002) (declining to take judicial notice of Web sites, in part, because the court "doubt[ed] that a website can be said to provide an 'accurate' reference, at least in normal circumstances where the information can be modified at will by the web master and, perhaps, others. There is, in other words, the question of whether the defendants, the magistrate judge, the district judge, and any reviewing court are literally on the same page when they visit the site on different dates."); San Luis v. Badgley, 136 F. Supp. 2d 1136, 1146 (E.D. Cal. 2000) (declining to take judicial notice of information from U.S. Bureau of Reclamation Web site); Knight v. Standard Ins. Co., No. CIV. 07-1691 WBS EFB, 2008 WL 343852, at *2 n.2 (E.D. Cal. Feb. 6, 2008) ("Taking judicial notice of facts on a webpage . . . poses heightened concerns because anyone can say anything on a webpage, and the posting of a 'fact' on a webpage does not necessarily make it true. . . . The unregulated content of webpages poses significant hurdles for the court to find that a webpage, or its host or author, is necessarily 'a source whose accuracy cannot reasonably be questioned.'" (quoting FED. R. EVID. 201(b)(2)) (citations omitted)).

137. *See* Victaulic Co. v. Tieman, 499 F.3d 227, 236–37 (3d Cir. 2007) (holding that the district court erred in using a company's Web site to establish facts about that company's business); Baker v. Barnhart, 457 F.3d 882, 891–92 (8th Cir. 2006) (reversing district court because it took judicial notice of facts using a printout of an article from a Web site); Scanlan v. Tex. A&M Univ., 343 F.3d 533, 536–37 (5th Cir. 2003) (noting that it was improper for a trial court to take judicial notice of a report located on a Web site).

that a trial court committed error by *failing* to judicially notice such facts.[138] To further complicate this issue, appellate decisions frequently take judicial notice of facts from the Internet, although typically only from government Web sites.[139]

Modern technology also provides courts with new methods of authenticating ESI. For example, some courts have recognized that metadata provides a "useful tool" that can be used to authenticate ESI under Rule 901(b)(4).[140] This is because metadata often reveals the date and time ESI was created, as well as the identity of its creator and any subsequent changes.[141] However, in light of the potential for manipulation, "this method is not foolproof."[142]

Additionally, courts have used various burden-shifting measures to establish authenticity. One common approach is to find that producing any ESI as part of a discovery request establishes its authenticity.[143] Some courts create a rebuttable presumption of authenticity, stating that unless the opposing party can raise an issue about the authenticity or reliability of the ESI, it will be admitted.[144] Commentators, however, have sharply criticized this approach as

---

138. *See* O'Toole v. Northrop Grumman Corp., 499 F.3d 1218, 1224–25 (10th Cir. 2007) (noting the propriety of taking judicial notice of information found on the Internet and concluding that "the district court abused its discretion by failing to take judicial notice of the actual earnings history provided by Northrop Grumman on the internet"); Denius v. Dunlap, 330 F.3d 919, 926 (7th Cir. 2003) (noting that "the district court abused its discretion in withdrawing its judicial notice of the information from NPRC's official website").

139. *See, e.g.*, Nebraska v. EPA, 331 F.3d 995, 998 & n.3 (D.C. Cir. 2003) (taking judicial notice of information in the EPA's online database); United States v. Bervaldi, 226 F.3d 1256, 1266 n.9 (11th Cir. 2000) (taking judicial notice of a fact from the U.S. Naval Observatory Web site); *see also* Miller v. Vocational Rehab. Workshop, Inc., Civ. Action No. 2:09-39-JFA-RSC, 2009 WL 482349, at *3 n.3 (D.S.C. Feb. 25, 2009) ("The court may take judicial notice of factual information located in postings on government websites.").

140. *See Lorraine*, 241 F.R.D. at 547–48; *see also* Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640, 646 (D. Kan. 2005).

141. *See Lorraine*, 241 F.R.D. at 547–48; *see also supra* notes 39–45 and accompanying text.

142. *Lorraine*, 241 F.R.D. at 548.

143. *See, e.g.*, Orr v. Bank of Am., NT & SA, 285 F.3d 764, 777 n.20 (9th Cir. 2002); Schaghticoke Tribal Nation v. Kempthorne, 587 F. Supp. 2d 389, 397 (D. Conn. 2008); *In re* Homestore.com, Inc. Sec. Litig., 347 F. Supp. 2d 769, 781 (C.D. Cal. 2004) (e-mails); Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1153–54 (C.D. Cal. 2002); Pierre v. RBC Liberty Life Ins., Civ. Action No. 05-1042-C, 2007 WL 2071829, at *2 (M.D. La. July 13, 2007) (e-mails); Sklar v. Clough, Civ. Action No. 1:06-CV-0627, 2007 WL 2049698, at *4 (N.D. Ga. July 6, 2007) ("The e-mails in question were produced by Defendants during the discovery process. Such documents are deemed authentic when offered by a party opponent."); Superhighway Consulting, Inc. v. Techwave, Inc., No. 98 CV 5502, 1999 WL 1044870, at *2 (N.D. Ill. Nov. 16, 1999) (e-mails); Indianapolis Minority Contractors Ass'n, Inc. v. Wiley, No. IP94-1175-C-T-G, 1998 WL 1988826, at *6 (S.D. Ind. May 13, 1998). *But see* Kirby v. Anthem, Inc., No. IP98-0954-C-H/G, 2001 WL 1168166, at *5 (S.D. Ind. Aug. 8, 2001) ("The mere fact of production is not sufficient by itself to establish the authenticity of the document to support its admission into evidence.").

144. *See, e.g.*, Midwest Retailers Ass'n, Ltd. v. City of Toledo, 582 F. Supp. 2d 931, 934–35 (N.D. Ohio 2008); Mortgage Mkt. Guide, L.L.C. v. Freedman Report, L.L.C., No. 06-CV-140, 2008 WL 2991570, at *12 n.3 (D.N.J. July 28, 2008); Telewizja Polska USA, Inc. v. Echostar Satellite Corp., No. 02C3293, 2004 WL 2367740, at *6 (N.D. Ill. Oct. 15, 2004) (Web site).

ignoring both traditional authentication principles and the susceptibility of ESI to hacking.[145]

A related question with ESI is whether, and if so under what circumstances, ESI can be self-authenticating. Similar to authentication generally, a limited number of courts have found that some forms of ESI, such as Web sites, can never be self-authenticating.[146] Other courts, however, have *presumed* that e-mails are self-authenticating.[147] Of the courts that recognize the potential for self-authentication, there is near unanimity that government Web sites are self-authenticating as official publications under Rule 902(5).[148] Beyond that, the requirements for self-authentication vary.[149]

As the preceding analysis indicates, "there is a wide disparity between the most lenient positions courts have taken in accepting electronic records as authentic and the most demanding requirements that have been imposed."[150] Accordingly, litigants remain uncertain about the steps that courts will require them to take to authenticate electronic evidence.[151]

---

145. *See, e.g.*, Eric Van Buskirk & Vincent T. Liu, *Digital Evidence: Challenging the Presumption of Reliability*, 1 J. DIGITAL FORENSIC PRAC. 19 (2006); Paul, *supra* note 9.

146. *See, e.g.*, *In re Homestore.com*, 347 F. Supp. 2d at 782 ("Printouts from a web site do not bear the indicia of reliability demanded for other self-authenticating documents under Fed. R. Evid. 902."); Sun Prot. Factory, Inc. v. Tender Corp., No. 604CV732ORL19KRS, 2005 WL 2484710, at *6 n.4 (M.D. Fla. Oct. 7, 2005) ("[W]ebsites are not self-authenticating." (citing *In re Homestore.com*, 347 F. Supp. 2d at 782)).

147. *See, e.g.*, *Superhighway Consulting, Inc.*, 1999 WL 1044870, at *2 (indicating that e-mails and faxes are self-authenticating under Rule 902(17) unless opposing party can produce evidence disputing their authenticity).

148. *See, e.g.*, Williams v. Long, 585 F. Supp. 2d 679, 689–90 (D. Md. 2008); United States v. 52" Flat Screen Television, No. 1:08-cv-1534-OWW-SMS, 2009 WL 1770134, at *4 (E.D. Cal. June 23, 2009); United States *ex rel.* Parikh v. Premera Blue Cross, No. C01-0476P, 2006 WL 2841998, at *3–4 (W.D. Wash. Sept. 29, 2006) (finding that a government site was self-authenticating, but a printout from an online newspaper was not); Colt Def. L.L.C. v. Bushmaster Firearms, Inc., No. Civ.04-240-P-S, 2005 WL 2293909, at *5 n.10 (D. Me. Sept. 20, 2005) (noting that "printouts from government web sites have been held to be self-authenticating pursuant to Federal Rules of Evidence 901(a) and/or 902(5)"); EEOC v. E.I. DuPont de Nemours & Co., No. Civ.A. 03-1605, 2004 WL 2347559, at *2 (E.D. La. Oct. 18, 2004) (concluding that postings on a Web site of the U.S. Census Bureau were self-authenticating); Hispanic Broad. Corp. v. Educ. Media Found., No. CV027134CAS, 2003 WL 22867633, at *5 n.5 (C.D. Cal. Oct. 30, 2003) (noting that "records from government websites, such as the FCC website, are self-authenticating"); Sannes v. Jeff Wyler Chevrolet, Inc., No. C-1-97-930, 1999 WL 33313134, at *3 n.3 (S.D. Ohio Mar. 31, 1999) ("The FTC press releases, printed from the FTC's government world wide web page, are self-authenticating official publications under Rule 902(5) of the Federal Rules of Evidence.").

149. *Compare* United States v. Safavian, 435 F. Supp. 2d 36, 39 & n.1 (D.D.C. 2006) (stating that a party must produce more than basic information in an affidavit to fall within Rule 902(11)'s provision for the self-authentication of certified domestic records of regularly conducted activity), *with* DirecTV, Inc. v. Murray, 307 F. Supp. 2d 764, 772 (D.S.C. 2004) (affidavit with basic information sufficient for Rule 902(11)). This self-authentication provision is closely related to the business records exception to the hearsay rules. *See, e.g.*, Lorraine v. Markel Amer. Ins. Co., 241 F.R.D. 534, 552 (D. Md. 2007) (drawing parallel between 902(11) and hearsay analysis under 803(6)); *see also infra* note 185.

150. *Lorraine*, 241 F.R.D. at 558; *see* Finkelstein & Storch, *supra* note 123, at 14.

151. *See Lorraine*, 241 F.R.D. at 559.

B. Hearsay

1. *General Hearsay Rules*

The Federal Rules of Evidence generally prohibit a party from introducing evidence containing hearsay.[152] Rule 801 defines hearsay as "a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted."[153] A statement is defined as "(1) an oral or written assertion or (2) nonverbal conduct of a person, if it is intended by the person as an assertion."[154] The Rules exclude, in limited circumstances, prior statements by a witness and a party opponent's admission from the definition of hearsay.[155] Rule 803 also provides twenty-three separate exceptions to the hearsay rules.[156] Basically, these exceptions provide for the admission of hearsay in circumstances where the statement has indications of trustworthiness.[157]

The hearsay rules seek to promote the policy goal of ensuring the reliability and trustworthiness of evidence.[158] Accordingly, these rules generally exclude hearsay because an out-of-court declarant is not subject to the reliability safeguards present with in-court testimony.[159] Specifically, an out-of-court declarant is not speaking under oath while making the statement.[160] The opposing party is also unable to test potential weaknesses in the declarant's statement through cross-examination, the "greatest legal engine ever invented for the discovery of truth."[161] Further, by generally requiring a declarant's

---

152. FED. R. EVID. 802 ("Hearsay is not admissible except as provided by these rules or by other rules prescribed by the Supreme Court pursuant to statutory authority or by Act of Congress.").

153. FED. R. EVID. 801(c).

154. FED. R. EVID. 801(a).

155. *See* FED. R. EVID. 801(d).

156. *See* FED. R. EVID. 803. In criminal cases, however, hearsay may be admissible pursuant to an exception, yet be excluded under the Confrontation Clause of the Sixth Amendment. *See generally* Crawford v. Washington, 541 U.S. 36 (2004) (outlining the history of the Confrontation Clause and how it interacts with the hearsay rules in criminal cases).

157. *See, e.g.*, RICE, *supra* note 9, at 409; 5 JOHN HENRY WIGMORE, EVIDENCE IN TRIALS AT COMMON LAW § 1420, at 251–52 (James H. Chadbourn rev. 1974). There is also a catchall residual exception provided for in Rule 807. *See* FED. R. EVID. 807.

158. *See, e.g.*, RICE, *supra* note 9, at 403. For a complete discussion of the rationales supporting the hearsay rules, as well as their historical origins, see generally Edmund M. Morgan, *Hearsay Dangers and the Application of the Hearsay Concept*, 62 HARV. L. REV. 177 (1948).

159. *See, e.g.*, Roger Park, *A Subject Matter Approach to Hearsay Reform*, 86 MICH. L. REV. 51, 55–56 (1987).

160. *See, e.g.*, Ellicott v. Pearl, 35 U.S. (10 Pet.) 412, 436 (1836) (noting that the exclusion of hearsay is justified, in part, because of "the general consideration that it is not upon oath"); 2 DIX ET AL., *supra* note 2, § 245, at 125–26; 5 WIGMORE, *supra* note 157, § 1420, at 7–10.

161. California v. Green, 399 U.S. 149, 158 (1970) (quoting 5 JOHN HENRY WIGMORE, A TREATISE ON THE ANGLO-AMERICAN SYSTEM OF EVIDENCE IN TRIALS AT COMMON LAW § 1367 (3d ed. 1940)); *see also Ellicott*, 35 U.S. (10 Pet.) at 436 (noting that the exclusion of hearsay is justified, in part, because "the party affected by it has no opportunity of cross-examination"); 2 DIX ET AL., *supra* note 2, § 245, at 126 ("The lack of any opportunity for the adversary to cross-examine the absent declarant whose out-of-court statement is reported is today accepted as the main justification for the exclusion of hearsay."); Park, *supra* note 159, at 55–56 (noting that

personal presence at trial, the fact finder has the opportunity to observe the declarant's demeanor for purposes of evaluating credibility.[162] Thus, these concerns, along with a general fear of potential fabrication or fraud, justify the hearsay rules.[163]

It is important to note that a significant amount of ESI does not fall within the definition of hearsay. Hearsay requires a "statement," which must be made by a "declarant."[164] Because the rules define a declarant as a "*person* who makes a statement,"[165] many courts conclude that an electronically generated record that is solely the creation of a computerized system or process is not hearsay.[166] As a result, any information automatically generated by a computer, including metadata, does not fall within these rules.[167] For example, one court concluded that header information accompanying an electronic image, which a computer automatically generated when the defendant uploaded the image to the Internet, was not subject to the hearsay rules.[168] Information created by a person using a computer, however, such as an e-mail, remains a "statement" and subject to the requirements of the hearsay rules.[169] Notably,

---

"hearsay's fundamental evidentiary flaw is the absence of an opportunity to reveal an out-of-court declarant's weaknesses through cross-examination").

162. *See, e.g.*, 2 DIX ET AL., *supra* note 2, § 245, at 126. Personal presence also "eliminates the danger that the witness reporting the out-of-court statement may do so inaccurately." *Id.*

163. *See, e.g.*, *Ellicott*, 35 U.S. (10 Pet.) at 436 (noting that hearsay is "peculiarly liable to be obtained by fraudulent contrivances"); Queen v. Hepburn, 11 U.S. (7 Cranch) 290, 295–96 (1813) (Marshall, C.J.) (noting the "frauds which might be practiced" under the cover of hearsay); Park, *supra* note 159, at 56–57.

164. FED. R. EVID. 801.

165. FED. R. EVID. 801(b) (emphasis added).

166. *See, e.g.*, United States v. Lamons, 532 F.3d 1251, 1263–64 (11th Cir. 2008) (finding that evidence was not hearsay because "the statements in question are the statements of machines"); United States v. Washington, 498 F.3d 225, 231 (4th Cir. 2007) ("Only a *person* may be a declarant and make a statement. Accordingly, 'nothing "said" by a machine . . . is hearsay.'" (quoting 4 CHRISTOPHER B. MUELLER & LAIRD C. KIRKPATRICK, FEDERAL EVIDENCE § 380, at 65 (2d ed. 1994))); United States v. Khorozian, 333 F.3d 498, 505 (3d Cir. 2003); Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 564 (D. Md. 2007).

167. *See* RICE, *supra* note 9, at 417 ("Although mechanical devices, such as computers, can record hearsay statements from other sources, such as business records and third-party statements, such devices do not create an additional hearsay link."); RIEDY ET AL., *supra* note 12, at 201 ("There is substantial authority for the proposition that information that is neither created nor maintained by a human—or computer-generated records—should not be considered hearsay."); 5 WEINSTEIN & BERGER, *supra* note 88, § 900.07(1)(a) ("Computer-generated data, which includes metadata, automated teller machine transactions, and direct-dialed telephone calls, are extrajudicial statements that are not hearsay."); Burns et al., *supra* note 52, at 224 (noting that "the hearsay rule . . . does not apply to many types of electronic evidence").

168. *See* United States v. Hamilton, 413 F.3d 1138, 1142–43 (10th Cir. 2005).

169. *See, e.g.*, *Hamilton*, 413 F.3d at 1142 n.4 (noting the distinction, for purposes of the hearsay rule, between information that is computer-generated and information that is merely stored electronically using a computer); Means v. Cullen, 297 F. Supp. 2d 1148, 1151–52 (W.D. Wis. 2003) (noting that none of the hearsay exceptions applied and thus "the truth of the matter asserted in the e-mail is hearsay and cannot be considered"); Nokes v. U.S. Coast Guard, 282 F. Supp. 2d 1085, 1089 (D. Minn. 2003) ("[A]s an out of court statement offered as proof of the matter it asserts, the e-mail is inadmissible hearsay.").

like all hearsay, this information may still fall within the non-hearsay provisions of Rule 801(d).[170]

When the rules apply, however, electronically stored information poses several potential hearsay issues. Some ESI evidence, such as e-mails, e-mail chains, and Internet service provider logs, raises issues regarding how such evidence fits within the various exceptions contained in Rule 803.[171] Further, ESI may present multiple levels of hearsay, such as when an e-mail contains information that the sender received from another source.[172] Overall, though, "[t]he application of the hearsay rule to electronic evidence does not differ from its application to all other forms of evidence," but the rules are "made more difficult to apply because of the new context."[173]

2. *ESI, Hearsay, and the Rule 803 Exceptions*

Courts have taken a wide variety of approaches when addressing the hearsay issues presented by electronically stored information. Similar to how courts address the authentication of ESI, two schools of thought exist. One approach has been to recognize how commonplace electronic information is and to liberally interpret the hearsay rules to ensure its admissibility.[174] In

---

170. *See, e.g.*, Schaghticoke Tribal Nation v. Kempthorne, 587 F. Supp. 2d 389, 398 (D. Conn. 2008) (concluding that e-mails were admissions of party-opponents and therefore excluded from the definition of hearsay under Rule 801(d)(2)(D)); United States v. Safavian, 435 F. Supp. 2d 36, 43 (D.D.C. 2006) ("The context and content of certain e-mails demonstrate clearly that [the defendant] 'manifested an adoption or belief' in the truth of the statements of other people as he forwarded their e-mails. They therefore are admissible as adoptive admissions under Rule 801(d)(2)(B)." (citation omitted)); X17, Inc. v. Lavandeira, No. CV06-7608-VBF(JCX), 2007 WL 790061, at *3 (C.D. Cal. Mar. 8, 2007); Bouriez v. Carnegie Mellon Univ., No. Civ.A. 02-2104, 2005 WL 2106582, at *9 (W.D. Pa. Aug. 26, 2005). *Accord* United States v. Dupre, 462 F.3d 131, 136–37 (2d Cir. 2006); Sea-Land Serv., Inc. v. Lozen Int'l, L.L.C., 285 F.3d 808, 821 (9th Cir. 2002).

171. *See Lorraine*, 241 F.R.D. at 562 ("Hearsay issues are pervasive when electronically stored and generated evidence is introduced.").

172. *See, e.g.*, ARKFELD, *supra* note 1, § 8.13(C)(4)(a); RICE, *supra* note 9, at 403. For example, "e-mail strings" or "chains" are "[a] series of e-mails linked together by e-mail responses or forwards. The series of email messages created through multiple responses and answers to an originating message." SEDONA CONFERENCE GLOSSARY, *supra* note 12, at 19. When confronted with such evidence containing multiple levels of hearsay, each level must satisfy a hearsay exception in order for that level to be admissible. *See* FED. R. EVID. 805 ("Hearsay included within hearsay is not excluded under the hearsay rule if each part of the combined statements conforms with an exception to the hearsay rule provided in these rules.").

173. RICE, *supra* note 9, at 403.

174. *See, e.g.*, Border Collie Rescue, Inc. v. Ryan, 418 F. Supp. 2d 1330, 1350 n.16 (M.D. Fla. 2006) ("Even though [the parties] authenticate the website printouts, they do not establish that the website printouts are nonhearsay, plaintiffs' business records, or subject to some other hearsay exception. The Court nevertheless considered the website for purposes of summary judgment as it deems this evidence the type that can be reduced to admissible form at trial."); Microware Sys. Corp. v. Apple Computer, Inc., 126 F. Supp. 2d 1207, 1211 n.2 (S.D. Iowa 2000) ("As to the internet and e-mail postings, . . . the Court recognizes Apple's hearsay concerns, but will receive the evidence in any case. . . . [I]n a case involving an industry where e-mail and internet communication are a fact of life, these technical deficiencies must go to the weight of such evidence, rather than to their admissibility."); Van Westrienen v. Americontinental Collection Corp., 94 F. Supp. 2d 1087, 1109 (D. Or. 2000) (holding that content of a Web site was not hearsay when a

contrast, another approach has been to remain skeptical of new sources of information and the potential for fraud or manipulation and, therefore, strictly apply the hearsay rules to severely restrict the admissibility of ESI.[175]

Generally, courts follow a more traditional analysis when applying most of the hearsay exceptions in Rule 803 to ESI.[176] For example, courts examine the same factors when determining whether a statement in an e-mail constitutes a present sense impression.[177] Similar trends exist for the exception for statements of a declarant's then-existing mental, emotional, or physical condition.[178]

One hearsay exception that has not been applied consistently to ESI is the business records exception.[179] This exception states that the hearsay rule does not exclude various forms of business records if they meet several elements.[180] First, the records must be "made at or near the time by, or from information transmitted by, a person with knowledge."[181] Second, the records must be "kept in the course of a regularly conducted activity."[182] Finally, it must be part of the business's regular activity to make the record.[183] The basis for this exception is that a business is motivated to ensure that its regularly kept re-

---

witness testifies as to what he or she viewed); *In re* Dow Corning Corp., 250 B.R. 298, 318 (Bankr. E.D. Mich. 2000) ("There is nothing in the record to suggest that these computer-generated reports are untrustworthy."); *see also* United States v. Moore, 923 F.2d 910, 915 (1st Cir. 1991) (noting that the elements of the business records exception are sufficient to indicate the trustworthiness of computer records, absent counsel's ability to point to specific evidence of untrustworthiness); V Cable, Inc. v. Budnick, 23 F. App'x 64, 65–66 (2d Cir. 2001) (finding no error in the admission of computer printouts over defendant's hearsay objection, despite a break in the chain of custody, because there were other indications of trustworthiness).

175. *See, e.g.*, United States v. Jackson, 208 F.3d 633, 637 (7th Cir. 2000); Tolliver v. Fed. Republic of Nig., 265 F. Supp. 2d 873, 876 (W.D. Mich. 2003); St. Clair v. Johnny's Oyster & Shrimp, Inc., 76 F. Supp. 2d 773, 775 (S.D. Tex. 1999) (noting that "any evidence procured off the Internet is adequate for almost nothing, even under the most liberal interpretation of the hearsay exception rules").

176. *See, e.g.*, H. Christopher Boehning & Daniel J. Toal, *Electronic Discovery: Overcoming Evidentiary Hurdles*, N.Y. L.J., Oct. 23, 2007, at 5 ("Many of the exceptions [to the hearsay rules] are applied to ESI in a wholly conventional manner.").

177. *See* FED. R. EVID. 803(1); United States v. Ferber, 966 F. Supp. 90, 99 (D. Mass. 1997); Canatxx Gas Storage Ltd. v. Silverhawk Capital Partners, L.L.C., Civ. Action No. H-06-1330, 2008 WL 1999234, at *13–14 (S.D. Tex. May 8, 2008); New York v. Microsoft Corp., No. CIV A.98-1233, 2002 WL 649951, at *2 (D.D.C. Apr. 12, 2002).

178. *See* FED. R. EVID. 803(3); McInnis v. Fairfield Communities, Inc., 458 F.3d 1129, 1143–44 (10th Cir. 2006); United States v. Safavian, 435 F. Supp. 2d 36, 44 (D.D.C. 2006); Tibbetts v. RadioShack Corp., No. 03 C 2249, 2004 WL 2203418, at *13 (N.D. Ill. Sept. 29, 2004).

179. *See* FED. R. EVID. 803(6); Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 572 (D. Md. 2007); Burns et al., *supra* note 52, at 225 (noting that the business records exception is the most commonly litigated hearsay exception for electronic evidence that contains hearsay).

180. *See* FED. R. EVID. 803(6).

181. *Id.*

182. *Id.*

183. *Id.*

cords are accurate and precise.[184] The exception is also tied to the method of self-authentication in Rule 902(11).[185]

Most courts agree that electronically stored information qualifies for the business records exception.[186] Indeed, the Advisory Committee noted that "[t]he form which the 'record' may assume under the rule is described broadly" and "includes, but is by no means limited to, electronic computer storage."[187] However, as one court observed, decisions applying the business records exception to ESI "demonstrate a continuum running from cases where the court was very lenient in admitting electronic business records, without demanding analysis, to those in which the court took a very demanding approach and scrupulously analyzed every element of the exception."[188]

These differences are similar to the differences in how courts view ESI for purposes of authentication.[189] Some courts emphasize the potential for the altering of electronic records and require an enhanced showing to ensure that proffered evidence is identical to the original document.[190] Many courts, however, have a significantly less stringent standard for computerized business records.[191] Indeed, as one court noted, "[t]he existence of an air-tight security system is not . . . a prerequisite to the admissibility of computer printouts."[192]

---

184. *See, e.g.*, 2 DIX ET AL., *supra* note 2, § 286, at 304.

185. *See* FED. R. EVID. 902(11) (stating that extrinsic evidence of authenticity is not required for "[t]he original or a duplicate of a domestic record of a regularly conducted activity that would be admissible under Rule 803(6) if accompanied by a written declaration of its custodian or other qualified person"); *see also* Rambus, Inc. v. Infineon Techs. AG, 348 F. Supp. 2d 698, 701 (E.D. Va. 2004) ("Rules 803(6) and 902(11) go hand in hand.").

186. *See, e.g.*, DAVID F. BINDER, HEARSAY HANDBOOK § 16:5 (4th ed. 2001); RIEDY ET AL., *supra* note 12, at 199 (noting that "with an appropriate foundation, computer printouts qualify as business records"); *see also* United States v. Hutson, 821 F.2d 1015, 1019 (5th Cir. 1987) ("Computer records are admissible if the requirements of Rule 803(6) have been met." (citing United States v. Young Brothers Inc., 728 F.2d 682, 693 (5th Cir. 1984), *cert. denied* 469 U.S. 881 (1984))); United States v. Croft, 750 F.2d 1354, 1364 (7th Cir. 1984) ("It is well-settled that computer data compilations may constitute business records for purposes of Fed. R. Evid. 803(6) and may be admitted at trial if a proper foundation is established.").

187. FED. R. EVID. 803 advisory committee's note ("The form which the 'record' may assume under the rule is described broadly as a 'memorandum, report, record, or data compilation, in any form.' The expression 'data compilation' is used as broadly descriptive of any means of storing information other than the conventional words and figures in written or documentary form. It includes, but is by no means limited to, electronic computer storage.").

188. Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 572 (D. Md. 2007).

189. *See supra* Part II.A.2.

190. Am. Express Travel Related Servs. Co. v. Vee Vinhnee (*In re* Vee Vinhnee), 336 B.R. 437, 444 (B.A.P. 9th Cir. 2005); *see also Lorraine*, 241 F.R.D. at 573 (describing this case as "[p]erhaps the most demanding analysis regarding the admissibility of electronic evidence under the business record exception to the hearsay rule").

191. *See, e.g.*, United States v. Fujii, 301 F.3d 535, 539 (7th Cir. 2002); Sea-Land Serv., Inc. v. Lozen Int'l, L.L.C., 285 F.3d 808, 819–20 (9th Cir. 2002); United States v. Salgado, 250 F.3d 438, 451–53 (6th Cir. 2001); United States v. Kassimu, 188 F. App'x 264, 264 (5th Cir. 2006); McAninch v. Fed. Express Corp., 398 F. Supp. 2d 1025, 1036 (S.D. Iowa 2005); *see also* 2 DIX ET AL., *supra* note 2, § 294, at 325 (noting that "the trend among courts has been to treat computer records like other business records and not to require the proponent of the evidence initially to show trustworthiness beyond the general requirements of the rule").

192. United States v. Glasser, 773 F.2d 1553, 1559 (11th Cir. 1985).

Courts also differ about how the exception should apply to e-mails. Many, if not most, courts impose stringent requirements for e-mail to qualify under the business records exception.[193] For example, some courts require a proponent of e-mail evidence to prove not only that it was the business's routine practice to send that type of e-mail, but also that the business had policies *requiring* the preservation of those types of e-mails.[194] In contrast, other courts have held that the sending of an e-mail in the regular course of business is sufficient.[195] Similar differences exist over how the exception applies to e-mail chains.[196] Accordingly, "[t]he lesson to be taken from these cases is that some courts will require the proponent of electronic business records or e-mail evidence to make an enhanced showing in addition to meeting each element of the business records exception."[197]

C. Best Evidence Rule

1. *The Best Evidence Rule Generally*

Another barrier to the admissibility of evidence is the best evidence rule.[198] Generally, the best evidence rule, also known as the original writing

193. *See* RIEDY ET AL., *supra* note 12, at 197.

194. *See, e.g.*, Schaghticoke Tribal Nation v. Kempthorne, 587 F. Supp. 2d 389, 397–98 (D. Conn. 2008); United States v. Ferber, 966 F. Supp. 90, 98–99 (D. Mass. 1997); Westfed Holdings, Inc. v. United States, 55 Fed. Cl. 544, 565–66 (2003), *aff'd in part and rev'd in part*, 407 F.3d 1352 (Fed. Cir. 2005); *In re* Hechinger Inv. Co. of Del., Inc., 298 B.R. 240, 242–43 (Bankr. D. Del. 2003); Canatxx Gas Storage Ltd. v. Silverhawk Capital Partners, L.L.C., Civ. Action No. H-06-1330, 2008 WL 1999234, at *12 (S.D. Tex. May 8, 2008); *see also* Monotype Corp. P.L.C. v. Int'l Typeface Corp., 43 F.3d 443, 450 (9th Cir. 1994) (excluding an e-mail under Rule 803(6) because "[e]-mail is far less of a systematic business activity than a monthly inventory printout. E-mail is an ongoing electronic message and retrieval system whereas an electronic inventory recording system is a regular, systematic function of a bookkeeper prepared in the course of business.").

195. *See, e.g.*, DirecTV, Inc. v. Murray, 307 F. Supp. 2d 764, 772–73 (D.S.C. 2004); Pierre v. RBC Liberty Life Ins., Civ. Action No. 05-1042-C, 2007 WL 2071829, at *2 (M.D. La. July 13, 2007); *see also* Tibbetts v. RadioShack Corp., No. 03 C 2249, 2004 WL 2203418, at *15 (N.D. Ill. Sept. 29, 2004) (report, in form of an attachment to e-mail, was made in ordinary course of business, even though it was not signed and lacked the "footer" normally included in such reports).

196. *Compare* United States v. Safavian, 435 F. Supp. 2d 36, 41 (D.D.C. 2006) ("The defendant is free to raise [the issue of alteration] with the jury and put on evidence that e-mails are capable of being altered before they are passed on. Absent specific evidence showing alteration, however, the Court will not exclude any embedded e-mails because of the mere possibility that it can be done."), *with* Rambus Inc. v. Infineon Tech. AG, 348 F. Supp. 2d 698, 706–07 (E.D. Va. 2004) (concluding that unless each element of the business records exception is satisfied for all statements made in the e-mail chain, the e-mail lacks trustworthiness and the exception will not apply), *and* New York v. Microsoft Corp., No. CIV A.98-1233, 2002 WL 649951, at *5 (D.D.C. Apr. 12, 2002) (similar holding to *Rambus Inc.*).

197. Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 574 (D. Md. 2007).

198. The nomenclature "best evidence rule" may be somewhat of a misnomer, in part because it does not require a party to produce the best available evidence. *See Lorraine*, 241 F.R.D. at 576 n.54. Further, the principle is outlined in the Federal Rules of Evidence as a series of rules, rather than a single "best evidence rule." *See* FED. R. EVID. 1001–08. For a discussion of the historical origins of the rule, see generally Edward W. Cleary & John W. Strong, *The Best Evidence Rule: An Evaluation in Context*, 51 IOWA L. REV. 825 (1966).

rule,[199] states that "[t]o prove the content of a writing, recording, or photograph, the original writing, recording, or photograph is required."[200] Because of the broad definition of "writing" and "recording," this requirement clearly applies to electronic evidence.[201]

Unlike other admissibility requirements, the definition of "original" in the federal rules explicitly addresses computer-generated evidence, stating that if "data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original.'"[202] In other words, the physical medium in which ESI is stored, such as a hard drive, does not need to be admitted into evidence.[203] Instead, a printout of that information constitutes an "original" and satisfies the best evidence rule.[204]

If an original is lost or destroyed, a party has several options. First, a duplicate[205] is admissible to the same extent as an original, "unless (1) a genuine question is raised as to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original."[206] Further, an original is not required if the original is lost or destroyed, not obtainable, in the possession of a party opponent, or if it relates to a collateral matter.[207] If any of these circumstances exist, all forms of secondary evidence[208] are admissible to prove the contents of the writing.[209]

There are several justifications for the best evidence rule. One rationale espoused by courts and commentators is the prevention of fraud.[210] Another

---

199. *See* FED. R. EVID. 1001 advisory committee's note.

200. FED. R. EVID. 1002.

201. *See* FED. R. EVID. 1001(1) ("'Writings' and 'recordings' consist of letters, words, or numbers, or their equivalent, set down by handwriting, typewriting, printing, photostating, photographing, magnetic impulse, mechanical or electronic recording, or other form of data compilation."); *see also id.* advisory committee's note (stating that "the considerations underlying the rule dictate its expansion to include computers, photographic systems, and other modern developments").

202. FED. R. EVID. 1001(3); *see also* DirecTV v. Reyes, No. 03 C 8056, 2006 WL 533364, at *7 (N.D. Ill. Mar. 1, 2006) ("A computer printout of information stored on a computer is an 'original' for purposes of FED. R. EVID. 1001(3) and 1002."). Accordingly, there are fewer reported decisions addressing how the rule applies to ESI. *See* Burns et al., *supra* note 52, at 226.

203. *See, e.g.*, RICE, *supra* note 9, at 303–04.

204. *See* FED. R. EVID. 1001(3); 2 DIX ET AL., *supra* note 2, § 235, at 97–98; RICE, *supra* note 9, at 303–04.

205. FED. R. EVID. 1001(4) ("A 'duplicate' is a counterpart produced by the same impression as the original, or from the same matrix, or by means of photography, including enlargements and miniatures, or by mechanical or electronic re-recording, or by chemical reproduction, or by other equivalent techniques which accurately reproduces the original.").

206. FED. R. EVID. 1003.

207. *See* FED. R. EVID. 1004.

208. This term derives from the use of the phrase "other evidence" in Rule 1004. *See* 5 MUELLER & KIRKPATRICK, *supra* note 84, § 10:26. Secondary evidence can include a copy of a lost writing or testimony as to its contents. *See id.*; *see also* Wiley v. United States, 257 F.2d 900, 909 (8th Cir. 1958) ("Secondary evidence of a document may consist of a copy proved to be correct, or, when the absence of the primary evidence is satisfactorily accounted for, oral evidence of the contents by one who has seen it and knows its contents.").

209. *See* FED. R. EVID. 1004.

210. *See, e.g.*, United States v. Reyburn, 31 U.S. (6 Pet.) 352, 367 (1832); Renner v. Bank of Columbia, 22 U.S. (9 Wheat.) 581, 596–97 (1824); United States v. Holton, 116 F.3d 1536, 1545

premise for the rule is simply the law's preference for the written word over oral testimony.[211] Essentially, this rationale revolves around a desire for accuracy and precision.[212] Finally, the rule also is concerned about completeness, or potential "internal evidence" that is present in the original but not contained in a copy.[213] As Wigmore stated when explaining this rationale, "the original may contain, and the copy will lack, such features . . . as may afford the opponent valuable means of learning legitimate objections to the significance of the document."[214]

ESI presents several unique best evidence issues. Because every printout is an "original," a party could cut and paste information from a Web site into a word processor and print it for use in court, and theoretically this would satisfy the best evidence rule.[215] Among other problems, this "original" may lack the potentially useful metadata contained in an electronic version.[216] For these reasons, ESI poses many challenges to the application of the best evidence rule.

2. *ESI and the Applicability of the Best Evidence Rule*

Several differences have arisen in how courts apply the best evidence rule to ESI. First, courts differ on whether electronic modifications to ESI constitute violations of the rule. Some courts hold that the best evidence rule precludes the admission of ESI if there are electronic modifications.[217] The major-

---

(D.C. Cir. 1997); United States v. Howard, 953 F.2d 610, 613 (11th Cir. 1992); United States v. Yamin, 868 F.2d 130, 134 (5th Cir. 1989); 2 DIX ET AL., *supra* note 2, § 232, at 88–89; 1 SIMON GREENLEAF, A TREATISE ON THE LAW OF EVIDENCE § 82, at 93 (2d prtg. 1972). This was the predominant rationale provided by commentators in the eighteenth and nineteenth centuries, but has played a lesser role in modern commentary. *See* Cleary & Strong, *supra* note 198, at 827. Wigmore sharply critiqued this rationale. *See* 4 JOHN HENRY WIGMORE, EVIDENCE IN TRIALS AT COMMON LAW § 1180 (James H. Chadbourn rev. 1972).

211. *See, e.g.*, Seiler v. Lucasfilm, Ltd., 808 F.2d 1316, 1319 (9th Cir. 1986); 2 DIX ET AL., *supra* note 2, § 232, at 88; Cleary & Strong, *supra* note 198, at 828.

212. *See* Cleary & Strong, *supra* note 198, at 828.

213. *See* 2 DIX ET AL., *supra* note 2, § 232, at 88–89; Cleary & Strong, *supra* note 198, at 829–30 (stating that "something of value may be gained from a physical inspection of the original by someone . . . which cannot be had from any copy, however produced"); *see also* Gordon v. United States, 344 U.S. 414, 421 (1953) ("The elementary wisdom of the best evidence rule rests on the fact that the document is a more reliable, complete and accurate source of information as to its contents and meaning than anyone's description . . . .").

214. 4 WIGMORE, *supra* note 210, § 1179, at 417.

215. *See* RICE, *supra* note 9, at 304; *see also* Porter v. United States, No. 08-CV-1497 (CPS), 2008 WL 5451011, at *4 (E.D.N.Y. Dec. 31, 2008) (finding that a printout of a cut-and-pasted transcript of an Internet instant messenger conversation satisfied the best evidence rule). *See generally* Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1155 & n.4 (C.D. Cal. 2002) (stating that computer printouts satisfy the best evidence rule).

216. *See* ARKFELD, *supra* note 1, § 8.12(D).

217. *See, e.g.*, United States v. Jackson, 488 F. Supp. 2d 866, 870–71 (D. Neb. 2007) (excluding logs of chat room conversations when the government attempted to introduce a modified "cut and paste" version instead of the original computer file); *see also In re* Gulph Woods Corp., 82 B.R. 373, 377 (Bankr. E.D. Pa. 1988) ("[A] computerized record may be admitted into evidence as an 'original' only after the court has made a fact-specific determination as to the intent of the drafters and the accuracy of the documents.").

ity of courts, however, hold that modified ESI remains an original and that the best evidence rule, therefore, does not apply.[218] One court held in this manner even though the conversion of an electronic file to a different format resulted in the loss of metadata that could have been useful to the opposing party in subsequent proceedings.[219]

The admissibility of secondary evidence also presents problems in connection with ESI. Indeed, in light of the numerous ways that ESI can be destroyed, secondary evidence is often admissible.[220] Courts also adapt their interpretation of the rule providing for the admissibility of secondary evidence, Rule 1004, to accommodate modern technology. For example, one court held that the plaintiff could testify about the content of an e-mail because it had been forwarded to the defendant, causing it to be in the defendant's possession as required by Rule 1004.[221] Other courts have used burden-shifting measures to require the opposing party to prove that the use of secondary evidence is improper.[222] Some courts, however, have been more hesitant to allow secondary evidence when a party attempts to introduce ESI and have readily excluded it.[223] These differences illustrate the division that currently exists as to the proper application of the best evidence rule to ESI.

III. AMENDING THE FEDERAL RULES OF EVIDENCE TO ADDRESS ESI

As the previous sections indicate, whether ESI will be admissible and, if it is, the procedural mechanisms for ensuring its admission, vary significantly from court to court. Generally, these varying standards reflect the theoretical differences in how courts approach ESI. Some courts, such as the *St. Clair*[224] court, are inherently skeptical of ESI evidence and, therefore, strictly apply the

218. *See, e.g.*, United States v. Seifert, 351 F. Supp. 2d 926, 927–28 (D. Minn. 2005) (holding that an electronic video was admissible even though it had been enhanced and edited); United States v. Sattar, No. 02 CR 395(JGK), 2003 WL 22510435, at *1–2 (S.D.N.Y. Nov. 5, 2003) (approving the production of ESI in a different file format).

219. *See Sattar*, 2003 WL 22510435, at *1–2 (concluding that the production of ESI in an altered format was acceptable, even if that meant that metadata was no longer present).

220. *See* Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 580 (D. Md. 2007); *Porter*, 2008 WL 5451011, at *4.

221. *See* King v. Kirkland's Stores, Inc., No. 2:04-cv-1055, 2006 WL 2239203, at *4–5 (M.D. Ala. Aug. 4, 2006) (plaintiff allowed to testify as to the content of an e-mail because the e-mail was forwarded to the defendant and therefore allegedly in defendant's possession).

222. *See* United States v. Culberson, No. 05-80972, 2007 WL 1266131, at *2–4 (E.D. Mich. Apr. 27, 2007) (placing the burden on the defendant to prove that the original e-mails were not available and thus that a transcript was inadmissible); *see also* Pfeffer v. Hilton Grand Vacations Co., L.L.C., No. CV. 07-00492 DAE-BAK, 2009 WL 37519, at *7 (D. Haw. Jan. 7, 2009) (rejecting a party's best evidence rule objection and concluding that anomalies in an e-mail were "not sufficient to make the e-mail so inherently untrustworthy that it should be disregarded").

223. *See, e.g.*, United States v. Bennett, 363 F.3d 947, 953–54 (9th Cir. 2004) (concluding that a police officer's testimony about GPS data violated best evidence rule).

224. St. Clair v. Johnny's Oyster & Shrimp, Inc., 76 F. Supp. 2d 773 (S.D. Tex. 1999).

Federal Rules of Evidence.[225] Others more liberally interpret the rules and adapt them to the unique characteristics of ESI.[226]

In light of these differences, amendments to the rules would provide more guidance to courts and result in a more uniform approach to the admissibility of ESI, reducing the judge-dependent nature of how the rules are currently applied. These amendments should also be coupled with increased training and educational programs for federal judges to create additional consistency and predictability.[227] Overall, while the e-discovery amendments to the Federal Rules of Civil Procedure began to address the problems caused by ESI before trial, it is time to amend the Federal Rules of Evidence to address the unique evidentiary issues presented by ESI at trial.

A. Are Amendments Necessary?

Initially, it is important to consider whether amendments to the Federal Rules of Evidence are the appropriate mechanism to address these concerns. After all, decisions regarding the admissibility of evidence have traditionally been left to the discretion of the trial court.[228] As a result, the current Federal Rules of Evidence are flexible enough to accommodate the changes brought by ESI,[229] particularly because Rule 102 instructs courts to construe the rules to "promote the growth and development of the law of evidence."[230] This discretion is especially appropriate in the context of ESI, as rapid technological changes consistently create new challenges that require case-by-case

225. *See* 5 MUELLER & KIRKPATRICK, *supra* note 84, § 9:9.

226. *See id.*

227. *See* Fred Galves, *Where the Not-So-Wild Things Are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance*, 13 HARV. J.L. & TECH. 161, 277–78 (2000) (discussing how consistency and predictability would improve if federal judges received additional training about computer-generated evidence).

228. *See, e.g.*, RICE, *supra* note 9, at 492; David P. Leonard, *Power and Responsibility in Evidence Law*, 63 S. CAL. L. REV. 937, 956–57 (1990) (noting that "rulemakers have recognized the unique position of the trial judge, who observes the context in which particular evidentiary issues arise and who is therefore in the best position to weigh the potential benefits and harms accompanying the admission of particular evidence"); Thomas M. Mengler, *The Theory of Discretion in the Federal Rules of Evidence*, 74 IOWA L. REV. 413, 458 (1989) (noting that "the Advisory Committee intended to give trial courts the maneuverability to craft its rulings to do individual justice"). *See generally* Jon R. Waltz, *Judicial Discretion in the Admission of Evidence under the Federal Rules of Evidence*, 79 NW. U. L. REV. 1097 (1984).

229. *See* Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 538 n.5 (D. Md. 2007); MANUAL FOR COMPLEX LITIGATION, *supra* note 3, § 11.446; Robins, *supra* note 27, at 315; *see also* James E. Carbine & Lynn McLain, *Proposed Model Rules Governing the Admissibility of Computer-Generated Evidence*, 15 SANTA CLARA COMPUTER & HIGH TECH. L.J. 1, 8 (1999) (noting that "[l]awyers and judges have easily adapted the rules of evidence and procedure" to computerized records).

230. FED. R. EVID. 102 ("These rules shall be construed to secure fairness in administration, elimination of unjustifiable expense and delay, and promotion of growth and development of the law of evidence to the end that the truth may be ascertained and proceedings justly determined.").

evaluation.[231] Further, there is no guarantee that textual amendments will necessarily create the desired national uniformity.[232]

However, the flexibility of the rules to adapt and address the challenges of ESI does not necessarily mean that amendments are not needed. Even with this flexibility, some of the changes wrought by technology have no common law analog, making it difficult for judges to resolve them.[233] Additionally, the current rules are premised on the concept of written, physical evidence, a concept that technological changes have significantly altered in the new millennium.[234] These changes necessitate the reconsideration of the traditional rules of evidence.[235]

Accomplishing these changes through the amendment process would provide a stronger mechanism for providing uniformity than relying upon appellate courts. On appeal, courts are constrained by the highly deferential standard of review for trial court evidentiary rulings.[236] Even when this highly deferential standard is overcome, reversal may not be appropriate.[237] Thus, action by appellate courts would not provide the predictability and uniformity necessary to address the challenges of ESI.[238]

---

231. RICE, *supra* note 9, at 492–94.

232. *See generally* DANIEL J. CAPRA, FED. JUDICIAL CTR., CASE LAW DIVERGENCE FROM THE FEDERAL RULES OF EVIDENCE (2000), *reprinted in* 197 F.R.D. 531 (2000), *available at* http://www.fjc.gov/public/pdf.nsf/lookup/CaseLawD.pdf/$file/CaseLawD.pdf. Accordingly, some commentators propose amending pretrial procedures instead of the rules of evidence to address the challenges of ESI. *See generally* Dean A. Morande, *A Class of Their Own: Model Procedural Rules and Evidentiary Evaluation of Computer-Generated "Animations,"* 61 U. MIAMI L. REV. 1069 (2007).

233. *See* RICE, *supra* note 9, at 492; *see also* Burns et al., *supra* note 52, at 227 ("Litigants will continue to face challenges simply from the amount of new data being created.").

234. *See* GEORGE L. PAUL, FOUNDATIONS OF DIGITAL EVIDENCE xxv (2008); *see also* Finkelstein & Storch, *supra* note 123, at 17 (noting that ESI presents "types of evidence not even contemplated when the rules were written").

235. PAUL, *supra* note 234, at xxv.

236. *See, e.g.*, United States v. Whitaker, 127 F.3d 595, 601 (7th Cir. 1997) ("Appellants who challenge evidentiary rulings of the district court are like rich men who wish to enter the Kingdom; their prospects compare with those of camels who wish to pass through the eye of a needle." (quoting United States v. Glecier, 923 F.2d 496, 503 (7th Cir. 1990))); Am. Express Travel Related Servs. Co. v. Vee Vinhnee (*In re* Vee Vinhnee), 336 B.R. 437, 443 (B.A.P. 9th Cir. 2005) (noting that "a trial court that is finicky about settled authentication requirements will be sustained unless we have the firm and definite conviction that there was a clear error of judgment in rejecting the proffered authentication"). For a more extensive discussion of the deference appellate courts give to the evidentiary rulings of trial courts, see generally David P. Leonard, *Appellate Review of Evidentiary Rulings*, 70 N.C. L. REV. 1155 (1992).

237. *See, e.g.*, ACTONet, Ltd. v. Allou Health & Beauty Care, 219 F.3d 836, 848 (8th Cir. 2000) (noting that even if a trial court erred by admitting Internet evidence, reversal was not appropriate because the affected party could not demonstrate prejudice).

238. *See* Randolph N. Jonakait, *Text, Texts, or Ad Hoc Determinations: Interpretation of the Federal Rules of Evidence*, 71 IND. L.J. 551, 553 (1996) (noting some of the difficulties in relying upon appellate courts to provide definitive answers to lower courts on evidentiary issues).

The Federal Judicial Conference, Congress, and the Supreme Court have demonstrated their willingness in the past to address the procedural problems posed by electronic communications.[239] Perhaps the most obvious example of this concept is the passage of the e-discovery amendments to the Federal Rules of Civil Procedure in 2006.[240]

In the evidence context, Congress recently adopted a new rule of evidence, Rule 502, in part to address the problems of inadvertent waiver caused by the production of electronically stored information.[241] This amendment illustrates not only a willingness to address the problems presented by ESI generally, but also an initial attempt to amend the Federal Rules of Evidence to accommodate the proliferation of ESI in litigation that resulted from the e-discovery amendments to the Federal Rules of Civil Procedure.[242] Further, at the state level, thirty-eight states have adopted the Uniform Rules of Evidence, which recognize the unique challenges of electronic evidence and have provisions specifically designed to address them.[243]

Similarly, the rules of authentication, hearsay, and the best evidence rule should be amended to address the unique issues presented by ESI.[244] Under the current system, a tremendous amount of uncertainty has arisen.[245] As a result, parties spend a significant amount of time and resources preparing for the toughest admissibility standard, with no guarantee of success.[246] By amending the rules to address these issues, litigants and judges can avoid potentially

---

239. For a complete description of the amendment process, see generally 6 WEINSTEIN & BERGER, *supra* note 88, § 1102.02. To summarize, within limits and subject to specific procedures, Congress delegated power to the Supreme Court to "prescribe general rules of practice and procedure and rules of evidence for cases" in federal courts. 28 U.S.C. § 2072(a) (2006). However, Congress retains the authority to review or reject proposed rules. *See id.* § 2074. Further, Congress can also enact rules of evidence directly, for example, as it did when it adopted Federal Rule of Evidence 412. *See* The Privacy Protection for Rape Victims Act of 1978, Pub. L. No. 95-540, 92 Stat. 2046 (codified as amended as FED. R. EVID. 412). The Judicial Conference of the United States, by statute, has the responsibility of initially reviewing and proposing new federal rules as well as amendments. *See* 28 U.S.C. § 331; *id.* § 2073. See generally 6 WEINSTEIN & BERGER, *supra* note 88, § 1102.03, for a complete description of the procedure for judicial amendments to the federal rules.

240. *See supra* Part I.B.

241. *See* S. REP. NO. 110-264, at 1–3 (2008).

242. *See id.*

243. *See* UNIF. R. EVID. 101 cmt. (1999); Legal Info. Inst., Uniform Rules of Evidence Locator, http://www.law. cornell.edu/uniform/evidence.html (last visited May 9, 2010) (listing the states that have adopted the Uniform Rules of Evidence).

244. Notably, these are not the sole areas in which amendments to the Federal Rules of Evidence may be necessary. Similar to the e-discovery amendments to the Federal Rules of Civil Procedure, a complete modernization may be appropriate. *See generally* Paul, *supra* note 9.

245. *See, e.g.*, RICE, *supra* note 9, at 492–94; Burns et al., *supra* note 52, at 227–29.

246. *See, e.g.*, Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 574 (D. Md. 2007); Burns et al., *supra* note 52, at 221; Dale Conder, Jr., *The Admissibility of Electronically Stored Information*, FOR THE DEF., Sept. 2008, at 22, 29 ("Failure to prepare for the most demanding standard may cost you the benefit of the electronic evidence you diligently collected during the pretrial phase of your case.").

wasteful expenditures of time and money, as well as benefit from greater predictability and uniformity in the admission of ESI at trial.[247]

Uncertainty also imposes costs on parties before trial. For example, a large business that may potentially be subject to suit in multiple jurisdictions will have to maintain its records in a manner to ensure admissibility according to the toughest evidentiary standard.[248] Clearly addressing this issue in the rules would allow businesses to avoid unnecessary expenses and efficiently structure their policies to ensure admissibility in subsequent litigation.[249]

The uncertainty created by differing admissibility standards is also significant because it affects summary judgment and other pretrial dispositive motions.[250] As a practical matter, these motions allow parties to minimize litigation costs by resolving cases quickly, and most cases are resolved in this manner.[251] When ruling on these motions, however, a court can only consider evidence that would be admissible at trial.[252] Thus, a court's approach to electronic evidence has significant effects both before and during trial.

B. Authentication

To address the varying standards used by courts, several changes should be made to the authentication rules.[253] By addressing the differences among

---

247. *See* Mengler, *supra* note 228, at 457 (noting that "the Federal Rules of Evidence are intended to provide some guidance to trial courts and litigants"); Laurence H. Tribe, *Triangulating Hearsay*, 87 HARV. L. REV. 957, 974 (1974) (noting the "definite need for clear, uniform, and predictable rules of evidence to serve as the basis for rapid judgments at trial and as a guide for trial preparation").

248. *See* RICE, *supra* note 9, at xvii–xxi.

249. *See, e.g.*, Leonard, *supra* note 228, at 1004 (noting how clear guidance on evidentiary issues allows litigants to avoid unnecessary expense and delay).

250. *See, e.g.*, Boehning & Toal, *supra* note 176 (noting that the evidentiary issues relating to ESI are important because "[c]learing the evidentiary hurdles . . . could mean the difference between a successful motion and the uncertainty of a trial").

251. *See, e.g.*, Arthur R. Miller, *The Pretrial Rush to Judgment: Are the "Litigation Explosion," "Liability Crisis," and Efficiency Clichés Eroding Our Day in Court and Jury Trial Commitments?*, 78 N.Y.U. L. REV. 982, 1048–56 (2003) (discussing the increased use of summary judgment in civil litigation). In 2009, only 1.2% of civil cases in federal district court went to trial. JAMES C. DUFF, ADMIN. OFFICE OF THE U.S. COURTS, 2009 ANNUAL REPORT OF THE DIRECTOR: JUDICIAL BUSINESS OF THE UNITED STATES COURTS 165 tbl.C-4 (2010), *available at* http://www.uscourts.gov/judbus2009/JudicialBusinespdfversion.pdf.

252. *See* FED. R. CIV. P. 56(e); Woods v. City of Chicago, 234 F.3d 979, 987–88 (7th Cir. 2000); Stuart v. Gen. Motors Corp., 217 F.3d 621, 636 n.20 (8th Cir. 2000); Gleklen v. Democratic Cong. Campaign Comm., Inc., 199 F.3d 1365, 1369 (D.C. Cir. 2000); Macuba v. Deboer, 193 F.3d 1316, 1322–24 (11th Cir. 1999); Pamintuan v. Nanticoke Mem'l Hosp., 192 F.3d 378, 387 n.13 (3d Cir. 1999); Raskin v. Wyatt Co., 125 F.3d 55, 66 (2d Cir. 1997); Bombard v. Fort Wayne Newspapers, Inc., 92 F.3d 560, 562 (7th Cir. 1996); Thomas v. Int'l Bus. Machs., 48 F.3d 478, 485 (10th Cir. 1995); Sakaria v. Trans World Airlines, 8 F.3d 164, 171 (4th Cir. 1993); Donaghey v. Ocean Drilling & Exploration Co., 974 F.2d 646, 650 n.3 (5th Cir. 1992); Finn v. Consol. Rail Corp., 782 F.2d 13, 16 (1st Cir. 1986); Hollingsworth Solderless Terminal Co. v. Turley, 622 F.2d 1324, 1335 n.9 (9th Cir. 1980).

253. *See* Galves, *supra* note 227, at 272 (stating that an explicit amendment to the authentication rules is needed to provide guidance to judges as to the proper foundation for computer-generated evidence). Commentators are divided as to the probability, under the status quo, that the authentication rules will be amended to address ESI. *Compare* RICE, *supra* note 9, at 359 n.40

courts on how ESI is authenticated, the Rules can begin to resolve the problems associated with ESI, such as the greater potential for fraud and manipulation, in a more efficient and effective manner.[254]

Initially, Rule 901(b)(1) should be amended to clarify the issues that arise when authenticating ESI through witness testimony.[255] Currently, courts differ over how much weight to give to concerns over the potential for technologically savvy individuals to alter electronic information.[256] Accordingly, as previously mentioned, some courts require testimony authenticating the content of electronic information.[257] With Web sites, for example, because of concerns about potential manipulation by hackers, these courts require testimony that the site owner or operator placed the information onto the site.[258]

One way to address these concerns for witness testimony is for authentication rules to distinguish between printouts of electronically stored information and situations where an electronic version is available. Because printouts of ESI do not contain all of the information available in an electronic version, such as metadata, that courts could use to verify authenticity, there should be a heightened authentication requirement when a party offers a printout into evidence without making an electronic copy available.[259] In these circumstances, testimony about the substance of the printout would be appropriate to prevent the admissibility of potentially compromised evidence.[260] Otherwise, if a party possesses the information in electronic form, such as when a party possesses a hard drive containing the information, that party should be able to authenticate the information using normal chain of custody testimony.[261] This distinction

---

(noting that amendments appear unlikely), *with* Paul, *supra* note 9 (noting current trends at the state and federal level to address the evidentiary challenges of electronic evidence).

254. *See* RICE, *supra* note 9, at 494.

255. *See supra* Part II.A.3; *see also* Galves, *supra* note 227, at 270–71 (arguing that changes should be made to the rules governing the witness testimony needed to authenticate computer-generated evidence).

256. *See supra* note 107 and accompanying text; *see also* Gregory P. Joseph, *Internet Evidence*, NAT'L L.J., June 11, 2001, at A14 (noting that some judges are inherently skeptical of anything from the Internet).

257. *See supra* note 105 and accompanying text.

258. *See supra* notes 105–07 and accompanying text.

259. *Cf.* 8B WRIGHT ET AL., *supra* note 5, § 2218 (noting the "substantial reasons for access" to electronic versions of computerized information in order for an opposing party to test the reliability of the evidence).

260. *See* Rudolph J. Peritz, *Computer Data and Reliability: A Call for Authentication of Business Records Under the Federal Rules of Evidence*, 80 NW. U. L. REV. 956, 990–93 (1986) (discussing the need for a more comprehensive authentication procedure for computer-generated data to address potential system insecurity and manipulation).

261. *See* ARKFELD, *supra* note 1, § 8.11(C); IMWINKELRIED, *supra* note 135, at 74–82; *see also* Erin E. Kenneally, *Confluence of Digital Evidence and the Law: On the Forensic Soundness of Live-Remote Digital Evidence Collection*, 2005 UCLA J.L. & TECH. 5, ¶¶ 25–26, http://www.lawtechjournal.com/articles/2005/05_051201_Kenneally.php (discussing the chain of custody procedures used by digital forensic practitioners to authenticate ESI). In the context of Web sites, a party could also compare the electronic version to a printout to verify the printout's authenticity. *See generally* ARKFELD, *supra* note 1, § 3.10(B)(3) (discussing how Web sites are stored electronically). Presumably, when a hard drive exists, a party can then obtain it, or an electronic copy of it, during discovery.

best serves the primary purpose of the authentication requirement: preventing fraud and mistake.[262]

Accordingly, Rule 901(b)(1) should be amended to read as follows: "In the case of electronically stored information, if the evidence has previously been produced or made available in electronic form, testimony about the process by which it was obtained will suffice. Otherwise, such testimony should refer to its substantive content."[263]

In practice, the effect of this amendment depends on the form of ESI that a party is offering into evidence. For Web sites, if the site was currently online and accessible by the opposing party, it would qualify as being "available" pursuant to the proposed amendment. In this situation, a witness would testify that he or she typed in the Web site's address, viewed the site, and that the printout accurately reflects what he or she viewed.[264] This testimony would be similar to the approach used to authenticate photographs.[265] Indeed, one court has already made this analogy.[266] Although the potential for fraud exists, the opposing party can explore this possibility through cross-examination.[267] Otherwise, if this information was not available electronically, the amended Rule would require a more elaborate showing, akin to the standard adopted by some courts requiring proof that the company actually placed the information on the site.[268]

For e-mails, providing an electronic version of an e-mail during discovery or before trial would qualify it as having "previously been produced." In that case, basic chain of custody testimony would suffice to authenticate it.[269] More specifically, a party could lay a foundation by printing the e-mail's electronic routing information, introducing the routing records for each server that handled the message, and establishing that the e-mail's purported author had primary or exclusive access to the computer where the message originated.[270]

If a party had not previously produced an electronic version, testimony about the e-mail's content would be necessary to comply with Rule 901(b)(1).[271] For example, a witness could testify that only the purported au-

---

262. *See supra* notes 84–87 and accompanying text.

263. This provision would presumably adopt a definition of electronically stored information that is consistent with that used by the Federal Rules of Civil Procedure. *See supra* note 54 and accompanying text.

264. *See* Gregory P. Joseph, *Internet and E-mail Evidence*, 13 PRAC. LITIG. 45, 46 (2002).

265. *See supra* note 76 and accompanying text.

266. *See* ACTONet, Ltd. v. Allou Health & Beauty Care, 219 F.3d 836, 848 (8th Cir. 2000) ("HTML codes are similar enough to photographs to apply the criteria for admission of photographs to the admission of HTML codes.").

267. *See* Joseph, *supra* note 264, at 46.

268. *See, e.g.*, United States v. Jackson, 208 F.3d 633, 638 (7th Cir. 2000); *see also supra* note 105–07 and accompanying text.

269. *See, e.g.*, IMWINKELRIED, *supra* note 135, at 80–81 (summarizing the traditional chain of custody method of authentication).

270. *See id.* at 81–82.

271. *Cf.* RICE, *supra* note 9, at 347 ("The 'cold,' or unanticipated, nature of many e-mail contacts, the susceptibility of manipulation of e-mail headers, and the possibility of hackers manipulating Web postings will often create the need for additional methods of proof."). It is worth

thor of the e-mail knew the information it contained.[272] Testimony that the alleged author took action consistent with the content of the message would be another method of authentication in this situation.[273]

Rule 901(b) should also be amended to explicitly incorporate the use of technology as a method of authentication.[274] Including a separate provision would provide a clear mechanism for parties to use when technological methods of authenticating ESI are available.[275] It could also address the current differences in the application of the "distinctive characteristics" illustration in Rule 901(b)(4).[276] An amendment, however, must remain broad enough to adapt with changes in technology.[277] Thus, as technological mechanisms for falsifying information develop and proliferate, the rule should be flexible enough to allow parties to use new measures to counter those mechanisms as well.[278]

One technology that could be used pursuant to this new illustration is electronic signatures.[279] The legitimacy of this technology is already recognized at the state and federal levels.[280] In 2000, Congress passed the Electronic Signatures in Global and National Commerce Act (E-SIGN) to address the problems associated with contracting in cyberspace.[281] E-SIGN defined "electronic signature" as "an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record."[282] The Uniform Electronic Transactions Act, adopted by forty-seven states, contains an identical definition.[283]

---

reiterating that this analysis pertains solely to authentication pursuant to Rule 901(b)(1). Other authentication methods would not be affected by this proposed amendment.

272. *See* IMWINKELRIED, *supra* note 135, at 75; RIEDY ET AL., *supra* note 12, at 188–89.

273. *See* IMWINKELRIED, *supra* note 135, at 75.

274. *See* Paul, *supra* note 9 (noting that "courts must become aware of the demise of the old authenticity paradigm, simultaneously acknowledging incipient solutions for authentication which are possibly superior to the old regime").

275. *See* Galves, *supra* note 227, at 270–72 (proposing the addition of a separate illustration to FED. R. EVID. 901(b) to provide guidance for courts faced with computer-generated evidence). For a general discussion of several potential technological authentication methods, see RICE, *supra* note 9, at 386–91 and IMWINKELRIED, *supra* note 135, at 75–82.

276. *See supra* notes 121–29 and accompanying text.

277. *See* RICE, *supra* note 9, at 335 ("While the advent of digital technology has expanded the ways in which documents can be corrupted or forged, it has also expanded the ways in which they can be authenticated.").

278. *See id. But see* Colin Miller, *Even Better than the Real Thing: How Courts Have Been Anything But Liberal in Finding Genuine Questions Raised as to the Authenticity of Originals Under Rule 1003*, 68 MD. L. REV. 160, 207–09 (2008) (stating that advances in the technology used to detect manipulation lags behind advances in the technology used to commit fraud).

279. *See* Paul, *supra* note 9 (discussing the use of digital signatures for authentication purposes).

280. *See id.*

281. Pub. L. No. 106-229, 114 Stat. 464 (2000) (codified as amended at 15 U.S.C. §§ 7001–7031 (2006)).

282. 15 U.S.C. § 7006(5) (2006).

283. *See* UNIF. ELEC. TRANSACTIONS ACT § 2(8) (1999); A Few Facts About the Uniform Electronic Transactions Act, http://www.nccusl.org/nccusl/uniformact_factsheets/uniformacts-fs-ueta.asp (last visited May 9, 2010) (listing the states that have adopted UETA). Other uniform laws have similar definitions. *See* UNIF. COMPUTER INFO. TRANSACTIONS ACT § 102(6) (1999).

Both laws have provisions recognizing the potential legal effect and enforceability of an electronic signature.[284]

Another new technology that courts have indicated may be useful for authentication purposes is the use of "hash marks" or "hash values."[285] "Hash" is a "mathematical algorithm that represents a unique value for a given set of data, similar to a digital fingerprint."[286] A party can apply this algorithm to an individual file, a section of a disk, or an entire hard drive, creating a unique "hash value" that will change if the affected data is subsequently altered.[287] If even a single word is changed, the algorithm creates a new hash value, making any alterations clearly identifiable.[288] For this reason, one court indicated that the use of hash marks could make ESI self-authenticating.[289] Indeed, some courts have adopted local protocols suggesting that parties use this technology during discovery to identify each unique file and to maintain its integrity throughout litigation.[290]

Providing for the use of authenticating technologies, such as electronic signatures and hash marks, is beneficial for several reasons. First, as previously outlined, many of these forms of authentication are already recognized as legitimate by other bodies of law.[291] Allowing for the use of such technolo-

---

284. *See* 15 U.S.C. § 7001(a)(1) (2006) (stating that "a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form"); UNIF. ELEC. TRANSACTIONS ACT § 7(a) ("A record or signature may not be denied legal effect or enforceability solely because it is in electronic form."); *see also* UNIF. ELEC. TRANSACTIONS ACT § 13 ("In a proceeding, evidence of a record or signature may not be excluded solely because it is in electronic form.").

285. *E.g.*, Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 546 (D. Md. 2007); Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640, 655–56 (D. Kan. 2005); ROTHSTEIN ET AL., *supra* note 11, at 24 (noting that hash values can be "used to guarantee the authenticity of an original data set"); Ralph C. Losey, *Hash: The New Bates Stamp*, 12 J. TECH. L. & POL'Y 1, 20 (2007) (noting that "[h]ash is . . . an excellent tool to guarantee the authenticity of ESI"); Paul, *supra* note 9.

286. SEDONA CONFERENCE GLOSSARY, *supra* note 12, at 25. For background on hash marks and their uses, see generally Losey, *supra* note 285.

287. *See* ARKFELD, *supra* note 1, § 5.5(B).

288. *See id.*; *see also* Losey, *supra* note 285, at 13 ("Even if the files have a different name, if their contents are exactly the same, they will have the same hash value. But if you simply change a single comma in a thousand page text, that document will have a completely different hash number than the original.").

289. *Williams*, 230 F.R.D. at 655 ("When an electronic file is sent with a hash mark, others can read it, but the file cannot be altered without a change also occurring in the hash mark. The producing party can be certain that the file was not altered by running the creator's hash mark algorithm to verify that the original hash mark is generated. This method allows a large amount of data to be *self-authenticating* with a rather small hash mark, efficiently assuring that the original image has not been manipulated." (emphasis added) (citations omitted)). Another court noted that hash values would be sufficiently distinctive characteristics to permit authentication under Rule 901(b)(4). *Lorraine*, 241 F.R.D. at 547.

290. *See, e.g.*, U.S. Dist. Ct. for Dist. of Md., Suggested Protocol for Discovery of Electronic Information, at 20–21, http://www.mdd.uscourts.gov/news/news/ESIProtocol.pdf (last visited May 9, 2010). This protocol "has not been adopted by the court but may be of assistance to counsel." *Id.* pmbl.

291. *See supra* notes 280–90 and accompanying text; *see also* Paul, *supra* note 9.

gies as an authentication tool would promote consistency between these areas of the law.[292] The technology is also widely available, often at a low price.[293]

Further, recognizing the potential of technological methods of authentication would promote efficiency by creating an evidentiary presumption of authenticity.[294] Although the potential for fraud remains, "[u]sers must be required to accept responsibility for a more heightened level of security . . . . If the device was misused, users should have to convince the jury of that fact."[295] A presumption, therefore, satisfies a party's burden of production and allows a jury to take any potential problems into consideration.[296] Thus, applying this presumption would achieve the proper balance between efficiency, predictability, and promoting the goals of the authentication requirement.

A technology-specific amendment would also address the differing standards regarding the authentication of e-mails.[297] Instead of relying upon testimony from the sender or the recipient, any e-mail or other electronic communication that contained a digital signature or a technological mechanism for establishing its authenticity would satisfy the authentication requirement.

Although these changes do not address the potential for another individual to use someone's e-mail account, a party opposing the admissibility of such evidence always has the ability to dispute an e-mail's authenticity.[298] This rebuttable presumption "may be the most reasonable, and perhaps the only successful, method of accomplishing identification of authorship."[299] However, in the absence of an authenticating technology the other amendments to Rule 901(b) would provide guidance about the substance of an authenticating witness's testimony.

Further, any amendments should encourage judicial notice of appropriate technological facts for authentication purposes.[300] The applicable rules are

---

292. *See* Miller, *supra* note 278, at 181–82 (noting the importance of construing federal rules consistently).

293. *See, e.g.*, Losey, *supra* note 285, at 16 (stating that the software used to perform a hash analysis of files is "widely available, easy to use, and many are free").

294. *See* RICE, *supra* note 9, at 388–89 ("In light of the compelling nature of the logical inference of authorized use that would arise from the presence of an electronic signature on an instrument, perhaps a formal evidentiary presumption (which does not currently exist) will eventually be recognized, shifting the burden of persuasion to the party claiming that the mark is not authentic.").

295. *Id.*

296. *See* Joseph, *supra* note 264, at 47; *see also* United States v. Barlow, 568 F.3d 215, 220 (5th Cir. 2009) ("The ultimate responsibility for determining whether evidence is what its proponent says it is rests with the jury.").

297. *See supra* notes 117–20 and accompanying text.

298. *See* RICE, *supra* note 9, at 349–50.

299. *Id.* at 350; *see also* Int'l Casings Group, Inc. v. Premium Standard Farms, Inc., 358 F. Supp. 2d 863, 873 n.13 (W.D. Mo. 2005) ("[T]he fact that the e-mail header with the name of the sender can be electronically 'forged,' should not render it an insufficient signature as a matter of law.").

300. *See* RICE, *supra* note 9, at 483–84; Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 553 (D. Md. 2007) ("Judicial notice could be a helpful way to establish certain well known characteristics of computers, how the internet works, scientific principles underlying calculations performed within computer programs, and many similar facts that could facilitate authenticating electronic evidence.").

sufficiently flexible to allow a court to take judicial notice of the reliability of science and technology and would not require any changes.[301] Accordingly, courts could use judicial notice for the purpose of establishing the reliability of underlying technologies.[302]

This approach would not, however, eliminate other evidentiary hurdles, such as logical relevance, authentication, the best evidence rule, or hearsay, and a party could always introduce evidence of manipulation or fraud.[303] Although a court could take notice of the underlying technology, a party would still have to establish the reliability of the particular application of that technology, establish that it was used properly, and authenticate any printouts or other results produced.[304] This approach can be incorporated into any amendments to Rule 901(b), which courts could use for guidance when asked to take judicial notice of facts relating to ESI for other purposes as well.

Practically, an amendment addressing these issues could take the form of a new illustration in Rule 901(b).[305] This new illustration could be worded as follows:

> Electronically Stored Information. The content of electronically stored information, in addition to any other method of authentication, by evidence, through testimony or otherwise, of the presence of specific technological measures. The accuracy of a specific technological measure is a fact of which a court may take judicial notice, provided such notice complies with all applicable rules.[306]

For an example of how this amendment could apply in practice, consider the case of *United States v. Whitaker*, discussed earlier.[307] In *Whitaker*, the defendant raised concerns over potential manipulation when his co-conspirator assisted police in retrieving information from a computer.[308] Applying the proposed amendment, the police could have implemented a technology such as hash values before the evidence was retrieved. Had this been done, any ma-

---

301. *See* RICE, *supra* note 9, at 483; *see also* Daubert v. Merrell Dow Pharms., Inc., 509 U.S. 579, 593 n.11 (1993) ("Of course, well-established propositions are less likely to be challenged than those that are novel, and they are more handily defended. Indeed, theories that are so firmly established as to have attained the status of scientific law, such as the laws of thermodynamics, properly are subject to judicial notice under Federal Rule of Evidence 201.")

302. *See* RICE, *supra* note 9, at 483–84; *see also* 2 DIX ET AL., *supra* note 2, § 294, at 324–25 n.11 ("The principles of electronic data processing are a proper subject of judicial notice and should not require proof.").

303. RICE, *supra* note 9, at 484; *see also supra* note 82 and accompanying text.

304. *See* RICE, *supra* note 9, at 485.

305. *See* Galves, *supra* note 227, at 270–72 (arguing for the addition of a new illustration in Rule 901(b) to address the challenges of computer-generated evidence).

306. This provision is worded to mimic the style used by the illustration addressing the authentication of telephone conversations. *See* FED. R. EVID. 901(b)(6). Note that under this provision, a court could take judicial notice of a specific technology's accuracy, but it would still require the proponent of ESI to demonstrate that it was properly applied to the evidence at issue.

307. *See supra* notes 112–16 and accompanying text.

308. *See* United States v. Whitaker, 127 F.3d 595, 602 (7th Cir. 1997).

nipulation clearly would have been evident.[309] The court could have taken judicial notice of how such technology operates.

The proposed amendment would lead to similar results with e-mails. For example, an e-mail could be authenticated through testimony about encryption technology used to send the e-mail.[310] Foundational testimony about the use of a digital signature would also suffice for authentication purposes.[311] Again, a court could take judicial notice of how these technologies operate—the key foundation necessary to authenticate the evidence would be proof that such technologies were in place and operational when the e-mail was originally sent. Thus, combining this amendment with amendments to other illustrations in Rule 901 would begin to provide the necessary clarity to allow a party to predictably and reliably authenticate ESI, while still ensuring that the purposes of the authentication requirement are not eviscerated.

C. Hearsay

As previously outlined, one of the most significant issues that arises when courts apply the hearsay rules to ESI is the application of the business records exception in Rule 803(6).[312] Courts generally agree that printouts of computerized records qualify under this exception.[313] This outcome is consistent with the text of the exception, which explicitly contemplates its application to electronically stored business records by stating that it applies to records "in any form."[314]

Fine-tuning the business records exception is important, however, because businesses are shifting toward maintaining most, if not all, of their records electronically.[315] E-mail also plays an essential role in the modern business model.[316] As one recent study found, a company with 100,000 employees generated twenty-two million new e-mail messages each week.[317] This volume of e-mails grows annually.[318]

---

309. *See supra* note 288 and accompanying text.

310. *See* IMWINKELRIED, *supra* note 135, at 75–78.

311. *See id.* at 78–79.

312. *See supra* Part II.B.3. Some commentators argue in favor of broader changes to the hearsay rules with respect to ESI. *See, e.g.*, RIEDY ET AL., *supra* note 12, at 206 (arguing that even records that are entirely computer-generated should be subject to the hearsay rules).

313. *See supra* note 186 and accompanying text.

314. FED. R. EVID. 803(6); *see also id.* advisory committee's note ("The form which the 'record' may assume under this rule is described broadly . . . . It includes, but is by no means limited to, electronic computer storage.").

315. *See, e.g.*, 2 DIX ET AL., *supra* note 2, § 294, at 323 ("With the explosive development of electronic data processing, most business records are now processed by computers."); Carbine & McLain, *supra* note 229, at 8 ("Even most small businesses keep their records on computers and use computers for their bookkeeping.").

316. *See, e.g.*, RIEDY ET AL., *supra* note 12, at 197 (noting that "business today runs on e-mail"); Scheindlin & Rabkin, *supra* note 27, at 338 ("E-mail is fast becoming the primary means of communication between businesses and individuals."); Robins, *supra* note 27, at 222–23.

317. RIEDY ET AL., *supra* note 12, at 5.

318. *Id.*

In light of these changes, the business records exception is increasingly important.[319] If the exception did not apply, it would be difficult, if not impossible, for a business to locate and present as witnesses all of the individuals who may have supplied computerized information.[320] Further, the modern business model requires a daily reliance on ESI and electronic communications.[321] Accordingly, businesses are highly motivated, if only for self-serving reasons, to ensure the accuracy and reliability of their electronic data.[322] The current approach taken by many courts, however, fails to recognize these changing business practices.[323]

The first issue that amendments should address is the requirement that records be "kept in the course of a regularly conducted business activity."[324] Many courts narrowly construe this requirement in the context of ESI to require a business to have a policy mandating the preservation of ESI, particularly e-mails.[325] Rule 803(6) should be amended to reject this heightened burden.

Specifically, a provision should be added to Rule 803(6) that reads as follows: "In the case of electronically stored information, including electronic communications, it must be the regular practice of that business entity to retain the information, either intentionally or unintentionally, in any form."

United States v. Ferber provides an example of the potential practical effect of this proposed amendment.[326] In *Ferber*, a mail and wire fraud case, the disputed evidence was an e-mail from the defendant's co-worker that described a telephone conversation that the coworker had with the defendant.[327] At trial, the government sought to introduce a printout of this e-mail.[328] The government properly authenticated the e-mail and provided foundation testimony that it was the coworker's routine practice to send it as part of the company's business.[329] The court, however, excluded this evidence, concluding that there was no showing that the company required e-mails to be maintained.[330] Without such a showing, the court concluded that "virtually any document found in the files of a business which pertained in any way to the functioning of that business would be admitted willy-nilly as a business record."[331]

---

319. *See* BINDER, *supra* note 186, § 16:17; Finkelstein & Storch, *supra* note 123, at 15.
320. *See* BINDER, *supra* note 186, § 16:17.
321. *See id.*
322. *See id.*; 5 WIGMORE, *supra* note 157, § 1522, at 442.
323. *See* BINDER, *supra* note 186, § 16:17.
324. FED. R. EVID. 803(6).
325. *See supra* notes 193–94 and accompanying text.
326. United States v. Ferber, 966 F. Supp. 90 (D. Mass. 1997).
327. *Id.* at 98.
328. *Id.*
329. *Id.*
330. *Id.* at 98–99.
331. *Id.* at 99.

The proposed amendment would dictate a different result in *Ferber*. If the government could demonstrate that the coworker had a duty to send the e-mail and regularly did so as part of the company's business, the fact that the company lacked a policy requiring that the e-mails be maintained would not prevent admissibility. In other words, as long as the company retained the e-mail, even unintentionally, the "kept" requirement would be satisfied.[332]

However, if a party could demonstrate suspicious circumstances, a court, in its discretion, could still exercise its authority to exclude the record as lacking indications of trustworthiness.[333] For example, if a company had policies in place requiring the deletion of e-mails on a regular basis, yet a particularly damning e-mail mysteriously survived, a court could decide to exclude it. Overall, by maintaining the traditional foundational requirements, but adjusting them for the ESI context, this change would not erode the purposes of the business records exception, nor permit the wholesale introduction of all of a business's files "willy-nilly."[334]

Another issue deserving attention through an amendment to the Federal Rules of Evidence is how the business records exception interacts with the self-authentication requirement. One of the benefits of the business records exception is that, when combined with Rule 902, it allows businesses to submit self-authenticating records to a court without the cost, delay, and hassle of sending the appropriate personnel to testify.[335] Otherwise, practical problems and substantial costs may prevent such records from being admissible altogether.[336] Ensuring a streamlined process for the admission of ESI pursuant to the business records exception allows companies to avoid these problems and realize significant cost savings.

---

332. As outlined earlier, ESI is often retained unintentionally. *See supra* notes 28–29 and accompanying text.

333. *See* FED. R. EVID. 803(6) (providing that business records are excluded from the hearsay rule if the foundational requirements are met, "unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness"); BINDER, *supra* note 186, § 16:17 (noting that Rule 803(6) "give[s] the trial judge discretion to exclude hearsay that would otherwise qualify for exception from the hearsay rule as an entry in a business record, if the judge finds that the source of information, or the method or circumstances of preparation, indicate lack of trustworthiness").

334. *Ferber*, 966 F. Supp. at 99.

335. *E.g.*, FED. R. EVID. 803(6) advisory committee's note (stating that, when combined with the self-authentication provision of Rule 902(11), "the foundation requirements of Rule 803(6) can be satisfied . . . without the expense and inconvenience of producing time-consuming foundation witnesses"); BINDER, *supra* note 186, § 16:17; 5 WEINSTEIN & BERGER, *supra* note 88, § 900.07(1)(d)(iii) (noting that this procedure results in "saving time and money for the court and [the] parties"); *see also* United Asset Coverage, Inc. v. Avaya Inc., 409 F. Supp. 2d 1008, 1052 (N.D. Ill. 2006) ("One of the most useful . . . accomplishments of the Judicial Conference's Advisory Committee on the Rules of Evidence during this Court's tenure as its Chairman was in adding a new Rule 902(11) . . . . That new provision was intended to obviate the need for live witnesses to parade to the stand to support the admission into evidence of business records."); DirecTV, Inc. v. Murray, 307 F. Supp. 2d 764, 772 n.3 (D.S.C. 2004) ("Rule 902(11) was designed to work in tandem with an amendment to Rule 803(6) to allow proponents of business records to qualify them for admittance with an affidavit or similar written statement rather than the live testimony of a qualified witness.").

336. *See* BINDER, *supra* note 186, § 16:17.

Accordingly, Rule 902(11) should be amended to complement the proposed changes to Rule 803(6). Specifically, in light of the changes to Rule 803(6), Rule 902(11) should be amended to add a new subsection (d) that reads as follows: "In the case of electronically stored information, these requirements must be accompanied by evidence reasonably demonstrating the integrity of the medium in which the evidence was stored."

Imposing this additional requirement for self-authentication purposes addresses the concerns of many courts and commentators over the potential for manipulation or alteration of ESI.[337] This amendment would address these concerns by requiring evidence showing that the computer, database, or other electronic storage mechanism had reasonable security procedures in place.[338]

More specifically, this amendment would have several real-world effects. Traditionally, when a party introduces a business record and seeks to take advantage of the self-authentication provision in Rule 902(11), a written declaration from the records custodian establishing the foundational requirements will accompany the record.[339] The rule also requires a party to give notice of its intent to use this provision, along with a copy of the record and declaration, to the opposing party.[340] Thus, requiring foundational evidence about the security measures in place provides the opposing party with the opportunity to investigate if it suspects fraud or alteration once it receives this notice.

Next, consider *In re Vee Vinhnee*, where the disputed evidence consisted of computerized credit card records.[341] To comply with Rule 902(11), the credit card company provided a declaration from an employee identifying the type of equipment used by the company, the software used to generate the records, and a conclusory statement that the industry deemed it reliable.[342] The trial court excluded this evidence as improperly authenticated for purposes of the business records exception.[343]

The appellate court affirmed this decision.[344] The court emphasized that a party seeking to admit electronic business records must demonstrate the circumstances in which the record was maintained.[345] According to the court, such circumstances included "custody, access, and procedures for assuring that the records in the files are not tampered with."[346] In this case, the declaration provided by the credit card company contained no information about the company's computer policy, system control procedures, or how the company con-

337. *See supra* note 175 and accompanying text.

338. *Cf.* Stanley A. Kurzban, *Authentication of Computer-Generated Evidence in the United States Federal Courts*, 35 IDEA 437, 452–53 (1995) (discussing the need for business records to be assessed in combination with the entire process by which they are maintained and stored).

339. *See* FED. R. EVID. 902(11).

340. *Id.*

341. Am. Express Travel Related Servs. Co. v. Vee Vinhnee (*In re* Vee Vinhnee), 336 B.R. 437, 441–42 (B.A.P. 9th Cir. 2005).

342. *Id.* at 447 & n.14.

343. *Id.* at 440.

344. *Id.*

345. *Id.* at 444.

346. *Id.* at 444–45.

trolled access, logged changes, or used procedures to ensure the integrity of records.[347]

This is the type of information contemplated by the proposed amendment to Rule 902(11). The proposed change achieves a balance between ensuring some threshold showing of reliability and avoiding the imposition of an onerous burden on parties attempting to introduce business records. It contemplates only a minimal showing of the mechanisms in place by the party offering the evidence, similar to the Rule 104(b) standard used by a judge when determining the admissibility of evidence.[348] In other words, a party does not need to conclusively establish that its system is impregnable, but rather must demonstrate what it has done to minimize the risk of fraud or alteration.[349]

However, the proposed amendments would not require as heavy a burden as that outlined by the *Vee Vinhnee* court. That court indicated that a party must demonstrate that "the document being proffered is the same as the document that was originally created."[350] Under the proposed revisions, a business would only need to provide information about its policies relating to access, recording changes in records, or similar information. Moreover, a party could still introduce evidence indicating the alteration of electronic records if it suspects fraud or hacking.[351] The pretrial notice required by Rule 902(11) would also provide a party with the opportunity to explore potential weaknesses before trial.[352] In combination, these amendments would address the most prevalent issues involving the application of the hearsay rules to ESI evidence and provide predictable mechanisms for courts to use when determining its admissibility.

D. Best Evidence Rule

In modern society, technological changes have rendered the best evidence rule meaningless.[353] As a result, the Federal Rules of Evidence that implement the best evidence rule should be amended to address a theoretical gap that currently exists in how courts apply it to ESI.[354]

---

347. *Id.* at 448–49.

348. *See* 5 WEINSTEIN & BERGER, *supra* note 88, § 900.06(1)(c)(i) ("Most courts agree that Rule 104(b), rather than Rule 104(a), governs the authentication determination."). The Rule 104(b) standard is a preliminary determination by the judge that there is evidence sufficient to support a jury finding that the proffered evidence is relevant. *See* FED. R. EVID. 104(b); 5 WEINSTEIN & BERGER, *supra* note 88, § 900.06(1)(c)(i).

349. *See* Peritz, *supra* note 260, at 933.

350. *In re Vee Vinhnee*, 336 B.R. at 444.

351. *See, e.g.*, United States v. Safavian, 435 F. Supp. 2d 36, 41 (D.D.C. 2006) (noting that a party opposing the admissibility of e-mails is free to raise issues of potential alteration with the jury).

352. *See* FED. R. EVID. 902(11).

353. *See* RICE, *supra* note 9, at 305.

354. *See id.* (stating that the best evidence rule has become meaningless in the Internet age, with the only solution being to revise the doctrine to reflect these technological changes); Galves, *supra* note 227, at 272–73 (arguing that amendments to the best evidence rules are needed to address the challenges of computer-generated evidence).

For example, multiple parties can view a Web site at the same time.[355] While the images that each visitor to the site sees are typically identical, technically, there is a distinct image displayed on each visitor's computer screen.[356] Thus, no single original exists, and the total number of originals corresponds to the total number of visitors to a site.[357] Each computer, therefore, ends up being a potential source of an "original," but "mutual observation of each . . . party's hard drive is not possible" to prevent fraud and alteration.[358] Whether illustrated by Web sites or other forms of ESI, this result creates a disconnect between the theory of the best evidence rule and its application to ESI.[359]

To address this problem, the definition of "original" under Rule 1001 should be amended to require, when dealing with ESI, proof that the form produced is the final, unaltered form of the information or document. Specifically, in the definition of original, following the provision for data stored in a computer, a sentence should be added that states: "This provision does not include a printout or other output readable by sight unless its proponent presents evidence sufficient to support a finding that it has not been subsequently altered or modified."

Practically, this standard may be difficult to satisfy, as it may be difficult to find the "final" version of a specific e-mail, document, or other piece of electronically stored information.[360] Technological tools, such as hash values, are one potential method of making this showing.[361] This change would also remove enhanced or altered digital images, recordings, or similar forms of ESI from the definition of "original."

However, this would not necessarily mean that the evidence now classified as a duplicate is not admissible. Rather, this issue can be addressed by amending the definition of "duplicate" to include any ESI that would be excluded from the new definition of "original," and by amending the rule governing the admissibility of duplicates.[362] Initially, an additional sentence should be added to Rule 1001(4) which states: "This definition includes a printout or other output readable by sight that its proponent cannot present evidence sufficient to support a finding that it has not been subsequently altered or modified."

---

355. *See* RICE, *supra* note 9, at 303.

356. *Id.*

357. *Id.*

358. *Id.*

359. *See id.*

360. *See, e.g.*, Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 547 (D. Md. 2007) ("Because it is so common for multiple versions of electronic documents to exist, it sometimes is difficult to establish that the version that is offered into evidence is the 'final,' or legally operative version."); RICE, *supra* note 9, at 303.

361. *See supra* notes 285–88 and accompanying text.

362. *See* Paula Noyes Singer, *Proposed Changes to the Federal Rules of Evidence as Applied to Computer-Generated Evidence*, 7 RUTGERS J. COMPUTERS, TECH. & L. 157, 187–88 (1979) (proposing a similar approach for addressing how the best evidence rule applies to computer-generated evidence).

The rule governing the admissibility of duplicates, Rule 1003, should also be amended to state that a duplicate of ESI may be admissible if its proponent produced it to the opposing party in its "original form."[363] This amendment could read as follows: "In the case of data or output readable by sight, a duplicate is admissible if the data or output was produced to all opposing parties in its electronic or original form, unless it would be unfair under the circumstances."

This change to Rule 1003 would clarify how courts would administer the new definition of "original" and "duplicate," as well as promote consistency with the Federal Rules of Civil Procedure.[364] Judges could also apply the provision that excludes evidence when admitting it would be "unfair under the circumstances"[365] to those circumstances where an opposing party previously had the opportunity to use discovery mechanisms to obtain an electronic copy of evidence, yet refrained from doing so.[366] Further, the new provision would dovetail with Federal Rule of Civil Procedure 34(b), which generally requires a party to produce ESI in the form in which it is normally maintained.[367]

As previously outlined, one of the purposes of the best evidence rule is to promote greater access to the more valuable and complete original version of evidence.[368] The proposed amendment would further this goal by providing access to the electronic version of proffered evidence, which provides valuable

363. *See In re* Gulph Woods Corp., 82 B.R. 373, 377–78 (Bankr. E.D. Pa. 1988) (noting that "where a written record, prepared prior to the computer record, contains a more detailed and complete description of the transaction than that contained in the computer record, the proponent of the evidence should be required to produce the more detailed record, or account for its nonproduction").

364. *Cf.* Miller, *supra* note 278, at 181–84 (arguing that Rule 1003 should be applied consistently with the Federal Rules of Civil Procedure).

365. FED. R. EVID. 1003.

366. For example, this provision could be applied if the party had the opportunity to request the evidence in electronic form as per FED. R. CIV. P. 34, yet declined to do so. In criminal cases, there are no rules regulating the form in which ESI is produced. *E.g.*, Burns et al., *supra* note 52, at 228 (noting that "ESI may be relevant in criminal cases, but there are no rules providing guidance on document production in such instances"); *see also* United States v. O'Keefe, 537 F. Supp. 2d 14, 18–19 (D.D.C. 2008) ("In criminal cases, there is unfortunately no rule to which the courts can look for guidance in determining whether the production of documents by the government has been in a form or format that is appropriate."). At least one court applied FED. R. CIV. P. 34 in a criminal case by analogy. *See O'Keefe*, 537 F. Supp. 2d at 19 ("The Federal Rules of Civil Procedure in their present form are the product of nearly 70 years of use and have been consistently amended . . . to meet perceived deficiencies. It is foolish to disregard them merely because this is a criminal case, particularly where . . . it is far better to use these rules than to reinvent the wheel when the production of documents in criminal and civil cases raises the same problems.")

367. *See* FED. R. CIV. P. 34(b)(2)(E)(ii).

368. *See* Cleary & Strong, *supra* note 198, at 840 (noting that "the best evidence rule is in large part predicated upon the assumption that important differences in value exist between original writings and copies of them"); *see also supra* notes 213–14 and accompanying text.

information, such as metadata, that does not exist in a printed version.[369] To complement this change, Rule 1003(2) should be amended to include the unavailability of an electronic version as a "circumstance" for the court to consider.[370] These changes would provide additional guidance for courts when confronting the best evidence rule issues raised by ESI.

In combination, these amendments would have several practical effects on how the best evidence rule is applied to ESI. Under the current regime, because any printout qualifies as an original, the best evidence rule serves a minimal purpose.[371] This led one court to conclude that a party satisfied the best evidence rule, even though the alteration of an electronic media file resulted in the loss of metadata.[372]

With the proposed changes, however, the Rules would now classify most ESI as a duplicate. As a result, a court would generally admit it as an original unless an opposing party raises a "genuine question" about its authenticity, or it would be "unfair" under the circumstances to admit it as a duplicate.[373] Returning to the altered audio file example, applying the proposed rule changes would allow a court to conclude that the loss of metadata made the admission of the file into evidence "unfair under the circumstances" and to exclude it as violating the best evidence rule. Despite this conclusion, pursuant to the proposed change to Rule 1003, if a party produced an electronic copy of the file before trial, the duplicate would nonetheless be admissible.

Overall, these amendments would begin to address the issues currently created by the potential for numerous originals of ESI to exist. They would also address how the purpose of the best evidence rule is undermined when a party modifies ESI, yet courts still consider it an original. Under the proposed revisions, in order for such evidence to satisfy the best evidence rule, a party would have to show that a duplicate is admissible pursuant to Rules 1003 and 1004. Clarifying this distinction would also address the uncertainty over when secondary evidence is admissible.

---

369. *See* 8B WRIGHT ET AL., *supra* note 5, § 2218 (noting the importance of a party receiving ESI in its electronic form instead of a printed copy); *see also* Armstrong v. Executive Office of the President, 810 F. Supp. 335, 341 (D.D.C. 1993) ("A paper copy of the electronic material does not contain all of the information included in the electronic version. For example, a note distributed over these [sic] computer system includes information that is not reproduced on the paper copy regarding who has received the information and when the information was received, neither of which is reproduced on the paper copy."); *see also supra* notes 39–45 and accompanying text.

370. Specifically, FED. R. EVID. 1003(2) could read as follows: "A duplicate is admissible to the same extent as an original unless . . . (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original *In the case of data or output readable by sight, these circumstances shall include the availability of such evidence in electronic form.*" (proposed amendment italicized).

371. *See* RICE, *supra* note 9, at 305.

372. *See* United States v. Sattar, No. 02 CR 395(JGK), 2003 WL 22510435, at *1–2 (S.D.N.Y. Nov. 5, 2003).

373. FED. R. EVID. 1003.

As one commentator noted, "Fitting the rules of evidence into the Internet age is a bit like pouring old wine into new bottles. Some will fit neatly, while others will require a degree of dexterity and ingenuity, and there will be an occasional miss and mess."[374] The evidentiary issues posed by electronically stored information may be difficult to resolve effectively, but that does not mean that inaction is preferable. While not comprehensive, this article proposes specific rule amendments in an attempt to facilitate the discussion of modernizing evidentiary rules to confront the unique issues posed by technological advancements. Until such changes are implemented, judges and attorneys will be forced to confront the challenges of ESI on a case-by-case basis, and to live with the uncertainty, inefficiencies, and varying standards that result.

374. RICE, *supra* note 9, at 492.