Loyola of Los Angeles Law Review

Volume 38
Number 4 *Developments in the Law: Electronic Discovery*

Article 6

6-1-2005

VI. Electronic Evidence and the Federal Rules

Leah Voigt Romano

VI. ELECTRONIC EVIDENCE AND THE FEDERAL RULES*

A. Introduction

Application of evidentiary rules to electronic information is not as controversial as other aspects of electronic discovery. Nevertheless, as the following Section demonstrates, it is an evolving and complex area of the law. Federal courts apply the Rules in virtually the same way as non-electronic, "hard copy" evidence. However, there are applications of the Rules that are relatively untested, and courts are hesitant to admit as evidence any electronic information that can be manipulated or falsified. As technology evolves, and as federal courts become more facile in handling electronic evidence, the Rules as they currently exist may not be able to keep pace with these developments.

Yet, amended or not, the Federal Rules of Evidence[1] will continue to be a significant hurdle to the use of electronic information in litigation. Though the Rules do not come into play until after litigants obtain discovery, the Rules can—and should—inform the entire discovery process. For instance, although litigants can rely on an increasingly wide range of digital and electronic information, not all types of evidence are treated the same under the Federal Rules. Thus, the use of electronic evidence in federal courts raises another series of practical challenges.

Electronic evidence can be a litigant's best friend or worst nightmare, depending on the type of evidence, how it is used, and in what court it is offered. During the latter half of the twentieth

---

* Leah Voigt Romano: J.D. Candidate, May 2006, Loyola Law School, Los Angeles; M.P.H., University of Michigan, April 2003; B.A., Biology and Dance, Smith College, May 1996. I would like to thank Josie Lee-Nozaki, whose advice, support, and sense of humor have made all the difference for me. Special thanks also to Professor David Leonard, for taking the time to give invaluable feedback, and to Heather Barber, for a fabulous job of putting it all together.

1. All references to rules are to the Federal Rules of Evidence (FED. R. EVID.)

century, courts quickly recognized the admissibility of computer-based business and public records.[2] In fact, some courts have concluded that "computer evidence is not intrinsically unreliable,"[3] and they have become relatively adept at dealing with the complexity of electronic and digital evidence. However, courts have not categorically accepted this form of evidence. In particular, they are wary of technologies, like the Internet, which can be accessed and manipulated by a wide range of users. At least one court has remarked that Internet-based evidence is "inherently untrustworthy."[4]

Today, courts consider highly sophisticated digital and electronic evidence, from global positioning satellite tracking data to electronic tollbooth records.[5] As electronic evidence proliferates and grows increasingly complex, federal courts might be more skeptical of its use and origins. Alternatively, courts may continue to take the "more relaxed view" and apply the Rules much as they would for any other form of evidence.[6] Whichever approach the courts follow,

---

2. *See* United States v. Catabran, 836 F.2d 453, 457 (9th Cir. 1988) (holding that computer records of a bankrupt corporation were admissible because the corporation's bookkeeper testified that she input sales, inventory and payroll information on a regular basis and that the printout accurately reflected that information); Rosenberg v. Collins, 624 F.2d 659, 665 (5th Cir. 1980) (holding that testimony of the comptroller of a bankrupt company was sufficient to establish authenticity of computer records).

3. United States v. Vela, 673 F.2d 86, 90 (5th Cir. 1982) (records of phone company's computerized billing process); *see also* Brown v. Town of Chapel Hill, 79 F.3d 1141 (4th Cir. Mar. 19, 1996) (unpublished), *available at* 1996 WL 119932, at *2) (computer printouts of memoranda from town's personnel and transportation departments); United States v. Linn, 880 F.2d 209, 216 (9th Cir. 1989) (computer record of a telephone call to a hotel room); United States v. Croft, 750 F.2d 1354, 1364–65 (7th Cir. 1984) (computer records from university's payroll system); United States v. Young Bros., 728 F.2d 682, 693–94 (5th Cir. 1984) (state's computer records).

4. St. Clair v. Johnny's Oyster & Shrimp, Inc., 76 F. Supp. 2d 773, 774 (S.D. Tex. 1999) (referring to information taken from the Worldwide Web).

5. *See* United States v. Bennett, 363 F.3d 947 (9th Cir. 2004) (reviewing the admissibility of a customs officer's testimony about global positioning satellite data); *see also* Tresa Baldas, *New Data Used as Evidence: Surveillance with Toll Booth and Cellphone Data Is on the Rise*, NAT'L L.J., Aug. 16, 2004, at 1 (describing new forms of electronic evidence "popping up in courtrooms nationwide").

6. *See* Thomas J. Casamassima & Edmund V. Caplicki III, *Electronic Evidence at Trial: The Admissibility of Project Records, E-Mail, and Internet Websites*, CONSTRUCTION LAW., Summer 2003, at 13–14 (stating that most

the Federal Rules will undoubtedly play an integral role in shaping both discovery and admissibility.[7]

This Section describes recent developments in admissibility of computer generated, electronic, and digital evidence.[8] Litigants must anticipate three important obstacles to the admission of electronic evidence.[9] Part B explores the first hurdle of authentication. Before electronic discovery may be admitted into evidence, its proponent[10] must provide "evidence sufficient to support a finding that the matter in question is what its proponent claims."[11] As with other forms of evidence, authenticity of electronic evidence can be proven in a variety of ways.

After proving authenticity, a party offering electronic evidence might have to overcome the hearsay barrier. Part C focuses on

---

courts find the foundation requirement for computer records is the same as that required for other business records); *see also* 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, 963–64 (1986) (noting that, in the context of computerized business records, courts have relaxed conditions of trustworthiness "in deference to the exigencies of modern business practices and the desire for an efficient trial process").

7. The Federal Rules of Evidence apply in both civil and criminal actions. Generally, federal courts treat a particular type of electronic evidence, such as public business records, the same in both criminal and civil contexts. However, the predominant type of electronic evidence used in each context differs. For instance, in cases involving illegal transmission of data over the Internet or via e-mail, prosecutors rely more heavily on computer forensic examinations, while civil litigators are more likely to present electronic evidence derived from business records. Nevertheless, there are no hard and fast rules for what types of electronic evidence can or should be used in criminal or civil cases. *See, e.g.*, Sea-Land Serv., Inc., v. Lozen Int'l, LLC, 285 F.3d 808, 821 (9th Cir. 2002) (characterizing the use of an e-mail message as an "adoptive admission" where one employee authored and forwarded a message to a co-worker who then proceeded to copy the message's contents and add a preface); United States v. Meienberg, 263 F.3d 1177, 1181 (10th Cir. 2001) (using public agency records in criminal prosecution).

8. These terms are used interchangeably to refer to evidence that is "electronic."

9. For an excellent overview of the admissibility of electronically stored evidence in both state and federal courts, see J. Shane Givens, Comment, *The Admissibility of Electronic Evidence at Trial: Courtroom Admissibility Standards*, 34 CUMB. L. REV. 95 (2003–2004).

10. For the purposes of this Section, "litigant" refers broadly to any party to a lawsuit, whereas "proponent" refers specifically to the party seeking to admit an item of evidence.

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

computerized private business records, while Part D highlights the admission of electronically stored public documents. Both types of records can fit squarely within an exception to the hearsay rule.[12] However, as described in Part E, problems arise when this rule is applied to e-mail messages and evidence obtained from the Internet.[13]

Finally, a party sometimes has to contend with a third barrier—the best evidence rule.[14] Part F discusses how this rule might be applied to electronically stored evidence. In general, the rule is a relatively low hurdle because printouts of data stored in electronic or digital format are usually admissible as "originals."[15] However, in cases where data must be manipulated before it can be used as evidence, the best evidence rule may pose a challenge.

B. Foundations for Electronic Evidence: Authentication

Electronic evidence is created "whenever a person enters information into a computer, a computer generates information in response to a request by an operator, or a computer uses or processes information."[16] Unlike other forms of real evidence, electronic evidence can be created almost instantaneously, with a few rapid keystrokes or with no human input at all. Each day, people and computers generate countless bits of electronic information that can potentially be used as evidence. As a result, electronic evidence is virtually everywhere.

---

12. *See id.* 803(6).

13. For instance, an .html posting on a website is considered "Internet evidence."

14. When a party seeks to prove the content of a writing, recording, or photograph—that is, what a writings "says" or what a picture "shows"—the best evidence rule requires that the party provide the court with the original writing, recording, or photograph. *Id.* 1002 (Requirement of Original); *Id.* 1001 (Definitions).

15. *See* Casamassima & Caplicki, *supra* note 6, at 16.

16. 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, 8 (1998). Common or traditional forms of electronic evidence include databases, operating systems, software programs, electronic messages, and computer generated models or images. *Id.*

The first hurdle to the admission of any real evidence is authentication.[17] Unless a party shows that the evidence is what that party claims it to be, the court will view the evidence as irrelevant.[18] Thus, a proponent must prove authenticity before the factfinder will be permitted to consider the evidence. Fortunately (for the proponent), this hurdle remains relatively low: a proponent need only present "evidence sufficient to support a finding" of authentication or identification.[19] By way of illustration, Federal Rule of Evidence 901(b) provides different methods by which the proponent may satisfy this requirement.[20] This is not an exclusive list, and a proponent is not limited to only one method of authentication.[21]

In addition, the Rule is intended to "guide and suggest, leaving room for growth and development in this area of the law."[22] Notably, in 1972, the Federal Rules Advisory Committee recognized that electronic processes or systems[23] and "data stored in computers and similar methods"[24] play an important role in the authentication of real evidence. With this flexibility, proponents can cobble together

17. FED. R. EVID. 901(a) states that the requirement of authentication or identification is a condition precedent to admissibility.

18. United States v. Meienberg, 263 F.3d 1177, 1181 (10th Cir. 2001); *see also* United States v. Hernandez-Herrera, 952 F.2d 342, 343 (10th Cir. 1991) ("The rationale for the authentication requirement is that the evidence is viewed as irrelevant unless the proponent of the evidence can show that the evidence is what its proponent claims."). According to the Advisory Committee for the Federal Rules of Evidence, authentication is therefore "a special aspect of relevancy." FED. R. EVID. 901(a) advisory committee's note.

19. FED. R. EVID. 901(a). Nevertheless, "the need for suitable methods of proof still remains, since . . . unforeseen contingencies may arise, and cases of genuine controversy will still occur." *Id.* 901(a) advisory committee's note; *see also* United States v. Tank, 200 F.3d 627, 630 (9th Cir. 2000) ("The government made a prima facie showing of authenticity because it presented evidence sufficient to allow a reasonable juror to find that the chat room log printouts were authenticated.").

20. FED. R. EVID. 901(b) (e.g., testimony of a witness with knowledge; nonexpert opinion on handwriting; distinctive characteristics and the like; voice identification; public records or reports).

21. *Id.* 901(b) advisory committee's note.

22. *Id.*

23. *Id.*

24. *Id.*

more than one of these methods to prove the authenticity of electronic evidence.[25]

1. Authentication of Business Records

Since the second half of the twentieth century, courts have recognized the evidentiary role of private, computer generated business records. Some courts have required a more extensive foundation for computer records than for other conventional forms of evidence.[26] For instance, in the 1977 case of *United States v. Scholle*,[27] the Eighth Circuit held that a proponent must identify the "original source of the computer program . . . and the procedures for input control including tests used to assure accuracy and reliability."[28] But since then, courts have declined to follow the Eighth Circuit's lead and instead have shown little hesitancy in accepting computer technology and its inherent lack of human control.[29] For instance, in *United States v. Vela*,[30] the Fifth Circuit set the pace with the generally accepted notion that computer evidence is as reliable as other forms of real evidence.[31] Despite *Scholle*'s suggestion that computer records should be subject to unique foundational requirements,[32] the Fifth Circuit reiterated its previous holding that "computer data compilations . . . should be

25. *See, e.g.*, United States v. Tank, 200 F.3d 627, 630–31 (9th Cir. 2000) (relying on computer printouts, notes made by the defendant, and co-conspirator testimony to authenticate chat room discussions between the defendant and a federal agent); United States v. Siddiqui, 235 F.3d 1318, 1322–23 (11th Cir. 2000) (concluding that an e-mail message was authenticated with circumstantial evidence).

26. *See* United States v. Catabran, 836 F.2d 453 (9th Cir. 1988); Rosenberg v. Collins, 624 F.2d 659 (5th Cir. 1982); United States v. De Georgia, 420 F.2d 889 (9th Cir. 1969); Chung & Byer, *supra* note 16, at 41.

27. 553 F.2d 1109 (8th Cir. 1977).

28. *Id.* at 1125.

29. *See, e.g.*, *Catabran*, 836 F.2d at 457 ("The use of a computer to create the ledger does not change the result."); *Rosenberg*, 624 F.2d at 665 (5th Cir. 1982) (supporting the admissibility of computerized business records); United States v. Vela, 673 F.2d 86, 90 (5th Cir. 1982) (stating that computer evidence can be reliable).

30. 673 F.2d 86 .

31. *Id.* at 90.

32. *Id.*

treated as any other record of regularly conducted activity."[33] Thus, when a court considers authenticity, any inaccuracy or material alteration in the electronic record involves the weight of the evidence, not its admissibility.[34]

Today, courts differ in their application of the foundational requirements for electronic evidence. In one line of cases, courts first consider whether electronic evidence has been properly authenticated under Rule 901.[35] For this purpose, courts treat computerized business records the same as records kept in a company's books,[36] and the methods of authentication are generally the same.[37] After finding that electronic evidence has been properly authenticated, a court will next consider whether the evidence constitutes hearsay, and, if so, whether it may nevertheless be admissible under an exception to the hearsay rule, i.e., the business records exception under Rule 803(6).[38] In a second line of cases, courts have sidestepped an explicit authentication analysis and have

---

33. *Id.*; *Rosenberg*, 624 F.2d at 665. The Fifth Circuit also accepted the district court's statement that computerized telephone bills are "even more reliable than . . . average business record[s] because they are not even touched by the hand of man." *Vela*, 673 F.2d at 90.

34. Both federal courts and the Advisory Committee of the Federal Rules follow this general rule. *See, e.g.*, United States v. Meienberg, 263 F.3d 1177, 1180–81 (10th Cir. 2001) (involving public records); United States v. Tank, 200 F.3d 627, 629–31 (9th Cir. 2000) (involving an investigation of chat room logs in a criminal case); *Catabran*, 836 F.2d at 456–58 (9th Cir. 1988) (involving private business records). The reader should bear in mind that this general rule does *not* apply when courts focus on the business records exception to the hearsay rule. In such a case, the requirement of trustworthiness may preclude an electronic record that bears an inaccuracy or is subject to manipulability. *See infra* Part VI.C.2.c (discussing the trustworthiness requirement for the business records exception).

35. *See infra* Parts VI.B.1.a–b, B.2.b (discussing authentication of private and public business records and recovered electronic data).

36. *See Catabran*, 836 F.2d at 457 ("'[I]t is immaterial that the business record is maintained in a computer rather than in company books' assuming that the proponent lays a proper foundation."); United States v. De Georgia, 420 F.2d 889, 893 n.11 (9th Cir. 1969); *infra* Part VI.C.1.

37. *See* Stanley A. Kurzban, *Authentication of Computer-Generated Evidence in the United States Federal Courts*, 35 IDEA 437, 439–40 (1995) (stating that authentication of computer generated evidence has been governed by principles and rules of evidence that existed before computer usage became widespread and that application of rules "requires analogizing computer-related processes to those that pre-dated the computer's invention").

38. *E.g.*, *Catabran*, 836 F.2d at 457.

focused instead on the business records exception to the hearsay rule.[39] As discussed below, proponents may be able to satisfy both authentication and the hearsay exception by meeting the requirements of the latter.[40]

a. Private business records and witness testimony

To prove authenticity, proponents often use the testimony of a witness with knowledge.[41] This method of authentication "contemplates a broad spectrum [including] . . . testimony of a witness who was present at the signing of a document . . . ."[42] For electronic evidence, courts accept witness testimony that the computer generated documents are records that were produced and maintained in the regular course of business.[43] In *United States v. Catabran*,[44] the Ninth Circuit ruled that the trial court properly admitted computerized ledgers and inventories when one of the company's bookkeepers testified that she input sales, inventory, and payroll information on a regular basis and that the printout of those records accurately displayed the information.[45] Similarly, in *United*

39. *See infra* Parts VI.C–D. This hearsay exception may incorporate the authenticity requirement because one prong of the "test" is the trustworthiness of evidence. Gregory P. Joseph, *Internet Evidence II*, NAT'L L.J., July 30, 2001, at B10; *see, e.g.*, United States v. Jackson, 208 F.3d 633, 638 (7th Cir. 2000) (noting that even if Web postings qualified as "business records," they lacked trustworthiness); Rosenberg v. Collins, 624 F.2d 659, 665 (5th Cir. 1980) (holding that computer data compilations "should be treated as any other record of regularly conducted activity" and hence, subject to the business records exception to the hearsay rule).

40. *See infra* notes 180–192 and accompanying text.

41. *See* FED. R. EVID. 901(b)(1); United States v. Henry, 164 F.3d 1304, 1309 (10th Cir. 1999) ("Rule 901(b)(1) provides that a witness with knowledge may authenticate evidence by testifying that a matter is what it is claimed it be."); United States v. Hernandez-Herrera, 952 F.2d 342, 343 (10th Cir. 1991)).

42. FED. R. EVID. 901 advisory committee's note.

43. See *infra* Part VI.C.2 for a discussion of the business records exception to the hearsay rule.

44. 836 F.2d 453 (9th Cir. 1988).

45. *Id.* at 457. Although the Ninth Circuit concluded that the qualified witness laid the foundation required by Rule 803(6), this also would satisfy the requirement of authentication because the proponent demonstrated that this was a witness with knowledge. *See id.* at 458. For a discussion of how courts apply the hearsay rule as the foundational requirement for electronic evidence, see *infra* Parts VI.C–D, E.1.b.

States v. Linn,[46] the Ninth Circuit held that testimony of the hotel's director of communications, who was on duty when a computer record was printed, provided a sufficient foundation for the record.[47]

Other circuits have adopted a similar analysis, requiring that the witness be able to identify the records and their purpose. In *Zayre Corp. v. S.M. & R. Co.*,[48] the Seventh Circuit distinguished between the affidavit of Zayre's controller, which was insufficient to authenticate computer invoices, and the controller's testimony, which was sufficient to establish his knowledge about the printouts in question.[49] Specifically, "[t]he affidavit state[d] nothing about why [the controller] would be familiar with the computer system and data processing procedures that produced the printouts."[50] Moreover, without such knowledge, the witness's title of "controller" was "meaningless" to support authentication.[51] On the other hand, the court noted that the controller's testimony did support authentication because he indicated that he reviewed the printouts and that they accurately reflected the amount in dispute.[52]

Similarly, in *Hardison v. Balboa Insurance Co.*,[53] the Tenth Circuit held that company employees properly authenticated computer generated copies of cancellation notices by identifying them as records produced and maintained in the regular course of business.[54] In that case, an insurance company offered electronic evidence to prove that it cancelled plaintiff's policy before a tornado struck her home.[55] The company's Vice President of Tracking Operations explained in his affidavit how the records were processed

---

46. 880 F.2d 209 (9th Cir. 1989).

47. *Id.* at 216.

48. 882 F.2d 1145 (7th Cir. 1989).

49. *Id.* at 1149–50. The court's discussion here is dicta. *Id.* at 1150. Although the court analyzed authentication in some detail, it did not make a formal ruling on the issue because the defendant failed to raise the objection at trial. *Id.*

50. *Id.* at 1149.

51. *Id.*; *see also* Kurzban, *supra* note 37, at 443 (stating that "[s]uccessful challenges to witnesses' qualifications have all involved witnesses who were ignorant of the procedures involved in the processing of the records they were authenticating.").

52. *Zayre*, 882 F.2d at 1149. In addition, the opposing party failed to call the witness's knowledge into question. *Id.*

53. 4 Fed. Appx. 663 (10th Cir. 2001).

54. *Id.* at 669–70.

55. *Id.* at 665, 669.

and maintained.[56] In addition, answers to the plaintiff's interrogatories provided detailed information about the company's computerized record keeping system.[57] As Rule 901[58] and the above cases demonstrate, a proponent does not need detailed or highly technical testimony to authenticate an electronic record.

b. Public records or reports

At least one court has recognized that public records may also be authenticated with witness testimony.[59] In *United States v. Meienberg*,[60] the Tenth Circuit held that printouts of records kept by the Colorado Bureau of Investigation were properly certified and authenticated under Rule 901(b)(7).[61] Quoting the Advisory Committee, the court noted that "[p]ublic records are regularly authenticated by proof of custody, without more."[62] In this case, the defendant was convicted of selling a firearm in violation of federal and state law.[63] To show that the defendant failed to contact the Bureau for a background check on potential customers and instead recorded phony approval numbers, the government introduced printouts of computerized records with the approval numbers issued by the Bureau.[64]

The defendant argued that the government did not authenticate the evidence because its witness did not verify the accuracy of the

---

56. *Id.* at 669.

57. *Id.* Two of the company's employees verified the answers. *Id.*

58. *See supra* note 42 and accompanying text.

59. United States v. Meienberg, 263 F.3d 1177, 1181 (10th Cir. 2001). To date, no other federal appellate court has considered an objection to the admission of electronic evidence under Rule 901(b)(7). Nonetheless, this rule has been used in a variety of other cases involving public records. *See* United States v. Hernandez-Herrera, 952 F.2d 342, 343–44 (10th Cir. 1991) (Immigration and Naturalization Service records); United States v. Williams, No. 90-5731, 1991 WL 199870, at *11 (4th Cir. Oct. 23, 1991) (unpublished opinion) (certified copy of military pay, leave and earnings statements); Vote v. United States, No. 90-16116, 1991 WL 5487, at *2 (9th Cir. Apr. 12, 1991) (unpublished opinion) (IRS Certificates of Assessment and Payment); United States v. Quezada, 754 F.2d 1190, 1194–95 (5th Cir. 1985) (INS record of deportation).

60. 263 F.3d 1177 (10th Cir. 2001).

61. *Id.* at 1181.

62. *Id.* (citation omitted).

63. *Id.* at 1179.

64. *Id.* at 1180.

printouts.[65] The court disagreed, however, because testimony that the computer printouts reflected the Bureau's record of approval numbers assigned to the defendant's business was "evidence sufficient to support a finding" of the records' authenticity.[66] Moreover, the court noted that public records, including data compilations under Rule 901(b)(7), can be authenticated by testimony that the record "is from the public office where items of this nature are kept."[67]

Public records or reports may also be self-authenticating under Rule 902. Under subsection four of the Rule, copies of public records, "including data compilations in any form," are self-authenticating if they are certified as correct by a "custodian or [an]other person authorized to make the certification.[68] In federal litigation, the most common public records are tax documents offered by the government to prove tax evasion.[69] In many cases, courts have found that computerized tax records are self-authenticating.[70] For instance, in *United States v. Ryan*,[71] the Seventh Circuit held that the government laid a proper foundation for the admission of certified computer records of the United States Treasury Department, which showed that the defendant failed to file his income tax returns.[72] Likewise, a court in the Southern District of California held in *United States v. Boyce*[73] that income tax assessment forms certified by an authorized person were self-authenticating even though they were generated exclusively for

65. *Id.* at 1181.

66. *Id.*; FED. R. EVID. 901(a).

67. *Meienberg*, 263 F.3d at 1181; FED. R. EVID. 901(b)(7).

68. FED. R. EVID. 902(4).

69. While tax records are the most common self-authenticating public records, courts have considered other types of records. For example, in *United States v. Darveaux*, 830 F.2d 124, 125–26 (8th Cir. 1987), the Eighth Circuit ruled that copies of a prior conviction were properly authenticated by the signature of the district court clerk and the seal of the Texas Department of Corrections.

70. *E.g.*, United States v. Gabel, No. C98-04241 SBA, 2002 WL 1396782, at *2 (N.D. Cal. Mar. 26, 2002); United States v. Thurner, 21 Fed. Appx. 477, 478–79 (7th Cir. 2001); United States v. Bisbee, 245 F.3d 1001, 1006–07 (8th Cir. 2001); United States v. Ryan, 969 F.2d 238, 239–40 (7th Cir. 1992); United States v. Boyce, 148 F. Supp. 2d 1069, 1082 (S.D. Cal. 2001).

71. 969 F.2d 238 (7th Cir. 1992).

72. *Id.* at 240.

73. 148 F. Supp. 2d 1069 (S.D. Cal. 2001).

litigation purposes.[74] And, in *United States v. Bisbee*,[75] the Eighth Circuit held that IRS records of a trust fund penalty assessment, along with a certificate attesting to their authenticity, were admissible under Rule 902.[76]

2. Electronic Forensics[77]

In criminal cases,[78] or in cases where electronic files have been deleted or destroyed,[79] parties can use recovery programs and other forensic techniques to capture data that otherwise would be inaccessible to the average computer user. In addition to the foundational requirements discussed above, courts may impose "best practices" and rules regarding expert testimony to control the admissibility of forensic evidence. Although such requirements have been enforced in only a few reported cases, judges are increasingly sophisticated when it comes to their knowledge and analysis of forensic technology.[80] As such, more courts may hold proponents of electronic evidence to high technical standards.

---

74. *Id.* at 1082. The court held the records were authenticated under Rule 902 (1), domestic public documents under seal. *Id.* This rule provides that a document bearing a seal of the agency and a signature purporting to be an attestation or execution thereof satisfies the condition of authenticity. FED. R. EVID. 902(1). The court also held that these records were admissible under the public records exception to the hearsay rule 803(8). *Boyce*, 148 F. Supp. at 1082; *see also infra* Part VI.D (discussing in detail the admissibility of public business records).

75. 245 F.3d 1001 (8th Cir. 2001).

76. *Id.* at 1006–07. In this case, the records were also authenticated under seal of the United States and by signature of attestation. *Id.* at 1006.

77. An entire industry is devoted to providing practitioners and clients with tools for electronic discovery and computer forensics. For an example, visit http://www.krollontrack.com (last visited Feb. 10, 2005).

78. *See infra* notes 92–97, 103–106 and accompanying text.

79. *See infra* notes 99–102 and accompanying text.

80. Some district courts have handled electronic evidence with a remarkably high degree of technical knowledge. For instance, in *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 305–11 (S.D.N.Y. 2000), Judge Kaplan devoted an entire section of his opinion to explaining the process of digital encryption and decompression used to reproduce movies on digital versatile disks, or DVDs.

a. Best practices

Although parties can authenticate electronic business records by traditional means for paper records,[81] a few district courts have suggested "best practices" for authenticating recovered electronic evidence.[82] For instance, in *Gates Rubber Co. v. Bando Chemical Industries, Ltd.*,[83] a Colorado district court concluded that the party offering recovered computer evidence had a duty to use the forensic technology that would "yield the most complete and accurate results."[84] To reach this conclusion, the court considered competing testimony from two computer forensics experts.[85] The plaintiff's expert used a program to retrieve "information . . . about files which were once present on [defendant's] computer's hard drive, but were deleted."[86]

The second expert testified that this method created a "file by file" backup that lost or failed to capture important information on the hard drive because it copied only existing, non-deleted files.[87] Instead, the plaintiff's expert should have used an "image backup" of the hard drive to collect every piece of available information.[88] The second expert also noted that technology for such an image backup, though rarely used, was available at the time of the first hard drive exam.[89] Taking this into account, the court concluded that the plaintiff had "failed to preserve evidence in the most appropriate manner."[90] Because the plaintiff sought to use the electronic information to its evidentiary advantage, the plaintiff—not the defendant—had a duty to use the best technology available to retrieve that information.[91]

---

81. As described above, business records can be authenticated with the testimony of a witness who is responsible for inputting or maintaining the electronic information. *See supra* notes 41–45 and accompanying text.

82. This issue has yet to reach the appellate court level.

83. 167 F.R.D. 90 (D. Colo. 1996).

84. *Id.* at 112.

85. *Id.*

86. *Id.*

87. *Id.*

88. *Id.*

89. *Id.*

90. *Id.*

91. *Id.* at 113.

Similarly, an Oregon district court noted that a forensic examiner may be obligated to use a particular program to narrowly tailor a computer search.[92] Charged with unlawful possession of child pornography, the defendant challenged the need for an offsite search of his eight computers by a forensics expert.[93] The investigating agent who seized the computers testified that, with a certain program, "a computer could be scanned for the presence of child pornography within just a few minutes."[94] However, the agent did not bring this program with him when he searched the defendant's house.[95]

The district court did not find that the government had a duty to use this program because the investigating agent had no way of knowing, before entering the defendant's home, that he would find eight computers instead of one.[96] Nevertheless, the court noted that had there been evidence that a number of computers would be found, the government (and its agents) might have had an obligation to use a

92. United States v. Greathouse, 297 F. Supp. 2d 1264 (D. Or. 2003).

93. *Id.* at 1275.

94. *Id.* at 1269. The investigating agent "explained that there is a computer preview program known as ENCASE that has been available for many years that makes it possible to quickly scan computers for certain information." *Id.*

95. *Id.*

96. *Id.* at 1275. Moreover, case law supports "the wholesale seizure of computers and computer disks and records for later review for particular evidence as the only reasonable means of conducting a search." *Id.*; *see, e.g.*, United States v. Meek, 366 F.3d 705, 715–16 (9th Cir. 2004) (holding that a warrant was sufficiently specific to search computer equipment, computer generated printouts, data storage devices, and documentation of computer hardware because evidence of child exploitation was explicitly described in the supporting affidavit); United States v. Wong, 334 F.3d 831, 837–38 (9th Cir. 2003) (holding that a search warrant including computer equipment was sufficiently specific); Guest v. Leis, 255 F.3d 325, 335 (6th Cir. 2001) (holding that because of the technical difficulties of conducting a computer search in a suspect's home, the seizure of the computers was reasonable to allow police to locate the offending files); United States v. Hay, 231 F.3d 630, 637 (9th Cir. 2000) (holding that search warrant including computer equipment was sufficiently specific and did not need to include all possible locations on computer where child pornography might be found). *But see* United States v. Carey, 172 F.3d 1268 (10th Cir. 1999) (holding that seizure of images of child pornography from defendant's computer hard drive was not authorized by the warrant because the images were in closed files and thus not in plain view).

preview program for a quick, on-site scan of the computer's hard drive.[97]

In ruling on discovery motions, district courts recognize that computer searches "are technical and complex and cannot be limited to precise, specific steps or only one permissible method."[98] But, when it comes to forensic recovery of files from computer hard drives, these same courts often require a "mirror image" copy of the data.[99] For example, in *Playboy Enterprises, Inc. v. Welles*,[100] a court in the Southern District of California ruled that the plaintiff was entitled to discover deleted e-mails on the defendant's computer hard drive.[101] In so ruling, the court appointed a computer expert (who specialized in the field of electronic discovery) to create a "mirror image" of the defendant's hard drive.[102]

In *United States v. Alexander*,[103] the defendant sought access to computer equipment seized from his home so that his expert witness could examine it before trial.[104] The government resisted the discovery motion, arguing that the computer, which allegedly contained obscene images, should not leave government control; if the defense expert wanted to examine the hard drive, he could do so at the Federal Bureau of Investigation ("FBI") office.[105] The court, however, granted the motion, requiring the FBI to furnish the defendant's forensic examiner with a mirror image copy of the computer's hard drive.[106]

---

97. *Greathouse*, 297 F. Supp. 2d at 1275.

98. United States v. Triumph Capital Group, Inc., 211 F.R.D. 31, 47 (D. Conn. 2002); *see also* United States v. IBM, 76 F.R.D. 97 (S.D.N.Y. 1977) (ordering production of electronic data by defendant and appointment of a court examiner "because of the complex and highly technical nature of the information sought").

99. *See Triumph Capital*, 211 F.R.D. at 48 (describing a series of methods used by a forensic expert to recover deleted data from a laptop computer and describing the "mirror image" as an "exact duplicate of the entire hard drive," which "includes all the scattered clusters of the active and deleted files and the slack and free space").

100. 60 F. Supp. 2d 1050 (S.D. Cal. 1999).

101. *Id.* at 1054–55.

102. *Id.* at 1055.

103. No. 04-20005-BC, 2004 WL 2095701 (E.D. Mich. Sept. 14, 2004).

104. *Id.* at *1.

105. *Id.* at *5.

106. *Id.* at *10. Note that the court conditioned the transfer of the mirror image copy on the expert's observance of a prescribed protocol. For instance,

b. Authentication of recovered electronic data

Because of the relative complexity of computer based data recovery, proponents often use—and courts often consider—a wide variety of methods to authenticate electronic forensic evidence. For example, courts will consider expert or non-expert witness testimony[107] or other clues that point to the identity of the evidence.[108] In some instances, courts will allow proponents to authenticate recovered data using a combination of these methods.

i. Expert testimony not required

Like business records, computer forensic evidence can be authenticated by the testimony of a witness with knowledge.[109] Because recovery techniques are technologically complex, "knowledge" may mean that the witness must have a certain level of skill or experience in the field of computer programming. However, federal courts do not require the testimony of an expert trained in forensic investigation. Rather, a witness must only demonstrate personal knowledge of the data recovery process.[110] In the realm of computer forensics, there is little case law on point. Nevertheless, as the following cases illustrate, courts allow proponents to authenticate electronic evidence with the testimony of someone who does not have particular expertise in the field.

In *United States v. Whitaker*,[111] the defendant was charged with conspiracy to distribute marijuana.[112] To prove that he was involved in a trafficking ring, the government offered computer records of the drug transactions.[113] To authenticate the records, the government

---

the examiner was required to maintain a log of any copies of any images that he made from the mirror image copy of the hard drive, and he was required to return the mirror image copy to the FBI at the conclusion of the case. *Id.*

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

108. *Id.* 901(b)(4). Such clues or traces of identity may also be referred to as "circumstantial evidence" in the traditional sense.

109. *Id.* 901(b)(1).

110. As discussed below, under Rule 702, an "expert" may be someone with technical or other specialized knowledge. Therefore, someone with skill or experience in computer programming or forensics—but who lacks formal training—could qualify as an expert. *See infra* notes 140–149 and accompanying text.

111. 127 F.3d 595 (7th Cir. 1997).

112. *Id.*

113. *Id.* at 598.

relied on the testimony of a special agent who was present when the recovery program was installed on the conspirator's computer and the records were retrieved.[114] The defendant argued that the government failed to comply with the requirements of Rule 901(a) because the agent did not have personal knowledge of the computer system's operation.[115] The Seventh Circuit ruled, however, that the agent's testimony was sufficient to establish the authenticity of the computer records of the drug business because the agent testified about his personal participation in obtaining the printouts.[116]

A Michigan district court echoed the Seventh Circuit in *United States v. Scott-Emuakpor*.[117] There, the court ruled that the testimony of a witness did not depend on his expertise or ability to develop a sophisticated software program.[118] The defendant moved to suppress computer evidence obtained from "zip disks" and hard drives seized by federal agents during a search of his home.[119] In so moving, he argued that the testimony of two Secret Service agents who examined the computer equipment and files was insufficient to authenticate because neither of the agents was an expert in the area of computer science.[120] The court denied the defendant's motion, reasoning that, under Rule 901(a), expert testimony is not required for authentication.[121] The court noted that the question was not whether the witnesses had the expertise to develop the sophisticated software programs, but only whether the agents had the skill to find out what was on the hard drive or zip disk.[122] Because the court found "no reason why either witness [could] not testify about what

114. *Id.* at 601.

115. *Id.*

116. *Id.*

117. No. 1:99-CR-138, 2000 U.S. Dist. LEXIS 3118 (W.D. Mich. Jan. 25, 2000). Citing United States v. Whitaker, 127 F.3d 595, 601 (7th Cir. 1997), the court indicated that "the Government may meet the authentication requirement through the testimony of a witness who was present and observed the procedure by which the documents were obtained from Defendant's computers." *Scott-Emuakpor*, 2000 U.S. Dist. LEXIS 3118, at *38–*39.

118. *Scott-Emuakpor*, 2000 U.S. Dist. LEXIS 3118, at *38–*39.

119. *Id.* at *1.

120. *Id.* at *32–*33, *37–*39.

121. *Id.* at *37–*38. Rather, "a proponent need only offer *some* proof showing that a piece of evidence is what the proponent claims it is." *Id.* (emphasis added); *see* FED. R. EVID. 901(a).

122. *Scott-Emuakpor*, 2000 U.S. Dist. LEXIS 3118, at *33.

they did in examining the computer and the results of their examinations," the testimony was admissible for the purposes of authentication.[123]

ii. When experts testify

Although an authenticating witness does not need to be an expert in computer forensics, a proponent may still rely on an expert to translate forensic evidence into a form that can be easily understood by both the court and the jury. Furthermore, because manipulation of electronic data may affect the reliability of the evidence,[124] computer experts may be called on to explain the impact of the retrieval process.[125] Like that of other experts, the testimony of computer forensic examiners must meet standards of reliability and relevancy.[126] Although only a handful of federal cases involve electronic forensics and expert testimony,[127] it is important for litigants to predict whether and how they might offer such testimony to support or challenge the admissibility of electronic evidence.[128]

---

123. *Id.* ("By analogy, a person need not be an expert on English literature in order to know how to read.").

124. *See, e.g.*, United States v. Tank, 200 F.3d 627, 630 (9th Cir. 2000); United States v. Catabran, 836 F.2d 453, 458 (9th Cir. 1988) ("Any question as to the accuracy of the printouts . . . would have affected only the weight of the printouts, not their admissibility.")

125. *See, e.g.*, United States v. Quinn, 18 F.3d 1461, 1464–65 (9th Cir. 1994) (using an expert to explain how the suspect's height was calculated from video surveillance).

126. *See* Daubert v. Merrell Dow Pharms., Inc., 509 U.S. 579 (1993).

127. *See, e.g.*, *Scott-Emuakpor*, 2000 U.S. Dist. LEXIS 3118, at *37; United States v. Whitaker, 127 F.3d 595, 601 (7th Cir. 1997); *Quinn*, 18 F.3d at 1464–65.

128. The key to understanding these issues is the federal courts' role as "gatekeeper" of expert testimony. The need for a "gatekeeper" was first articulated in 1923 in *Frye v. United States*, 293 F. 1013 (D.C. Cir. 1923). In its decision, the Court of Appeals for the District of Columbia presciently noted that "[j]ust when a scientific principle or discovery crosses the line between experimental and demonstrable stages is difficult to define." *Id.* at 1014. Nevertheless, the Court attempted to define that line. For an excellent overview of the evolution of the federal courts' "gatekeeper" function since *Frye*, see Leslie Morsek, Comment, *Get on Board for the Ride of Your Life! The Ups, the Downs, the Twists, and the Turns of the Applicability of the "Gatekeeper" Function to Scientific and Non-scientific Expert Evidence:* Kumho's *Expansion of* Daubert, 34 AKRON L. REV. 689 (2001).

Before 1975, federal courts applied the "general acceptance" test articulated by the Court of Appeals for the District of Columbia in *Frye v. United States*.[129] According to this test, district courts could admit expert testimony only after the proponent "sufficiently established" that the method or principle on which the testimony was based had "gained general acceptance in the particular field in which it belong[ed]."[130] The applicability of *Frye*'s "general acceptance" test was called into doubt when Congress enacted the Federal Rules of Evidence.[131] The Rules expanded the subjects proper for expert testimony and the formats in which experts could testify.[132] In addition, the Rules did *not* incorporate the "general acceptance" test.[133] Nevertheless, many federal courts continued to follow the *Frye* standard, including the Ninth Circuit.[134]

In *Daubert v. Merrell Dow Pharmaceuticals, Inc.*,[135] the United States Supreme Court attempted to clarify the Rules by overruling a Ninth Circuit decision which applied the "general acceptance" test.[136] The Court held that "general acceptance" was not a "precondition to the admissibility of scientific evidence under the Rules of Evidence."[137] Instead, the Court interpreted Rule 702 and held that the trial judge must "ensur[e] that an expert's testimony both rests on a reliable foundation and is relevant to the task at

129. 293 F. 1013 (D.C. Cir. 1923).

130. *Id.* at 1014. This test of "general acceptance" served as the "first procedural barrier to the admission of scientific evidence and expert testimony" in the federal courts. *See* Morsek, *supra* note 128, at 698.

131. *See* Morsek, *supra* note 128, at 700–03.

132. *Id.* at 700 n.48; *see* FED. R. EVID. 702–705.

133. Morsek, *supra* note 128, at 701–02.

134. *Id.* at 703; *see, e.g.*, Christopherson v. Allied-Signal Corp., 939 F.2d 1106, 1110 (5th Cir. 1991) (applying both the *Frye* test and the Federal Rules of Evidence); United States v. Two Bulls, 918 F.2d 56, 60 (8th Cir. 1990) ("Rule 702 and *Frye* both require the same general approach to the admissibility of new scientific evidence."); United States v. Gillespie, 852 F.2d 475, 480 (9th Cir. 1988) ("Evidence that does not qualify under *Frye* must be excluded."); United States v. Shorter, 809 F.2d 54, 60 (D.C. Cir. 1987) ("*Frye* is still the law in this Circuit."); United States v. Solomon, 753 F.2d 1522, 1526 (9th Cir. 1985) (noting the *Frye* test as the proper standard for admissibility of evidence based on a novel scientific technique).

135. 509 U.S. 579 (1993).

136. *Id.* at 584, 597.

137. *Id.* at 597.

hand."[138] Yet, before the trial judge engages in these "gatekeeper" duties, two threshold questions must be answered: First, how can a witness qualify as an "expert" under the Federal Rules? And second, if the district courts' gatekeeping function applies to the admission of scientific evidence, does it also apply to the admission of non-scientific expert evidence?[139]

(a) How can a witness qualify as an "expert"?

To answer the first question, litigants can look to Rule 702's broadly phrased definition of "expert":[140]

> The fields of knowledge which may be drawn upon are not limited merely to the "scientific" and "technical" but extend to all "specialized" knowledge. Similarly, the expert is viewed, not in a narrow sense, but as a person qualified by "knowledge, skill, experience, training or education." Thus within the scope of the rule are not only experts in the strictest sense of the word, e.g., physicians, physicists, and architects, but also the large groups sometimes called "skilled" witnesses, such as bankers or landowners testifying to land values.[141]

With this Rule, Congress opened the door to testimony from a wide range of witnesses with skill or experience in computer forensics. For instance, although the court in *United States v. Whitaker*[142] did not explicitly address the qualifications of the witness as an "expert," it noted that the government established a foundation for forensic evidence when an FBI agent testified about his role in installing the retrieval program and subsequently obtaining the data printouts.[143]

In addition, at least one circuit court has recognized that expert testimony in the field of electronic evidence does not demand the use

---

138. *Id.*

139. *See* Morsek, *supra* note 128, at 719.

140. FED. R. EVID. 702.

141. *Id.* 702 advisory committee's note.

142. 127 F.3d 595 (7th Cir. 1997).

143. *Id.* at 601. And, as discussed earlier, the court in *United States v. Scott-Emuakpor*, No. 1:99-CR-138, 2000 U.S. Dist. LEXIS 3118, at *33 (W.D. Mich. Jan. 25, 2000) held that "expertise" in computer forensics did not require the witness to know how to develop a sophisticated software program. Rather, the witness only had to have the skill to find out what was on a hard drive or zip drive. *Id.*

of "scientific" techniques. In *United States v. Quinn*,[144] the lower court admitted testimony of a photogrammetry expert, who calculated the height of a bank robber using computer and video surveillance.[145] The Ninth Circuit held that the testimony was properly admitted because the lower court, applying Rule 702 and the *Daubert* standard, could conclude that the expert's testimony was reliable, even though it was based on a "series of computer-assisted calculation[s] that did not involve any novel or questionable *scientific technique*."[146]

As these cases illustrate, proponents of forensic evidence are not strictly limited by the credentials or techniques of their proposed expert witnesses. This does not mean, however, that the trial court will simply "tak[e] the expert's word for it."[147] "If the witness is relying solely or primarily on experience, then the witness must explain how that experience leads to the conclusion reached, why that experience is a sufficient basis for the opinion, and how that experience is reliably applied to the facts."[148] Nevertheless, the breadth of expert qualification under Rule 702 is particularly beneficial for proponents of forensic computer evidence because experience may be the predominant (or the only) basis for reliable testimony.[149]

---

144. 18 F.3d 1461 (9th Cir. 1994).

145. *Id.* at 1464.

146. *Id.* at 1465 (emphasis added).

147. FED. R. EVID. 702 advisory committee's note.

148. Daubert v. Merrell Dow Pharms., Inc., 43 F.3d 1311, 1399 (9th Cir. 1995), *vacated by* 509 U.S. 579 (1993); FED. R. EVID. 702 advisory committee's note.

149. *See* FED. R. EVID. 702 advisory committee's note; *see also* United States v. Jones, 107 F.3d 1147, 1161 (6th Cir. 1997) (finding no abuse of discretion in admitting the testimony of a handwriting examiner with years of practical experience and extensive training); Tassin v. Sears Roebuck, 946 F.Supp. 1241, 1248 (M.D. La. 1996) (holding that a design engineer's testimony was admissible when opinions were based in part on technical and mechanical expertise). In addition, qualification of a witness as an "expert" will raise strategic considerations, such as the cost of the witness and the jury's perception of an "expert" as perhaps more credible than other witnesses.

(b) Are district courts "gatekeepers" for non-scientific expert evidence?

Congress and the Supreme Court only recently answered the second question. While *Daubert* provided some guidance for federal judges in their "gatekeeper role," it did little or nothing to define the scope of an expert's testimony. In a footnote of the opinion, the Court recognized that Rule 702 also applies to "technical, or other specialized knowledge," but it limited its discussion to the scientific context, based on the nature of the testimony offered in that case.[150] Although no cases involving electronic evidence raised the issue of *Daubert*'s applicability to non-scientific testimony,[151] courts struggled with this distinction in other areas of expert testimony.[152] Some courts restricted *Daubert* to scientific evidence,[153] while others reasoned that *Daubert* was equally applicable to non-scientific evidence.[154]

Six years after *Daubert*, the Supreme Court weighed in on the conflict. In *Kumho Tire Co., Ltd., v. Carmichael*,[155] the Court held that although *Daubert* is not a "definitive checklist or test," the gatekeeping function of district courts applies to both "scientific" and "technical" or "other specialized" knowledge.[156] To further

---

150. *Daubert*, 509 U.S. at 590 n.8.

151. Although the court in *Scott-Emuakpor* does not expressly state so, it suggests that a witness without scientific expertise may nevertheless qualify as an "expert" and hence the "non-scientific" testimony of this expert may be weighed under a *Daubert* analysis: "The fact that Agent Christy admitted that he is not an expert in the area of computer science is not binding on the Court in performing its Daubert gatekeeping function as recently extended by the Supreme Court in Kumho Tire Co. v. Carmichael." 2000 U.S. Dist. LEXIS 3118, at *33 (citations omitted).

152. Morsek, *supra* note 128, at 720.

153. *See, e.g.*, Carmichael v. Samyang Tire, Inc., 131 F.3d 1433, 1436 (11th Cir. 1997); McKendall v. Crown Control Corp., 122 F.3d 803, 806–08 (9th Cir. 1997); United States v. Jones, 107 F.3d 1147, 1158 (6th Cir. 1997); Compton v. Subaru of Am., Inc., 82 F.3d 1513, 1518 (10th Cir. 1996); Iacobelli Const., Inc. v. County of Monroe, 32 F.3d 19, 25 (2d Cir. 1994).

154. *See, e.g.*, Wakins v. Telsmith, 121 F.3d 984, 988 (5th Cir. 1997); Cummins v. Lyle Indus., 93 F.3d 362, 368 (7th Cir. 1996).

155. 526 U.S. 137 (1999).

156. *Id.* at 138. The Court explained that Rule 702 "grant[s] all expert witnesses, not just 'scientific' ones, testimonial latitude unavailable to other witnesses." *Id.* Thus, courts do not have to administer evidentiary rules based on the kind of expert testimony or knowledge presented, because there is often

elucidate the courts' gatekeeping role, and in response to *Daubert* and *Kumho Tire*, Congress amended Rule 702 in 2000.[157] The Rule is now consistent with *Kumho*, providing that "all types of expert testimony present questions of admissibility for the trial court in deciding whether the evidence is reliable and helpful."[158] Further, it is intended to encompass and supersede a *Daubert* analysis: "The standards set forth in the amendment are broad enough to require consideration of any or all of the specific Daubert factors where appropriate."[159]

At least in theory, Rule 702 is important to the use of electronic evidence because experts often testify about non-scientific issues, such as the interpretation of computer records of a suspected drug trafficking business.[160] To date, no federal court presented with electronic evidence has drawn a distinction between expert testimony involving scientific knowledge and expert testimony involving non-scientific knowledge. Given Rule 702's flexibility and broad applicability to other types of evidence,[161] it is unlikely that courts will make such a distinction. Nevertheless, proponents must still be cognizant of the requirements of Rule 702.[162]

---

no clear line between what is "scientific" and what is merely "technical" or "other specialized" knowledge. *Id.*

157. FED. R. EVID. 702 advisory committee's note.

158. *Id.*

159. *Id.* Rule 702 now provides that an expert may testify if three requirements are met: "(1) the testimony is based upon sufficient facts or data, (2) the testimony is the product of reliable principles and methods, and (3) the witness has applied the principles and methods reliably to the facts of the case." FED. R. EVID. 702.

160. *See* United States v. Whitaker, 127 F.3d 595, 601–02 (7th Cir. 1997) (stating that a federal agent testified as an expert to interpret computer generated drug records).

161. FED. R. EVID. 702 advisory committee's note. Moreover, non-*Daubert* factors might also be relevant to determining whether expert testimony is sufficiently reliable. *Id.*; *see, e.g.*, Sheehan v. Daily Racing Form, Inc., 104 F.3d 940, 942 (7th Cir. 1997) (noting that the expert was not as careful as he would be in regular paid professional work); Claar v. Burlington N. R.R., 29 F.3d 499, 502 (9th Cir. 1994) (excluding testimony where the expert failed to consider other obvious causes of the plaintiff's condition).

162. FED. R. EVID. 702 advisory committee's note.

iii. Authentication by other methods

Because the authentication methods mentioned in Rule 901(b) are not exclusive, proponents of electronic evidence do not have to prove authentication by any particular method.[163] They are free to use any method or combination of methods that will provide evidence sufficient to support a finding of authenticity. In addition, a proponent may authenticate evidence by its "[a]ppearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances."[164] In other words, proponents can rely on circumstantial evidence of authenticity. Given the low burden of proof for authentication and courts' general acceptance of electronic evidence, it is not surprising that courts have adopted a flexible approach.

In *United States v. Simpson*,[165] the defendant argued that a computer printout of an alleged chat room discussion between an FBI agent and himself was not authenticated because the government could not identify the statements attributed to the defendant by his handwriting, writing style, or voice.[166] The Tenth Circuit rejected this argument, concluding instead that these specific examples of authentication were "merely illustrative . . . and [were] not intended as an exclusive enumeration of allowable methods of authentication."[167] The court held that the government properly authenticated the chat room printout, using a variety of facts: the printout of the chat room discussion revealed the screen name the defendant gave to the agent as well as the defendant's street address; the discussion included an e-mail address belonging to the defendant; and pages found near the computer in the defendant's home contained a notation of the name, street address, e-mail address, and telephone number the agent gave to the individual in the chat room.[168]

---

163. *See supra* notes 20–25 and accompanying text.

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

165. 152 F.3d 1241 (10th Cir. 1998).

166. *Id.* at 1249. The defendant referred to Rule 901(b)(2) through (5). *Id.* Subsection 2 provides for a nonexpert opinion as to the genuineness of handwriting; subsection 3 provides for comparison of specimens by the trier of fact or expert witness; subsection 4 provides for circumstantial evidence; and subsection 5 provides for voice identification. FED. R. EVID. 901(b)(2)–(5).

167. *Simpson*, 152 F.3d at 1249–50.

168. *Id.* at 1250.

Likewise, in *United States v. Tank*,[169] the Ninth Circuit held that the government adequately established a connection between the defendant and chat room log printouts.[170] Without citing a particular subsection of Rule 901, the court concluded that the logs were authenticated, based on testimony of a co-conspirator who described how the logs were created and who identified them as accurate representations of the chat room discussions.[171] In addition, the court pointed to evidence that defendant participated in these conversations: his screen name, "Cessna," appeared on the chat room printouts, and when participants arranged a meeting with the person who used the screen name "Cessna," the defendant showed up.[172]

The Eleventh Circuit has also adopted a flexible approach for authentication of electronic evidence. In *United States v. Siddiqui*,[173] the court determined that the government properly authenticated an e-mail message, using circumstantial evidence.[174] For instance, the message bore the defendant's e-mail address at the University of South Alabama, and when the recipient replied, the reply function in his e-mail system automatically sent a message to the defendant's address as the sender.[175] In addition, the message referred to the author as "Mo," the defendant's nickname, and when the recipient finally spoke to the defendant on the phone, he made the same requests made in the e-mail message.[176]

---

169. 200 F.3d 627 (9th Cir. 2000).
170. *Id.* at 630.
171. *Id.*
172. *Id.* at 630–31.
173. 235 F.3d 1318 (11th Cir. 2000).
174. *Id.* at 1322 (citing FED. R. CIV. P. 901(b)(4)); *see also* United States v. Reilly, 33 F.3d 1396, 1403–09 (3d Cir. 1994) (holding that a series of radiotelegrams were properly authenticated based on a combination of testimony and other circumstantial features); Mark D. Robins, *Evidence at the Electronic Frontier: Introducing E-Mail at Trial in Commercial Litigation*, 29 RUTGERS COMPUTER & TECH. L.J. 219, 229–30 (2003) (describing *Reilly* as an example of authenticating a chain of communications using Rule 901(b)(4)).
175. *Siddiqui*, 235 F.3d at 1322.
176. *Id.* at 1323.

C. Foundations for Electronic Evidence: Private Business Records & the Hearsay Exception

After crossing the first admissibility hurdle, a proponent may next face a hearsay objection. Since electronic business records are written assertions or communications made outside of court, they constitute hearsay when offered in evidence to prove the truth of the matter asserted.[177] However, Federal Rule 803(6) includes an exception for business records,[178] based on reliability and the need for a cumulative source of information.[179]

If electronic records are "unreliable," then they are probably inadmissible on both authenticity *and* hearsay grounds. This is so because the business records exception to the hearsay rule effectively incorporates an authentication requirement.[180] In particular, if all other requirements for the exception are met,[181] business records are admissible, "unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness."[182] This criterion is analogous to the Rule 901(a) requirement that there must be "evidence sufficient to support a finding that the matter in question is what its proponent claims."[183] Thus, evidence that is excluded on authenticity grounds should also be excluded as hearsay.[184]

With this in mind, some courts bypass an explicit authenticity analysis and instead look to the requirements of the hearsay exception to determine whether the proponent has established a proper foundation.[185] Courts do so not because of the more stringent requirements of the exception, but rather because they recognize computers as inherently reliable.[186] In fact, at least one court has stated that electronic evidence has "a prima facie aura of

177. *See* FED. R. EVID. 801.
178. *Id.* 803(6).
179. DAVID P. LEONARD & VICTOR J. GOLD, EVIDENCE: A STRUCTURED APPROACH 223 (2004).
180. *See* Joseph, *supra* note 39, at B10.
181. *See infra* notes 202–205 and accompanying text.
182. FED. R. EVID. 803(6); *see id.* 803(8).
183. *Id.* 901(a).
184. *See* Joseph, *supra* note 39, at B10.
185. For this and further criticism of the approach, see Givens, *supra* note 9, at 106–08.
186. *See id.* at 106.

reliability."[187] Thus, courts primarily concern themselves with whether electronic records meet other requirements of the hearsay exception, e.g., whether the records are kept in the course of a regularly conducted business activity.

Because requirements for the hearsay exception may be duplicative of those for authentication, it may be more efficient for litigants and courts to consider only the business records exception.[188] Specifically, the authenticity and hearsay exception analyses dovetail when a person with knowledge of the records testifies.[189] Although the Rules do not require it, a proponent *may* choose to authenticate electronic records with the testimony of a witness with knowledge.[190] However, as discussed below, the proponent *must* lay the foundation for the hearsay exception with a "person with knowledge."[191] Hence, a proponent could simultaneously satisfy the requirement of authentication and at least one of the requirements of the hearsay exception with witness testimony.[192]

1. Rule 803(6): Electronic or Paper?

When a proponent offers business records into evidence under the hearsay exception, a court will generally accept the records in electronic format.[193] Thus, whether a business record is maintained in a company computer or among the company's printed records is often immaterial to the court's analysis.[194] This is consistent with

187. Canadyne-Georgia Corp. v. Bank of Am., N.A., 174 F. Supp. 2d 1337, 1343 (M.D. Ga. 2001) (citing Olympic Ins. Co. v. H.D. Harrison, Inc., 418 F.2d 669, 670 (5th Cir. 1969)).

188. *See id.*; United States v. Whitaker, 127 F.3d 595 (7th Cir. 1997). There is a parallel trend in state courts. *See, e.g.*, People v. Lugashi, 205 Cal. App. 3d 632 (1988); People v. Huehn, 53 P.3d 733 (Colo. Ct. App. 2002); *see also* Givens, *supra* note 9, at 106 (suggesting that proponents of electronic evidence need not prove both foundational elements).

189. *See infra* Part VI.C.2.a.

190. *See supra* notes 20–21 and Part VI.B.1.a.

191. *See infra* Part VI.C.2.a.

192. As discussed below, there are other requirements that must be met before a court will admit a business record under the hearsay exception in 803(6). *See infra* Parts VI.C.2.b–c.

193. *See supra* notes 32–37 and accompanying text.

194. Over thirty years ago, the Ninth Circuit noted that "it is immaterial that the business record is maintained in a computer rather than in company books," assuming that a proper foundation is laid. United States v. De

Rule 803(6), which provides that a business record may be "[a] memorandum, report, record, or *data compilation*, in any form."[195] Accordingly, courts have found that a variety of computer generated records or forms fall within the exception. For instance, federal courts have admitted bills of lading,[196] Federal Express delivery records,[197] Medicaid claim forms,[198] insurance cancellation notices,[199] and memos of telephone conversations under Rule 803(6).[200]

2. Laying the Foundation

Like all types of evidence, computerized records are admissible only after the proponent establishes a sufficient foundation for their introduction. Rule 803(6) sets out several foundational elements for business records.[201] Although courts interpret these elements in various ways, they generally agree on three requirements.[202] First, a

---

Georgia, 420 F.2d 889, 893 n.11 (9th Cir. 1969). More recently, the Ninth Circuit noted that the use of a computer ledger does not change the result when the ledger is offered as evidence of the company's inventory and payroll. United States v. Catabran, 836 F.2d 453, 456–57 (9th Cir. 1988); *see also* Sea-Land Serv., Inc., v. Lozen Int'l, LLC, 285 F.3d 808, 819 (9th Cir. 2002) (concluding that electronic bills of lading are business records under the hearsay exception); United States v. Layne, 1994 U.S. App. LEXIS 9375, *17 (6th Cir. Apr. 19, 1994) (stating that computers do not need to be "tested for programming errors before computer records are admitted" (quoting United States v. Moore, 923 F.2d 910, 915 (1st Cir. 1991)).

195. FED. R. EVID. 803(6) (emphasis added). According to the Advisory Committee, "data compilation" is "broadly descriptive of any means of storing information other than the conventional words and figures in written or documentary form." The Committee also states that this is "by no means limited to . . . electronic computer storage." *Id.* advisory committee's note. As described above, this may open the door to new types of electronic evidence, like cellular tower and electronic toll booth records. *See also supra* note 5 and accompanying text (discussing potential application of the Federal Rules to new digital and electronic technologies).

196. *Sea-Land Serv. Inc.*, 285 F.3d at 819–20.

197. Dino Constr. Co. v. McWane, Inc., 198 F.3d 567, 575–76 (6th Cir. 1999).

198. United States v. Sanders, 749 F.2d 195, 197–98 (5th Cir. 1984).

199. Hardison v. Balboa Ins. Co., 4 Fed. Appx. 663, 669–70 (10th Cir. 2001).

200. United States v. Goodchild, 25 F.3d 55, 61–62 (1st Cir. 1994).

201. FED. R. EVID. 803(6).

202. According to *United States v. Catabran*, 836 F.2d 453, 457 (9th Cir. 1988),

foundation for the hearsay exception must be established by someone who demonstrates sufficient knowledge of the record-keeping system.[203] Second, the records must be "kept in the course of a regularly conducted business activity." [204] Third, the source of information and the method of preparation must be trustworthy.[205]

a. A person with sufficient knowledge

Before a court will admit electronic business records as evidence, a witness must describe how the records were created and maintained.[206] As early as 1980, the Fifth Circuit recognized that a foundational witness need only be in a position to attest to the authenticity of the electronic records.[207] In addition, the witness does

---

> [t]he proponent of the business records must satisfy the foundational requirements of the business records exception. [Rule] 803(6) allows for the admission of business records when they are: (1) made or based on information transmitted by a person with knowledge at or near the time of the transaction; (2) made in the ordinary course of business; and (3) trustworthy, with neither the source of information nor method or circumstances of preparation indicating a lack of trustworthiness.

Other courts have adopted a slightly different approach to the exception. For instance, the Tenth Circuit considers computer business records admissible if: "(1) they are kept pursuant to a routine procedure designed to assure their accuracy, (2) they are created for motives that tend to assure accuracy (*e.g.*, not including those prepared for litigation), and (3) they are not themselves mere accumulations of hearsay." United States v. Cestnik, 36 F.3d 904, 909–10 (10th Cir. 1994); *see* United States v. Hernandez, 913 F.2d 1506, 1512 (10th Cir. 1990). The Tenth Circuit follows the approach taken by the Eleventh and Fifth Circuits. *E.g.*, United States v. Glasser, 773 F.2d 1553, 1559 (11th Cir. 1985); Capital Marine Supply, Inc. v. M/V Roland Thomas, II, 719 F.2d 104, 106 (5th Cir. 1983); Rosenberg v. Collins, 624 F.2d 659, 665 (5th Cir. 1980); United States v. Fendley, 522 F.2d 181, 184 (5th Cir. 1975).

203. *Catabran*, 836 F.2d at 457; FED. R. EVID. 803(6).

204. FED. R. EVID. 803(6); *see also Catabran*, 836 F.2d at 457 (explaining foundational requirements for the business records exception).

205. *Catabran*, 836 F.2d at 457; *see* FED. R. EVID. 803(6).

206. *See* United States v. Miller, 771 F.2d 1219, 1237 (9th Cir. 1985); Casamassima & Caplicki, *supra* note 6, at 14. In some cases, a business record may be self-authenticating. Instead of presenting a qualified witness, the proponent may present certification of regularly conducted activity that complies with Rule 902(11) (domestic records), Rule 902(12) (foreign records), or with a statute that permits such certification. FED. R. EVID. 902.

207. Rosenberg v. Collins, 624 F.2d 659, 665 (5th Cir. 1980) (finding that testimony of the company's comptroller was "sufficient to lay the proper predicate for the admission of the records"). This too illustrates overlap

not need to know how the computer program works, nor must the witness be the one who personally prepared the records.[208] For instance, in *United States v. Catabran*,[209] the Ninth Circuit ruled that a printout of a company's ledger was admissible where the bookkeeper testified that she "put into the computer sales, inventory, payroll, and tax information on a current basis."[210]

Proponents of electronic business records can rely on a variety of witnesses, from any level of an organization's hierarchy. For example, courts in both the Ninth and Tenth Circuits have accepted testimony of upper management that the records were part of the company's business activities. In *Hardison v. Balboa Insurance Co.*,[211] the Tenth Circuit concluded that the vice-president of tracking operations satisfied this foundational requirement when, in her affidavit, she stated that she was "competent to testify about the computer system that created the documents and she explained how data was entered and retrieved from the system."[212] Similarly, in *Sea-Land Service, Inc. v. Lozen International*,[213] the Ninth Circuit held that a shipping company's manager of documentation was a qualified witness under 803(6) because she had sufficient knowledge to testify that computer records "did in fact contain the true and correct terms and conditions of [the company's] bills of lading."[214]

b. Kept in the course of business

A witness with knowledge may also help satisfy the second requirement for the hearsay exception. That is, the witness may testify that the records were "kept in the course of a regularly conducted business activity,"[215] and that "it was the regular practice of that business activity to make the . . . record, or data

---

between authentication and the hearsay exception. If a witness with knowledge can testify as to the authenticity of the record, then he has also properly authenticated it under FED. R. EVID. 901(b)(1), meaning that the witness has shown the matter to be what it is claimed to be.

208. *Rosenberg*, 624 F.2d at 665.
209. 836 F.2d 453 (9th Cir. 1988).
210. *Id.* at 457.
211. 4 Fed. Appx. 663 (10th Cir. 2001).
212. *Id.* at 670.
213. 285 F.3d 808 (9th Cir. 2002).
214. *Id.* at 820.
215. FED. R. EVID. 803(6).

compilation."[216] The purpose of this requirement is to ensure the reliability of the evidence, via a duty to make *and* regularly maintain such records.[217] Proponents satisfy this requirement with little difficulty because they need not use these records in any particular way or for any particular purpose. For instance, in *Catabran*, the defendant argued that computer printouts were not made in the ordinary course of business because he did not rely on them for inventory purposes; rather, they were used for financial reporting and to secure loans.[218] However, the court rejected this argument, stating that Rule 803(6) does not require that a business use the document in such a specific way.[219]

In addition, electronic business records do not have to be the result of an automated process or regular data entry. For instance, in *United States v. Goodchild*,[220] the First Circuit held that computer printouts of memos made by a credit card company's collection personnel during telephone calls to cardholders were properly admitted under 803(6).[221] The court concluded that the records met "the strictures of the rule" since they were made either during the telephone calls or immediately thereafter.[222] Moreover, the memos were made during the course of a regularly conducted business activity, i.e., investigations of delinquent credit card accounts, and it was the regular practice of the collections personnel to make a record of these calls.[223]

Although a business does not have to rely on electronic documents or records for any particular purpose, records may be inadmissible if they are made or printed solely for the purposes of

---

216. *Id.*

217. *See, e.g.*, Kassel v. Gannett Co., 875 F.2d 935, 945 (1st Cir. 1989); Willco Kuwait (Trading) S.A.K. v. deSavary, 843 F.2d 618, 628 (1st Cir. 1988); United States v. Ferber, 966 F. Supp. 90, 98 (D. Mass. 1997).

218. United States v. Catabran, 836 F.2d 453, 457 (9th Cir. 1988).

219. *Id.*

220. 25 F.3d 55 (1st Cir. 1994).

221. *Id.* at 62.

222. *Id.*

223. *Id.* The court also noted that the manager of the fraud department was a witness qualified to explain the memos. *Id.* Even though he did not record the memos himself, he "understood both the procedure followed by collections in investigating delinquent accounts and the records required to be kept of such investigations." *Id.*

litigation.[224] For instance, in *Potamkin Cadillac v. B.R.I. Coverage Corp.*,[225] the Second Circuit found inadmissible a computer generated history of insurance premiums that had been prepared at the request of counsel.[226] The Seventh Circuit in *United States v. Blackburn*[227] also refused to find that reports specifically prepared for the FBI were admissible under the hearsay exception.[228] In that case, a robbery suspect left a pair of eyeglasses on the front seat of a stolen automobile used to escape from the crime scene.[229] At the request of the FBI, a company that manufactured custom eyeglasses prepared an analysis of the prescription for the lenses, and the district court admitted the computer printouts of the lensometer readings as a record of regularly conducted activity.[230] However, the court of appeals held that the record was inadmissible because it was "specially prepared at the behest of the FBI and with the knowledge that any information it supplied would be used in an ongoing criminal investigation."[231]

In contrast, courts will admit business records that have been extracted from electronic files and printed for litigation purposes, as long as the original data compilation was prepared according to a business practice.[232] The Sixth Circuit held in *United States v. Russo*[233] that the computer printout of an insurance claim was admissible, even though it was made months after the claim was filed: "Since the computer printout is just a presentation in structured and comprehensible form of a mass of individual items, it is immaterial that the printout itself was not prepared until 11 months

224. This problem arises because Rule 803(6) states that, to be admissible, a business record of "acts, events, conditions, opinions, or diagnoses" must be "made at or near the time" of that event or condition. FED. R. EVID. 803(6).

225. 38 F.3d 627 (2d Cir. 1994).

226. *Id.* at 632–33. The court also held that the record was inadmissible as a business record because it constituted attorney work product. *Id.*

227. 992 F.2d 666 (7th Cir. 1993).

228. *Id.* at 670.

229. *Id.* at 669–70.

230. *Id.* at 670.

231. *Id.*

232. *See* Casamassima & Caplicki, *supra* note 6, at 15 ("Because the computer records offered at trial are often printed out solely for the trial, a party may object to the introduction of the printouts, based on the fact that the printouts were not contemporaneous with the events recorded on the computer . . . .").

233. 480 F.2d 1228 (6th Cir. 1973).

after the close of the year[]."[234] The court also noted that it would too severely restrict the admissibility of computerized records if the computer printout—as well as the input on which it was based—had to be produced at or within a reasonable time after the related transaction.[235]

The Seventh Circuit echoed this conclusion almost twenty years later in *United States v. Briscoe*.[236] There, the court noted in dicta that although the computer printouts of telephone call data were prepared specifically for that case, it was "sufficient that the data compiled in the printouts was entered into the computer contemporaneous with the placing of each telephone call."[237] Citing *Briscoe*, the Seventh Circuit in *United States v. Fujii*[238] held that an airline's reservation and check-in records were also admissible under the hearsay exception.[239] Even though the printouts of the records were made specifically for trial, it was the regular business practice of the airline to make the entries into the computer system, and the records were kept as part of the airline's regular business activity.[240] Likewise, the Tenth Circuit in *United States v. Hernandez*[241] held that immigration service printouts reflecting the defendant's amnesty status were admissible because the original computer data compilation was made "pursuant to a business duty in accordance with regular business practice."[242] That the printout was made for the purposes of litigation did not affect the records' admissibility.[243]

c. Trustworthiness

Before a court will admit a business record under the hearsay exception, the proponent must demonstrate that the underlying source of information and the method or circumstances of

234. *Id.* at 1240.
235. *Id.*
236. 896 F.2d 1476 (7th Cir. 1990).
237. *Id.* at 1494 n.13.
238. 301 F.3d 535 (7th Cir. 2002).
239. *Id.* at 539.
240. *Id.*
241. 913 F.2d 1506 (10th Cir. 1990).
242. *Id.* at 1512.
243. *Id.*

preparation are trustworthy.[244] Federal courts have rejected the argument that computer based records are inherently less trustworthy than paper records and thus in need of a more solid foundation.[245] For instance, in *United States v. Catabran*, the defendant argued that the lower "court erred in admitting [computer inventory] printouts because they were inaccurate and therefore untrustworthy."[246] He argued that the inaccuracy could have resulted from an error in data entry or from the computer program itself, which applied an automatic markup to the inventory figures.[247] The Ninth Circuit, however, concluded that the records were appropriately admitted because the witness who input the data testified that she double-checked her figures, and she could (and did) override the automatic markup function of the computer program.[248]

Importantly, the security of computer systems and their vulnerability to manipulation has not posed a significant problem for the admission of computer based records. For instance, in *United States v. Glasser*,[249] the defendant challenged the security of the computer system, but the court held that "[t]he existence of an air-tight security system is not a prerequisite to the admissibility of

244. FED. R. EVID. 803(6). Soon after the Federal Rules were enacted in 1975, "federal judges substantially agree[d] that computer output should be qualified like any other business record." Peritz, *supra* note 6, at 958. Peritz also notes that judicial consensus evolved "despite the fact that computer systems store, retrieve, and manipulate information in ways significantly different from earlier manual or mechanical systems." *Id.* at 958.

245. *See* United States v. Moore, 923 F.2d 910, 915 (1st Cir. 1991) (stating that "ordinary business circumstances . . . suggest trustworthiness"); United States v. Briscoe, 896 F.2d 1476, 1494–95 (7th Cir. 1990) (stating that a proponent of computer generated records need only "provide[] sufficient facts to warrant a finding that the records are trustworthy"); United States v. Young Bros., Inc., 728 F.2d 682, 693–94 (5th Cir. 1984) (rejecting the argument that computer generated records are less reliable than paper records and hence, in need of greater foundation); *see also* Kurzban, *supra* note 37, at 444–45 (describing this as the current federal standard).

246. 836 F.2d 453, 458 (9th Cir. 1988).

247. *Id.*

248. *Id.* The court went on to state that "[a]ny question as to the accuracy of the printouts . . . as with inaccuracies in any other type of business records, would have affected only the weight of the printouts, not their admissibility." *Id.* As this case illustrates, the testimony of one qualified witness can satisfy all the requirements of the business records exception.

249. 773 F.2d 1553 (11th Cir. 1985).

computer printouts."[250] Similarly, the Fifth Circuit in *United States v. Hutson*[251] ruled that computer printouts were trustworthy enough to be admitted in an embezzlement prosecution because access to the system was limited by the use of a special code.[252]

However, in recent cases involving the Internet, courts have been more skeptical of the source or method of preparation of evidence.[253] In *United States v. Jackson*, for example, the defendant tried to admit Web postings of alleged white supremacist groups, arguing that they were "business" records of the groups' Internet Service Providers.[254] The Seventh Circuit flatly rejected her argument, stating that Internet Service Providers are "merely conduits" which do not monitor the contents of Web sites.[255] Moreover, the court noted that "[t]he fact that the Internet Service Providers may be able to retrieve information that [their] customers posted or email that [their] customers sent does not turn that material into a business record . . . ."[256]

Thus, for regular, non-Internet based electronic records, fulfilling the normal foundational requirements, e.g., providing the testimony of a witness with knowledge and demonstrating the accuracy of the records, may expose any underlying manipulation or falsification. Yet where Internet or Web postings are offered as business records, courts may need to take a closer look at their trustworthiness. To date, no federal court has held that Web pages or Internet postings are "business records" according to the Rule 803(6) hearsay exception.[257]

---

250. *Id.* at 1559. The court also concluded that if such a system of security was a prerequisite to admissibility, "it would become virtually impossible to admit computer generated records; the party opposing admission would have to show only that a better security system was feasible." *Id.*

251. 821 F.2d 1015 (5th Cir. 1987).

252. *Id.* at 1020; *cf.* United States v. Tafoya, 757 F.2d 1522, 1528–29 (5th Cir. 1985) (holding billing memoranda were still admissible, even though they were sometimes falsified).

253. United States v. Jackson, 208 F.3d 633, 637 (7th Cir. 2000); St. Clair v. Johnny's Oyster & Shrimp, Inc., 76 F. Supp. 2d 773, 774–75 (S.D. Tex. 1999).

254. *Jackson*, 208 F.3d at 637.

255. *Id.*

256. *Id.*

257. However, data-driven functions on Web sites, e.g., online sales transactions, might meet the requirements of the hearsay exception, whereas "static" data, such as .html postings, might not.

D. Public Records

The records of public agencies or offices must also be supported by a proper evidentiary foundation. As with private business records, courts apply more than one standard for determining whether the proponent has satisfied this requirement. As discussed above, public records may be authenticated under Rule 901(b)(7), or they may be self-authenticating under Rule 902.[258] Once authenticated, these records are subject to a hearsay objection *and* a hearsay exception: computer records of a public office or agency may be admitted under the hearsay exception of Rule 803(8).[259] Unlike private business records, public records may be admitted without the testimony of a custodian or other qualified witness.[260] Underlying this rule is the assumption that public officials will perform their duties properly, but will not remember the details of countless, unspecified records.[261]

Not surprisingly, the federal government often seeks to introduce computer printouts of tax records to support allegations of tax evasion. Courts generally admit tax records under part of the public records hearsay exception that covers "matters observed pursuant to [a] duty imposed by law . . . ."[262] For example, in

---

258. *See supra* Part VI.B.1.b.

259. FED. R. EVID. 803(8).

260. *Compare id.* 803(6) (requiring "the testimony of the custodian or other qualified witness . . .") *with id.* 803(8) (no such requirement).

261. *Id.* 803(8) advisory committee's note. Although the exception under Rule 803(8) does not require a foundational witness, other factors weigh in admissibility. *Id.* In particular, admissibility of the public record hinges on the content of the record, e.g., whether it contains "matters observed" or evaluative reports, and whether it is used in a civil case or by or against the government in criminal cases. *Id.*

262. *Id.* 803(8); *e.g.*, Malkin v. United States, 243 F.3d 120, 123 (2d Cir. 2001) (holding that information in IRS database was sufficiently reliable to constitute a public record and hence, was admissible to prove that taxpayer had executed consent to extension of limitations period); E.W. Scripps Co. v. United States, 297 F. Supp. 2d 1018, 1025 n.7 (S.D. Ohio 2003) (holding that IRS document locator code was admissible under a hearsay exception, despite the government's urging to disregard the code); United States v. Boyce, 148 F. Supp. 2d 1069, 1082 (S.D. Cal. 2001) (holding that IRS Forms 4340 were admissible under the public records exception); United States v. Estabrook, 78 F. Supp. 2d 558, 561 (N.D. Tex. 1999) (holding that IRS transcript was within official records exception to hearsay rule); Rossi v. United States, 755 F. Supp. 314, 317 (D. Or. 1990) (holding that IRS Forms 4340 were admissible under the public records exception).

Hughes v. United States,[263] the Ninth Circuit held that IRS forms offered by the government to show the defendants' tax assessment were admissible under the hearsay exception.[264] Similarly, the Fourth Circuit in *United States v. Childress*[265] ruled that the defendant's tax records, as certified by the IRS, were admissible as public records under Rule 803(8).[266]

Because a tax evasion claim rests on an alleged failure to pay taxes, the government must often prove the absence of payment. In this situation, the pertinent exemption to the hearsay rule is Rule 803(10), which provides for the admission of evidence of the absence of a public record or entry.[267] To prove the "nonoccurrence or nonexistence of a matter," the proponent must offer "evidence of a certification in accordance with [R]ule 902, or testimony, that a diligent search failed to disclose the record, report, statement, or data compilation . . . ."[268] For instance, in *United States v. Bowers*,[269] the court admitted the government's compilation of assessments and payments, showing no electronic record of returns filed by the defendants.[270] The district court admitted the records under Rule 803(10), but the defendants challenged their admission, arguing that IRS employees in Philadelphia who prepared the compilations were not the "custodians" of the data stored in the IRS mainframe computer in Virginia.[271] The Fourth Circuit upheld the admission, concluding that the rule only required a "diligent search," and because the employees had remote access to the mainframe computer, the agency did not have to send a witness from the

263. 953 F.2d 531 (9th Cir. 1992).

264. *Id.* at 539–40.

265. 24 Fed. Appx. 139 (4th Cir. 2001) (unpublished decision).

266. *Id.* at 142. The court did not specify which part of the rule applied to the tax records. *Id.* Because this was a criminal case, and the records were admitted against the defendant, they were likely admitted by the court under part (A) of Rule 803(8), as records of "the activities of the office or agency . . . ." *See* FED. R. EVID. 803(8)(A).

267. FED. R. EVID. 803(10).

268. *Id.*

269. 920 F.2d 220 (4th Cir. 1990).

270. *Id.* at 223–24; *see also* United States v. Neff, 615 F.2d 1235, 1241–42 (9th Cir. 1980) (holding that IRS Certificate of Assessments and Payments were admissible under the Rule 803(10) absence of public record exception to prove defendants had not filed tax returns).

271. *Bowers*, 920 F.2d at 223.

physical location of the mainframe just to present the data in court.[272] Moreover, as long as the witness had full access to search the agency's computer, conducted the search diligently, and was available for cross-examination, "the concern for trustworthiness embedded in the rules of evidence [was] satisfied."[273]

E. Foundations for E-Mail and Internet Evidence

Although courts recognize the admissibility of electronic business records under the hearsay exception, they are less willing to admit e-mail and Internet evidence. Because e-mail can be created spontaneously and in response to individual events or conversations, courts often conclude that e-mail messages are *not* kept in the course of regularly conducted business activities.[274] In addition, courts struggle with the vulnerability and manipulability of Internet and e-mail evidence.[275]

1. E-mail Evidence

Compared with other forms of electronic evidence, e-mail evidence has received relatively little attention in the federal courts. A proponent could offer e-mail created in the business context as a "business record" and thus could try to satisfy the requirements of the hearsay exception. As discussed above, however, the business records exception to the hearsay rule has a number of conditions that must be satisfied.[276] Under the Federal Rules, the benefits of e-mail communication in today's business environment—notably, its spontaneity and rapid dissemination—are also roadblocks to its admission. Because e-mail can be created on the spur of the moment and in response to countless situations, it is difficult if not impossible for a proponent to establish that the message was created in the course of a *regularly conducted* business activity. Yet, despite this

---

272. *Id.* at 223–24.

273. *Id.* at 223.

274. *See* United States v. Ferber, 966 F. Supp. 90, 98–99 (D. Mass. 1997) ("Were it otherwise, 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. This is not the law.").

275. *See, e.g.*, United States v. Jackson, 208 F.3d 633, 637 (7th Cir. 2000) (rejecting web postings); St. Clair v. Johnny's Oyster & Shrimp, Inc., 76 F. Supp. 2d 773, 774–75 (S.D. Tex. 1999) (rejecting same).

276. *See supra* Part VI.C.2.

difficulty, courts have considered the admissibility of e-mail in a few notable cases.

a. Authentication

As with other electronically stored information, authentication and the hearsay rule present primary hurdles to the admission of e-mail evidence. In *United States v. Siddiqui*,[277] the defendant attacked the government's use of e-mail evidence on both grounds, arguing that it was offered without proper authentication *and* that it constituted inadmissible hearsay.[278] The Eleventh Circuit upheld the district court's holding that the e-mail evidence was admissible because it was properly authenticated under Rule 901(b)(4) based on circumstantial evidence.[279] The court of appeals also held that the defendant's hearsay objections were based on authenticity issues, and thus were not proper objections.[280]

Courts might also consider whether e-mail is self-authenticating. Under Rule 902, one category of self-authenticating documents includes "[i]nscriptions, signs, tags, or labels purporting to have been affixed in the course of business and indicating ownership, control, or origin."[281] Because an e-mail address may include a company's trademark or trade name, the address might authenticate the entire message.[282] For this reason, at least one district court has ruled that e-mail messages can be self-authenticated under Rule 902.[283] However, because the court did not explain in detail why the e-mail

277. 235 F.3d 1318 (11th Cir. 2000).

278. *Id.* at 1321–22.

279. *Id.* For instance, when the e-mail recipient replied to the message, the reply function "automatically dialed [the defendant's] e-mail address as the sender." *Id.* at 1321; *see also* Robins, *supra* note 174, *at* 230 (describing *Siddiqui* as "[a] good example of how e-mail messages can be authenticated in accordance with Rule 901(b)(4).").

280. *Siddiqui*, 235 F.3d at 1322.

281. FED. R. EVID. 902(7).

282. *See* Robins, *supra* note 174, at 240–43 (analogizing a return address to a trade inscription and suggesting that an address may be sufficient to make the message "self-authenticating").

283. *See* Superhighway Consulting, Inc. v. Techwave, Inc., No. 98 CV 5502, 1999 WL 1044870, at *2 (N.D. Ill. Nov. 16, 1999) (denying plaintiff's "motion in limine to bar defendant Techwave from offering unauthenticated [e-mail] evidence," the court shifted the burden of proving e-mails were not self-authenticating to plaintiff at trial).

messages were sufficiently self-authenticating, it is difficult to determine whether a return address *alone* would be sufficient.[284]

b. Hearsay is a much higher hurdle

As discussed above, courts hesitate to apply the business records exception to e-mail messages.[285] For example, the Ninth Circuit in *Monotype Corp. v. International Typeface Corporation* ("ITC")[286] held that an e-mail message was inadmissible under the business records exception because it was not kept in the regular course of business.[287] A Microsoft employee sent the message in question to his superior, voicing his concerns about potential infringement of an ITC copyright.[288] ITC argued that the court should admit the message because e-mail messages to superiors at Microsoft were records kept in the regular course of business.[289] However, the court determined that e-mail was "far less of a systematic business activity than a monthly inventory printout."[290] Moreover, the court noted that "[e]-mail is an ongoing electronic message and retrieval system whereas an electronic inventory recording system is a regular,

284. *Id.* at *2. *But see* Whitted v. General Motors Corp., 58 F.3d 1200 (7th Cir. 1995) (holding that a trade inscription on the cover of an automobile owner's manual did not render the manual admissible under Rule 902(7)).

285. *See supra* Part VI.E.1.a. For a thorough overview of e-mail and the business records exception, see Anthony J. Dreyer, Note, *When the Postman Beeps Twice: The Admissibility of Electronic Mail Under the Business Records Exception of the Federal Rules of Evidence*, 64 FORDHAM L. REV. 2285 (1996). Dreyer argues that e-mail is a "hybrid of computer-based records and correspondence, both of which may be admitted under FRE 803(6)." *Id.* at 2287. He also notes that while not all e-mail messages would qualify as business records, e-mail, as it is used by many organizations, satisfies the requirements and policies behind the rule. *Id.* at 2287, 2314–27. Moreover, he argues that a change in the Rules of Evidence "is necessary to provide a clear mandate as to the appropriate treatment of e-mail evidence." *Id.* at 2287; *see also* Givens, *supra* note 9, at 111–12 (noting that, despite commentator's pleas and the widespread use of e-mail, courts have been reluctant to accept e-mail messages into evidence as business records).

286. 43 F.3d 443 (9th Cir. 1994).

287. *Id.* at 450.

288. *Id.* The potential copyright violations at issue involved a typeface. *Id.*

289. *Id.*

290. *Id.*

systematic function of a bookkeeper prepared in the course of business."[291]

In rejecting another series of e-mails between the defendant Microsoft and a competitor firm, a District of Columbia court drew further distinction between *records* kept in the course of business and the *regular practice* of sending e-mail messages.[292] In *New York v. Microsoft Corp.*, an employee of Microsoft's competitor wrote an e-mail message wherein he referred to a particular phone call with Microsoft representatives.[293] The court concluded that while this e-mail may have been kept in the course of regularly conducted business activity, the competitor firm did not establish that it was the regular practice of employees to write such messages.[294]

In *Westfed Holdings, Inc. v. United States*,[295] the Court of Federal Claims concluded that e-mail messages "recounting telephone or hallway conversations or offering curbside opinions are too informal," and hence, inadmissible under the business records exception.[296] The court also noted that business records made systematically "reflect a higher 'probability of trustworthiness,'"[297] but "documents that are created solely at the author's discretion raise

---

291. *Id.* The court in *Monotype* distinguished *United States v. Catabran*, 836 F.2d 453, 457 (9th Cir. 1988), where the Ninth Circuit held that computer printouts were admissible under the business records exception once the proponent had laid a proper foundation. *Monotype*, 43 F.3d at 450. Notably, the *Monotype* court's discussion did not go beyond this technical distinction to consider the content or context of the message. *Id.* At least one commentator has criticized the Ninth Circuit's "perfunctory" application of the exception, noting the court's reasoning was inconsistent with evidence offered by the proponent which showed that this type of e-mail report was a regular activity for employees. Dreyer, *supra* note 285, at 2317.

291. *Monotype*, 43 F.3d at 450.

292. New York v. Microsoft Corp., No. CIV A. 98-1233 (CKK), 2002 WL 649951 (D.D.C. Apr. 12, 2002).

293. *Id.* at *2.

294. *Id.*

295. 55 Fed. Cl. 544 (2003).

296. *Id.* app. at 566.

297. *Id.*; *see also* Palmer v. Hoffman, 318 U.S. 109, 113–14 (1943) (holding that an engineer's accident report was not "typical of entries made systematically or as a matter of routine," and hence, there was a lower "probability of trustworthiness").

motivational concerns and lack the reliability and trustworthiness that business records are ordinarily assumed to have."[298]

Notwithstanding this line of cases, some e-mail messages may qualify as business records under Rule 803(6). Although the court in *New York v. Microsoft Corp.* rejected an e-mail message offered as evidence, it noted in dicta that its decision did not imply that *no* e-mail could qualify as a "business record." [299] For instance, if the foundational witness can establish that employees regularly keep e-mail memos of meetings or phone calls, then the business record exception may be satisfied.[300] In addition, at least one district court has held that e-mail messages are admissible under the hearsay exception when they are kept in the normal course of business and created at or near the time of the matters described therein.[301] E-mail purchase orders or automatic sales confirmation messages, for example, may be admissible under Rule 803(6).

Beyond the business records exception, proponents may find other ways to offer e-mail as evidence. For instance, an e-mail message may not be hearsay if the proponent offers it against the party who made the "statement."[302] Moreover, an e-mail message sent in the context of a business transaction might be admissible under another Rule 803 exception to the hearsay rule. Although singular in its approach to e-mail as hearsay, the *Ferber* case discussed below is nonetheless a valuable illustration of the potential admissibility of e-mail evidence.[303]

---

298. *Westfed*, 55 Fed. Cl. at 566 (citations omitted); *see also In re* Hechinger Investment Co. of Del., Inc., 298 B.R. 240, 242 (Bankr. D. Del. 2003) (holding that e-mail messages did not fall within the business records exception because they were direct responses to a solicitation for information and were made in preparation for the bankruptcy proceeding).

299. New York v. Microsoft Corp., No. CIV A. 98-1233 (CKK), 2002 WL 649951, at *2, n.4 (D.D.C. Apr. 12, 2002).

300. *Id.*

301. *See* DirecTV, Inc. v. Murray, 307 F. Supp. 2d 764, 772 (D.S.C. 2004) (noting that, although this was a close question, the declaration of the company's custodian of records, together with the affidavit of a paralegal who received copies of the records on compact disk, satisfied the business records exception).

302. *See* FED. R. EVID. 801(d)(2). In general, a statement is not hearsay if it is offered against a party and it is the party's own statement.

303. *See infra* Part VI.E.1.b.ii.

i. Party admission

A few courts have allowed e-mail messages into evidence as non-hearsay party admissions, pursuant to Rule 801(d)(2).[304] On appeal, the defendant in *Siddiqui* challenged the government's use of e-mail messages he sent to a colleague, on grounds that the messages were improperly authenticated *and* they constituted inadmissible hearsay.[305] At trial, however, the defendant objected *only* to the government's authentication.[306] The Eleventh Circuit determined that if the defendant had properly preserved his hearsay objection, the district court would still have been within its discretion to overrule the objection.[307] In particular, the court concluded that the e-mail messages would have been party admissions under Rule 801(d)(2)(A) and would therefore have been admissible as non-hearsay.[308]

In *Sea-Land Service, Inc. v. Lozen International, LLC*,[309] the Ninth Circuit concluded that the district court improperly excluded an e-mail message authored by one Sea-Land employee and forwarded to Lozen by a second Sea-Land employee.[310] The lower court found that Lozen did not present any evidence indicating the identity or job title of the employee who authored the e-mail.[311] But

---

304. Rule 801(d)(2) exempts "five categories of statements for which the responsibility of a party is considered sufficient to justify reception in evidence against him." FED. R. EVID. 801(d)(2) advisory committee's note. Specifically, a statement is not hearsay if it is offered against a party and is

> (A) the party's own statement in either an individual or representative capacity, or (B) a statement of which the party has manifested an adoption or belief in its truth, or (C) a statement by a person authorized by the party to make a statement concerning the subject, or (D) a statement by the party's agent or servant concerning a matter within the scope of the agency or employment, made during the existence of the relationship, or (E) a statement by a coconspirator of a party during the course and in furtherance of the conspiracy.

FED. R. EVID. 801(d)(2).

305. United States v. Siddiqui, 235 F.3d 1318, 1322–23 (11th Cir. 2000).

306. *Id.* at 1323.

307. *Id.*

308. *Id.* FED. R. EVID. 801(d)(2)(A) provides that a statement is not hearsay if it "is offered against a party . . . and is the party's own statement in either an individual or a representative capacity."

309. 285 F.3d 808 (9th Cir. 2002).

310. *Id.* at 821.

311. *Id.*

the Ninth Circuit, accepting Lozen's argument on appeal, held that the message was not hearsay because it was a statement by the party's agent, concerning a matter within the scope of his employment.[312] Because Rule 801 provides that the contents of the statement itself may be considered, but are not sufficient, to establish the scope of the employment relationship, the court also considered the electronic "signature" attached to the message and the author's role in the company.[313] The e-mail message also constituted an adoptive admission under 801(d)(2)(B) because a second Sea-Land employee copied the original message and forwarded it to Lozen.[314] This second employee was working for Sea-Land at the time the message was written, and the contents of the e-mail were also within the scope of her employment.[315]

In *Riisna v. ABC, Inc.*,[316] a court in the Southern District of New York admitted an e-mail message sent by an executive producer to Riisna, a freelance journalist. ABC, Inc. fired Riisna after she filed a malpractice suit against a plastic surgeon featured on the network's program "20/20."[317] Even though she retained a freelance position, Riisna filed an age discrimination suit against the network.[318] Shortly thereafter, she received an e-mail from an executive producer stating that her freelance project "[wasn't] going to [work][319] out . . . ."[320] Riisna sought to enter the producer's e-mail as evidence of the network's retaliatory scheme.[321] The district court held that the e-mail was a party admission because the producer was acting

312. *Id.*; *see* FED. R. EVID. 801(d)(2)(D).

313. *Sea-Land Serv. Inc.*, 285 F.3d at 821 (noting that the author was a service coordinator at Sea-Land at the time the e-mail was written and the message concerned a late delivery to Lozen).

314. *Id.* The second employee incorporated the first e-mail in her message to Lozen and prefaced it with the statement, "Yikes, Pls note the rail screwed us up . . ." *Id.*

315. *Id.*

316. 219 F. Supp. 2d 568 (S.D.N.Y. 2002).

317. *Id.* at 570. While producing a story for the network's program "20/20," Ene Riisna met a plastic surgeon who later performed surgery on Riisna's face. Upset with the surgical outcome, Riisna sued the surgeon for medical malpractice. *Id.*

318. *Id.*

319. Brackets in original.

320. *Id.* at 571.

321. *Id.* at 571–72.

within the scope of his employment,[322] and he was authorized by ABC to make a statement concerning the company's refusal to re-hire Riisna.[323]

ii. Other exceptions

In *United States v. Ferber*,[324] a Massachusetts district court considered whether an e-mail message fell within a number of other exceptions to the hearsay rule.[325] No federal court since *Ferber* has undertaken such a comprehensive analysis of e-mail statements under the hearsay rule. Nevertheless, this case illustrates the potential for proponents to offer e-mail evidence without first having to satisfy the requirements of the business records exception. For instance, a proponent could offer an e-mail message as a "present sense impression," without first demonstrating that the message was kept in the course of a regularly conducted business activity.[326]

Ferber, a financial advisor and investment banker, was convicted for violating fiduciary duties he owed to his public entity clients.[327] The court explained a number of its evidentiary rulings in this case, including the admission of an incriminating e-mail message.[328] After a telephone conversation with Ferber, Carey sent this message to his supervisor at Merrill Lynch,[329] describing Ferber's inculpatory

322. *Id.* at 572; *see* FED. R. EVID. 801(d)(2)(D).

323. *Riisna*, 219 F. Supp. 2d at 572; *see* FED. R. EVID. 801(d)(2)(C).

324. 966 F. Supp. 90 (D. Mass. 1997).

325. *Id.* at 98–99; *see also* Mota v. Univ. of Tex. Houston Health Sci. Ctr., 261 F.3d 512, 527 (2001) (noting that an e-mail sent by a university president after a jury found the university liable in a harassment suit would be admissible on a number of grounds, including Rule 803(3), as a statement of the declarant's then existing state of mind; however, the court's discussion was cursory, and it did not explain why this particular message fit within the hearsay exception).

326. *Compare id.* 803(6) *with* FED. R. EVID. 803(1), which exempts from the hearsay rule any "statement describing or explaining an event or condition made while the declarant was perceiving the event or condition, or immediately thereafter." For a discussion of hearsay exceptions in the context of non-electronic evidence and state court cases involving e-mail evidence, see Robins, *supra* note 174.

327. *Ferber*, 966 F. Supp. at 92.

328. *Id.* at 98–99.

329. One of Ferber's clients, the Massachusetts Water Resources Authority ("MWRA"), selected Merrill Lynch as underwriter for a bond issue. *Id.* at 93. The government alleged that Ferber aided Merrill Lynch during the underwriter selection process, in violation of the MWRA's "blackout rule,"

statements.[330] Carey ended the e-mail by saying, "my mind is mush!"[331]

The government first sought to admit the message as a business record, by demonstrating that it was Carey's routine practice to send messages to co-workers in the "relevant 'loop' immediately following an important telephone conversation with a client."[332] The court, however, rejected this foundation because there was insufficient evidence that Merrill Lynch required such records be maintained.[333] Without a duty to keep this type of record, the government could not demonstrate its reliability.[334]

The government then tried to admit the e-mail as an excited utterance under Rule 803(2), based on Carey's final comment, "my mind is mush!"[335] To lay the foundation for this exception, the government called Carey to testify that that he wrote the e-mail shortly after his conversation with Ferber, when he was "very upset" and "panicked."[336] The court rejected this argument as well.[337] Based on the detail and length of Carey's message, and the possibility that he spoke with someone else before writing it, the court concluded that Carey had ample time to reflect, and hence was no longer influenced by the "stress of excitement" caused by his conversation with Ferber.[338]

The government ultimately succeeded in admitting Carey's e-mail message as a present sense impression under Rule 803(1).[339] The court noted that while a present sense impression "is admissible so long as it explains an event immediately after it happens," the passage of a short amount of time does not necessarily preclude the

---

which prohibited investment banks from contacting any agent of the MWRA during the election process. *Id.*

330. *Id.* at 98.

331. *Id.*

332. *Id.*

333. *Id.*

334. *Id.*; *see also supra* note 274 and accompanying text.

335. *Ferber*, 966 F. Supp. at 99. FED. R. EVID. 803(2) exempts from the hearsay rule a "statement relating to a startling event or condition made while the declarant was under the stress of excitement caused by the event or condition."

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

337. *Id.*

338. *Id.*; *see* FED. R. EVID. 803(2).

339. *Ferber*, 966 F. Supp. at 99; *see* FED. R. EVID. 803(1).

evidence.[340] Thus, the court concluded that "although Carey's e-mail was removed from the 'stress' of the Ferber phone call, it was prepared shortly afterward and therefore qualified as a present sense impression."[341]

2. Internet Evidence: Foundational Issues

Courts view Internet evidence with skepticism, primarily because it can be altered by anyone with access to a Web site server. At least one district court has stated that a proponent of Internet evidence cannot "overcome the presumption that the information he discovered on the Internet is inherently untrustworthy."[342] This same court went on to say that it held "no illusions that hackers can adulterate the content on *any* web-site from *any* location at *any* time," and thus "any evidence procured off the Internet is adequate for almost nothing."[343]

While this may seem like an overly harsh stance against Internet evidence, a similar position was taken by the Seventh Circuit in *United States v. Jackson*.[344] There, the circuit court echoed the district court's distrust of Internet evidence[345] and concluded that

340. *Ferber*, 966 F. Supp. at 99 (citing United States v. Blakey, 607 F.2d 779, 785 (7th Cir. 1979) for the proposition that statements made within twenty-three minutes of an event are admissible under 803(1)); *see also* FED. R. EVID. 803(1) advisory committee's note ("[I]n many, if not most, instances precise contemporaneity is not possible, and hence a slight lapse is allowable.").

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

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

343. *Id.* at 775. This court, referring to "voodoo information taken from the Internet," summarized its skepticism toward Internet evidence: "While 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." *Id.* at 774–75.

344. 208 F.3d 633, 637 (7th Cir. 2000); *see supra* notes 253–256 and accompanying text.

345. *Jackson*, 208 F.3d. at 637 (quoting *St. Clair*, 76 F. Supp. 2d at 775). For the proposition that internet evidence is inherently untrustworthy, *St. Clair* has been cited by a number of federal district courts. *E.g.*, United States EEOC v. E.I. DuPont de Nemours & Co., No. Civ. A 03-1605, 2004 WL 2347559, at *2 (E.D. La. Oct. 18, 2004); Tolliver v. Fed. Republic of Nigeria, 265 F. Supp. 2d 873, 876 (W.D. Mich. 2003); Wady v. Provident Life & Accident Ins. Co. of America, 216 F. Supp. 2d 1060, 1064 (C.D. Cal. 2002);

Web site postings were inadmissible as business records of internet service providers because the defendant presented no evidence that the "service providers even monitored the contents of those web sites."[346]

Because of inherent reliability concerns, authentication of Internet evidence, in contrast to other forms of electronic evidence, is problematic. For instance, the *Jackson* court ruled that even if Web postings were admissible hearsay, the evidence still lacked authentication under Rule 901.[347] The defendant needed to show that the Web postings were actually posted by the groups that operated the sites, "as opposed to being slipped onto the groups' web sites by [the defendant] herself, who was a skilled computer user."[348] The untrustworthiness of Internet evidence may also be reflected in the fact that nearly all reported cases on point—excluding *Jackson*—have been decided at the district court level.[349] Thus, the inadmissibility of Internet evidence remains a non-controversial issue among federal courts. Interestingly, however, district courts have declined to follow the authentication and hearsay analyses of *Jackson* and *St. Clair*. In particular, courts that have addressed the hearsay rule have distinguished Internet evidence generated by a *party's* Web site from that of *non-parties*. When offered from a party's Web site (and against that party), the evidence constitutes a party admission and thus is admissible as non-hearsay.[350]

Westland Water Dist. v. United States, 153 F. Supp. 2d 1133, 1143 n.9 (E.D. Cal. 2001); Barbour v. Head, 178 F. Supp. 2d 758, 760 n.3 (S.D. Tex. 2001).

346. *Jackson*, 208 F.3d at 637.

347. *Id.* at 638.

348. *Id.* This supports the notion that courts should analyze *both* authentication and the applicability of a hearsay exception. Nevertheless, this ruling runs counter to the line of cases previously discussed, wherein proponents could easily satisfy both authentication and hearsay analyses by fulfilling the requirements of the latter. *See supra* Part VI.C.2.

349. *See supra* note 345.

350. *See* FED. R. EVID. 801(d)(2). In so holding, courts side-step the issues of authenticity, reliability and trustworthiness. In fact, one district court noted that where "technical deficiencies" of Internet evidence exist, they "must go to the weight of such evidence, rather than to their admissibility." Microware Systems Corp. v. Apple Computer, Inc., 126 F. Supp. 2d 1207, 1211 n.2 (S.D. Iowa 2000) (citing Squirt Co. v. Seven-Up Co., 628 F.2d 1086 (8th Cir. 1980)).

In *Van Westrienen v. Americontinental Collection Corp.*,[351] the plaintiffs sued a debt collection agency for violations of the Fair Debt Collection Practices Act.[352] In a collection letter, the defendants invited plaintiffs to view the collection agency's Web site.[353] The plaintiffs then sought to admit the Web site content as evidence of the defendants' misrepresentations.[354] The defendants argued that the Web site constituted inadmissible hearsay, but the Oregon district court ruled that the contents of the site were not hearsay because they were representations made by the defendants and offered into evidence by the plaintiffs.[355]

A California district court held the same when the plaintiff offered into evidence a report submitted by the defendant to the Securities and Exchange Commission ("SEC").[356] This report was filed with the SEC and later posted on the Internet.[357] The defendant objected to the admission of the reports on the ground that they were hearsay, but the court ruled that because the reports were submitted by the defendant (and the defendant did not offer any evidence to the contrary), they constituted a party admission.[358] The court also noted that the act of placing the SEC reports on the Internet was non-verbal conduct, not intended as an assertion, and therefore could not be hearsay under Rule 801.[359] In addition, the court rejected the defendant's contention that, under *St. Clair* and *Jackson*,[360] the Web site material should be barred.[361] The court concluded that *Jackson*

351. 94 F. Supp. 2d 1087 (D. Or. 2000).
352. *Id.* at 1094.
353. *Id.* at 1109.
354. *Id.* at 1095.
355. *Id.*; *see also* Telewizja Polska USA, Inc. v. Echostar Satellite Corp., No. 02 C 3293, 2004 WL 2367740, at *5 (N.D. Ill. Oct. 15, 2004) (holding that contents of plaintiff's Web site were an admission of party-opponent and thus not barred by the hearsay rule).
356. Fla. Conference Ass'n of Seventh-Day Adventists v. Kyriakides, 151 F. Supp. 2d 1223, 1225 (C.D. Cal. 2001).
357. *Id.*
358. *Id.* Defendant also raised an authenticity objection. But the court, in a footnote, rejected that argument because the "context in which Plaintiff obtained the documents as well as the content and appearance of the documents" indicated they were authentic. *Id.* at 1225 n.3.
359. *Id.* at 1225. Under FED. R. EVID. 801(a)(2), nonverbal conduct may be a "statement" if it is intended by the declarant as an assertion.
360. *See supra* notes 342–346 and accompanying text.
361. *Kyriakides*, 151 F. Supp. 2d at 1226.

and *St. Clair* were inapposite because, in those cases, statements posted on Web sites were statements by *non*-parties and hence were inadmissible hearsay.[362]

Another California district court determined that when a party offers the content of its own Web site into evidence, that evidence is admissible based on "circumstantial indicia of authenticity."[363] In *Perfect 10*, the court considered the admissibility of exhibits printed from the plaintiff's Web site.[364] The defendant, citing *Jackson* and *St. Clair*, argued that the exhibits were insufficiently authenticated.[365] The court noted that while these two "out-of-circuit cases are informative concerning the potential pitfalls of internet-based documents, [the] court must look to the Ninth Circuit for guidance."[366] The court then cited *United States v. Tank*[367] and concluded that circumstantial evidence supported the admissibility of the Internet printouts.[368] In particular, the court relied on a declaration of the plaintiff's CEO that the printouts were true and correct copies of pages printed from the Internet by the CEO himself or under his direction.[369] The court also concluded that, in concert with the dates and Web addresses on the printouts, a reasonable juror could believe that the documents were what the plaintiff purported.[370]

F. Best Evidence

The third obstacle to the admission of electronic evidence is the rule of best evidence. When a party seeks to "prove the content of a

362. *Id.*

363. Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1154 (C.D. Cal. 2002).

364. *Id.* at 1153–54.

365. *Id.* at 1153.

366. *Id.* In this court's opinion, the *St. Clair* court "took a more extreme view over the admissibility of data" taken from the Internet. *Id.*

367. United States v. Tank, 200 F.3d 627, 630 (9th Cir. 2000); *see supra* notes 169–172 and accompanying text.

368. *Perfect 10*, 213 F. Supp. 2d at 1154.

369. *Id.*

370. *Id.* Defendant also raised a hearsay objection to printouts from third-party Web sites. However, the court concluded that, based on the defendant's corporate affiliation with the third-party, the printouts fell outside the definition of hearsay and thus were admissible as statements of party-opponents under Rule 801(d)(2)(D). *Id.* at 1155.

writing, recording, or photograph," the Federal Rules require use of the original, or in some circumstances a "duplicate."[371] Electronic evidence falls within the ambit of the rule because "'[w]ritings' [or] 'recordings' consist of letters, words, or numbers, or their equivalent, set down by handwriting, typewriting, printing . . . *or other form of data compilation.*"[372] A proponent need not introduce a hard drive, disk or other electronic hardware because the Rules also provide that "[i]f 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'."[373] For instance, in *Perfect 10*, the court noted that to the extent printouts were used to demonstrate the images and text found on the Web site, the printouts were subject to—and met—the best evidence rule.[374]

1. Graphical Representation

While best evidence seems a relatively straightforward requirement, problems arise when the primary purpose of the data is to create a visual representation. A recent federal appellate case is illustrative. In *United States v. Bennett*,[375] the issue was whether a customs officer's testimony about global positioning satellite ("GPS") display data was barred by the best evidence rule.[376] Although the officer did not see the defendant's boat cross the border between Mexico and the United States, the officer did observe the display on a GPS device discovered during a search of that boat.[377] The officer testified that the display showed navigational points from waters off the coast of Mexico to points north of San Diego Bay.[378]

371. FED. R. EVID. 1002. Under Rule 1003, "[a] duplicate 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." *Id.* 1003.

372. *Id.* 1001(1) (emphasis added). According to the Advisory Committee's note, "the considerations underlying the rule dictate its expansion to include computers, photographic systems, and other modern developments." *Id.* 1001 advisory committee's note.

373. *Id.* 1001(3) (emphasis added).

374. 213 F. Supp. 2d at 1155 n.4.

375. 363 F.3d 947 (9th Cir. 2004).

376. *Id.* at 952–53.

377. *See id.* at 952.

378. *Id.*

At trial, the district court overruled the defendant's best evidence objection,[379] but the Ninth Circuit noted that the rule applies when a witness "seeks to testify about the contents of a writing, recording or photograph without producing the physical item itself."[380] Because the government was "not excused from the best evidence rule's preference for the original," and because "the government did not produce the GPS itself . . . or a printout or other representation of [the] data," the Ninth Circuit held the officer's testimony was inadmissible.[381]

2. "Hidden" Information and the Integrity of Electronic Evidence

Further problems arise when a hard copy printout or other data output does not reflect all of the data that might be needed to adequately present the evidence in its electronic context. While a computer printout of electronically stored data and the "actual electronic file may contain the same visible words [or] thoughts," the electronic file may include other "hidden" information.[382] In *Armstrong v. Executive Office of the President*,[383] the District of Columbia Circuit described "hidden" information in e-mail messages:[384]

> [B]oth the recipient and the author of a note can print out a "hard copy" of the electronic message containing essentially all the information displayed on the computer screen. That paper rendering will not, however, necessarily include all the information held in the computer memory as part of the electronic document. Directories, distribution lists, acknowledgments of receipts and similar materials do not appear on the computer screen—and thus are not reproduced when users print out the information that appears on the screen. Without this "non-screen" information, a later reader may not be able to glean from the

379. *Id.*
380. *Id.* at 953–54. According to the court, the best evidence rule applies "particularly when the witness [is] not privy to the events those contents describe." *Id.*
381. *Id.* at 954.
382. Givens, *supra* note 9, at 98.
383. 1 F.3d 1274 (D.C. Cir. 1993).
384. *Id.* at 1280.

> hard copy such basic facts as who sent or received a particular message or when it was received. . . . Consequently, if only the hard copy is preserved in such situations, essential transmittal information relevant to a fuller understanding of the context and import of an electronic communication will simply vanish.[385]

In this case, the court held that administrative agencies of the federal government did not fulfill their duties under the Federal Records Act ("FRA")[386] by simply printing copies of electronic messages and managing the "hard copy" documents in accordance with the Act.[387] Although the *Armstrong* court did not specifically address the evidentiary value of these messages, a few courts have addressed the utility of electronic evidence vis-à-vis its completeness and integrity.[388] These courts have considered electronic data in visual and audio formats and, notably, they have not followed *Armstrong*'s reasoning.[389]

In *United States v. Sattar*,[390] for example, a New York district court held that the production of intercepted evidence in a file format different from the original did not violate the best evidence rule.[391] The defendant argued that electronic surveillance evidence was inadmissible because the government provided the audio files in an .mp3 format rather than in their original file format.[392] He argued that the "deletion or non-disclosure of the [original] underlying . . . file formats amount[ed] to destruction of the original evidence for

---

385. *Id.*

386. *Id.* at 1278 (citing the FRA at 44 U.S.C. §§ 2101–19, 2901–10, 3101–07, and 3301–24 (2001)).

387. *Id.* at 1277, 1296; *see also* Public Citizen v. Carlin, 184 F.3d 900, 911 (D.C. Cir. 1999) ("'[U]nless the paper versions include all significant material contained in the electronic records . . . the two documents cannot be accurately termed 'copies.'" (quoting *Armstrong*, 1 F.3d at 1283)).

388. *See* United States v. Sattar, No. 02 CR. 395 (JGK), 2003 WL 22510435, at *4 (S.D.N.Y. Nov. 5, 2003); Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 313–14 (S.D.N.Y. 2000).

389. It may be that any loss of data is less perceptible when electronic or digital information is used in audio-visual formats. For instance, in *Universal City Studios, Inc.*, 111 F. Supp. 2d at 313–14, the court noted that the loss of data from decompression of a visual file resulted in an imperceptible loss of quality, that would be "of no importance to ordinary consumers."

390. No. 02 CR. 395 (JGK), 2003 WL 22510435 (S.D.N.Y. Nov. 5, 2003).

391. *See id.* at *4.

392. *Id.* at *1.

purposes of the best evidence rule."[393] The court, denying the defendant's motion for an evidentiary hearing, held that there was "no reason to believe that the file format . . . fail[ed] to maintain the [original] files'. . . fidelity, or that it compresse[d] or destroy[ed] the data."[394] Moreover, the court stated that the defendant made "no showing that the underlying electronic files contained [any] exculpatory evidence or that the [g]overnment deleted the files in bad faith."[395]

Although federal courts have not determined the best evidence implications of data compression, at least one intellectual property case suggests that it may not have any effect on the actual content of electronic files or the integrity of the evidence.[396] In *Universal City Studios, Inc.*, the district court determined that use of a software application to compress and then decompress movies on digital versatile disks ("DVDs") infringed movie copyrights, even though the compression involved an inexact replication of the original file.[397] Similarly, an inexact "duplicate" of electronic data with audiovisual output may suffice as an "original" under the best evidence rule.

3. Summaries

A few federal courts have addressed the use of computer generated summaries under Rule 1006, which provides that the contents of a "voluminous" writing or recording "which cannot conveniently be examined in court may be presented in the form of a chart, summary, or calculation."[398] In *AFD Fund v. United States*,[399] a Court of Federal Claims set forth four requirements for the use of a summary of evidence:

---

393. *Id.* at *4.
394. *Id.*
395. *Id.*
396. Data compression has been defined as "the process of reducing the size of the representation of a string of electronic data in order to permit it to be transmitted or stored more efficiently and later to be reconstructed without error." Storer v. Hayes Microcomputer Products, Inc., 960 F. Supp. 498, 501 (D. Mass. 1997).
397. 111 F. Supp. 2d 294, 313–15 (S.D.N.Y. 2000).
398. FED. R. EVID. 1006. The rule also provides that the "originals, or duplicates, shall be made available for examination or copying, or both, by other parties at reasonable time and place." *Id.*
399. 61 Fed. Cl. 540 (2004).

> First, the summarized writings must be so voluminous so as to be unable to be conveniently examined in court. Second, the underlying evidence must itself be admissible. Third, the original or copies of the summarized writings must be made available to the opposing party. And, fourth, the proposed summary (or chart or calculation) must accurately summarize (or reflect) the underlying document(s) and only the underlying document(s).[400]

In *United States v. King*,[401] the Third Circuit held that the government's charts and exhibits summarizing electronic communications between conspirators in a drug distribution ring were admissible.[402] Specifically, the district court did not abuse its discretion when it admitted the summaries because the government was able to "establish that all of the telephone and beeper numbers on the charts and exhibits were controlled by [the defendant] or his associates."[403] Moreover, the government accurately explained the charts and exhibits to the jury.[404]

Interestingly, while it is no trouble for a proponent to show that a summary accurately represents the underlying electronic information,[405] the third requirement that the underlying evidence be made available to the opposing party has been more problematic. For instance, in *AFD Fund*, the court determined that "AFD did not provide [a] complete set of electronic files to the government, including copies of the electronic [records] used to generate

400. *Id.* at 546; *see also* Bannum, Inc. v. United States, 59 Fed. Cl. 241, 244–45 (2003) (discussing the admissibility of a summary of evidence in federal court and these four foundational requirements); Bath Iron Works Corp. v. United States, 34 Fed. Cl. 218, 232–33 (1995) (discussing the same).

401. 93 Fed. Appx. 490 (3d Cir. 2004). This is one of a series of cases decided by the Third Circuit in April 2004, involving drug conspiracies and summaries of electronic communications. *See* United States v. Worrells, 94 Fed. Appx. 927, 929 (3d Cir. 2004) (holding that a summary was admissible when the government explained the summary "so as not to confuse the jury"); United States v. Watson, 93 Fed. Appx. 481, 482 (3d Cir. 2004).

402. *King*, 93 Fed. Appx. at 491–92.

403. *Id.*

404. *Id.* at 492.

405. The inaccuracy of the summary itself, like other electronic evidence, goes to the weight of the evidence, rather than its admissibility. *See* BD *ex rel.* Jean Doe v. DeBuono, 193 F.R.D. 117, 130 (S.D.N.Y. 2000).

invoices" and account summaries.[406] In contrast, the Ninth Circuit in *Hughes v. United States*[407] held that IRS certificates were admissible to show that the defendants owed federal income taxes.[408] The defendants argued that the forms were inadmissible under Rule 1006 "because neither the originals nor duplicates of the original assessment documents [had] been made available."[409] The court, however, held that this argument was misplaced because the forms were not merely a summary record of the proof, but rather were themselves proof that the IRS made the tax assessments.[410]

Finally, video summaries may be analogous to electronic sources in audio or visual format, such as digital images or DVDs.[411] In *Miracle Blade, LLC v. Ebrands Commerce Group, LLC*,[412] a seller of kitchen knives sued a competitor for copyright and trademark infringement based on a series of infomercials.[413] To prove no infringement, the defendants sought to admit a video summary of the infomercials in question.[414] The court held that although the defendants "did not comply with [Rule] 1006 to the letter," the summary was nevertheless admissible given the "unique exigencies" of the case.[415] In particular, the court determined that "presenting each comparison infomercial in its entirety would have been an inconvenience for the court to examine."[416] Moreover, the defendants sufficiently identified the source of the video excerpts, and the plaintiff had access to the material at least ten days prior to the hearing.[417] To date, no reported federal case involves the use of summaries of electronic evidence in audio or visual format.

406. AFD Fund v. United States, 61 Fed. Cl. 540, 546 (2004). AFD did not attempt to satisfy the other requirements of the rule since it denied that the evidence proffered constituted summaries. *Id.*

407. 953 F.2d 531 (9th Cir. 1992).

408. *Id.* at 539–40.

409. *Id.* at 539.

410. *Id.* at 540.

411. *See supra* notes 396–397 and accompanying text (discussing compression and decompression of data on DVDs).

412. 207 F. Supp. 2d 1136 (D. Nev. 2002).

413. *Id.* at 1141.

414. *See id.* at 1145–46.

415. *Id.* at 1146. The court did not explain how the defendants failed to comply with Rule 1006.

416. *Id.*

417. *Id.*

Nevertheless, cases like *Miracle Blade* illustrate the challenges that arise when a proponent seeks to admit electronic evidence.

G. New Frontiers of Electronic Evidence

Application of the Federal Rules to electronic evidence is still, to some degree, speculative. As forms of electronic communication and recordkeeping develop, the courts' interpretations of the Rules will also evolve. If the past is an indicator, this area of law will continue to advance at the district court level without much controversy: courts will become increasingly sophisticated and well-versed in handling electronic evidence, and the trend of assimilation of electronic evidence into the realm of real evidence will continue. In this case, electronic evidence will be the "best friend" of its proponents.

However, as electronic technology evolves, so too do the opportunities for manipulation of data. What now seems to be a healthy skepticism toward e-mail and the Internet may become a broader distrust on the part of courts. Only time will tell whether electronic evidence will push the evidentiary envelope so far that courts will no longer admit such evidence under the Rules as they exist today. In that case, textual revisions to the Rules may be necessary. Whatever the trend, litigators will undoubtedly face more and more evidence in electronic form, and they must be prepared to meet evidentiary hurdles with technological savvy and creativity.