Boston University
Journal of Science & Technology Law

Article

The Electronic Paper Trail: Evidentiary Obstacles to Discovery and Admission of Electronic Evidence

Christine Sgarlata Chung and David J. Byer

Table of Contents

The Electronic Paper Trail: Evidentiary Obstacles to Discovery and Admission of Electronic Evidence[†]

Christine Sgarlata Chung[*] and David J. Byer[**]

I. INTRODUCTION

1. Former Lazard Freres & Co. ("Lazard") partner Mark Ferber probably wishes that electronic mail had never been invented. During the 1990s, Ferber was a financial advisor to various state and federal government agencies.[1] On May 2, 1996, however, a federal grand jury indicted Ferber on a variety of fraud and corruption charges.[2] Prosecutors alleged Ferber used his relationship with government agencies to extract kickbacks from the Wall Street investment firm of Merrill, Lynch, Pierce, Fenner & Smith, Inc. ("Merrill Lynch").[3] Prosecutors also claimed Ferber failed to inform his government clients about his relationship with

---

[*] B.A., *magna cum* laude, 1989, Amherst College. J.D., *cum* laude, 1993, Harvard Law School. Christine Sgarlata Chung was formerly an associate at the Boston law firm of Testa, Hurwitz & Thibeault, LLP.

[**] B.A., *general honors*, 1972, Johns Hopkins University. M.A., 1975, Cornell University. J.D., 1984, Stanford University. David J. Byer is a partner at the Boston law firm of Testa, Hurwitz & Thibeault, LLP and chair of the Patent and Intellectual Property Practice Group. An adjunct faculty member at Boston University's School of Law, Mr. Byer teaches Trademark and Unfair Competition Law and moderated the Internet Law Symposium sponsored by Boston University. *See* 3 B.U.J. SCI & TECH. L.1-5 (1997).

[1] Ferber advised such agencies as the Massachusetts Water Resources Authority, the District of Columbia, the Michigan Department of Transportation, and the United States Postal Service. *See* United States v. Ferber, 966 F. Supp. 90, 92 (D. Mass. 1997).

[2] Specifically, the grand jury charged Ferber "with 39 counts of mail and wire fraud, . . . 13 counts of accepting bribes and unlawful gratuities, . . . one count of conspiracy, . . . 25 counts of using interstate travel to commit bribery, commercial bribery and extortion, . . . and one count of attempted extortion." *Id; see also* 18 U.S.C. § 666 (1996) (bribes); *id.* §§ 1341, 1343, 1346 (1996) (mail and wire fraud); *id.* § 1952 (1996) (racketeering). The court later dismissed some of these counts. *See Ferber*, 966 F. Supp. at 95.

[3] *See Ferber*, 966 F. Supp. at 93-95.

Merrill Lynch,[4] including an undisclosed contract under which Merrill Lynch paid Lazard millions so that Ferber, who had been hired by his clients to provide them with independent financial advice, would recommend Merrill Lynch.[5]

2. During Ferber's trial, prosecutors introduced a key piece of evidence, an electronic mail message ("e-mail"),[6] written by a Merrill Lynch employee to his supervisor shortly after the employee spoke with Ferber.[7] In the e-mail, the employee "recount[ed] a conversation with Ferber where Ferber inculpated himself."[8] The e-mail suggested ways in which the supervisor might deal with Ferber's improprieties,[9] urged the supervisor to speak with Ferber directly,[10] and concluded, "my mind is mush."[11]

3. Both sides vigorously contested the admissibility of this e-mail message at trial. The government first argued that the [e]-mail message was admissible under the business record exception to the hearsay rule.[12] The government argued that there was sufficient foundation for admitting the e-mail as a business record because the e-mail printout was "authentic and accurate," and because it was the employee's "routine practice" to e-mail relevant co-workers immediately after important conversations with clients.[13] The court, however, found that while the employee may routinely have sent such e-mails, his employer, Merrill Lynch, had no

---

4 *See id.*

5 *See id.* at 94-95.

6 Federal regulations define e-mail as a "document created or received on an electronic mail system including brief notes, more formal or substantive narrative documents, and any attachments, such as word processing and other electronic documents, which may be transmitted with the message." 36 C.F.R. § 1234.2 (1996).

7 *See Ferber,* 966 F. Supp. at 98.

8 *Id*

9 *See id.*

10 *See id.* at 99 n.9.

11 *Id.* at 98.

12 *See id.* "Records of regularly conducted [business] activity" include "a[ny] memorandum, report, record, or data compilation . . . made . . . [by] a person with knowledge, if kept in the course of a regularly conducted business activity," FED. R. EVID. 803(6), and the nature of the business activity gives rise to a duty to create such a business record. *See Ferber*, 966 F. Supp. at 98-99 (citing Willco Kuwait (Trading) S.A.K. v. deSavary, 843 F.2d 618, 628 (1st Cir. 1988)).

13 *Ferber*, 966 F. Supp. at 98.

business duty to make and retain records of this nature. Thus, the court held the e-mail was not admissible as a business record.[14]

4. The government next tried to admit the e-mail under the excited utterance exception to hearsay.[15] According to government elicited testimony, the employee wrote the message shortly after his conversation with Ferber and the employee felt "upset [and] panicked" following the conversation.[16] Again, the court refused to admit the e-mail, finding that it was not the typical outburst that qualifies as a spontaneous utterance.[17]

5. By the time the court made this ruling, the government had asserted a third ground for admission of the e-mail, the present sense impression exception to the hearsay rule.[18] Under this rule, courts may admit into evidence "[a] statement describing or explaining an event or condition made while the declarant was perceiving the event or condition, or immediately thereafter," even though the statement would normally be hearsay and the declarant is available as a witness.[19] The court found that the nature and tone of the message and the circumstances of its preparation qualified it as a present sense impression and admitted the e-mail into evidence.[20]

6. The e-mail message may have devastated Ferber's defense. A jury ultimately convicted Ferber on fifty-seven counts, finding that Ferber had deprived his clients, the public agencies, of the right to honest services.[21] After extensive

---

[14] *See id.* at 98-99 (citing Willco Kuwait (Trading) S.A.K. v. deSavary, 843 F.2d 618, 628 (1st Cir. 1988)). The court also noted that were the e-mail admitted, "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." *Id.* at 99.

[15] *See id.* at 99*; see also* FED. R. EVID. 803(2) (defining an excited utterance as "[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").

[16] *Ferber*, 966 F. Supp. at 99.

[17] *See id.* The judge noted that "[b]ecause the detail, the length, the possibility [the employee] spoke to this [co-worker] before he wrote it, all of it signals to me that whatever he may say about his mind being mush, there's ample time for him to reflect, fabricate." *Id.*

[18] *See id.*

[19] FED. R. EVID. 803(1).

[20] *See Ferber*, 966 F. Supp. at 99. The court explained that the employee'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." *Id.*

[21] *See id.* at 95.

negotiations between the parties, the judge sentenced Ferber to thirty-three months in prison, two years of supervised release, and a one million dollar fine.[22]

7. For many judges and lawyers, Ferber's story is colorful but not unique. Across America, in both criminal and civil proceedings, courts, lawyers, and juries are discovering that information stored in electronic form often contains critical evidence. This article gives a brief overview of some of the legal issues raised by electronic evidence. Part II examines how and why electronic evidence differs from the traditional litigation "paper trail." Part III examines principles governing the discovery of electronic evidence in civil litigation. Part IV addresses certain evidentiary issues that litigants encountered when attempting to use electronic evidence at trial.

II. WHAT IS ELECTRONIC EVIDENCE AND WHY IS IT SO IMPORTANT?

A. What is Electronic Evidence?

8. As a general rule, "electronic evidence" can be any information created or stored in digital form whenever a computer is used to accomplish a task.[23] As this broad definition suggests, electronic evidence may exist 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.[24] Electronic evidence, therefore, may include information databases, operating systems, applications programs, "computer-generated models", electronic and voice mail messages and records, and other information or "instructions residing in computer memory."[25]

B. Why is Electronic Evidence Important?

9. As the *Ferber* case and the expansive definition of electronic evidence suggest, electronic evidence has become critical to civil and criminal proceedings, largely because it differs from the traditional paper trail.

---

[22] *See id.* Ferber also agreed to pay an additional $650,000 to settle fraud charges brought by the Securities and Exchange Commission. *See* Laura Johannes, *Ferber, Ex-Partner at Lazard Freres, Gets Jail Sentence*, WALL ST. J., Dec. 20, 1996, at B5; Leslie Wayne, *Former Partner at Lazard Gets 33-Month Prison Term*, N.Y. TIMES, Dec. 20, 1996, at D5.

[23] *See, e.g.,* Susan E. Davis, *Elementary Discovery, My Dear Watson*, CAL. LAW., Mar. 1996, at 53, 53 (discussing different forms of electronic evidence); Susan J. Silvernail, *Electronic Evidence: Discovery in the Computer Age*, ALA. LAW., May 1997, at 176, 177 (explaining the expanding definition of discoverable "documents" in terms of electronic evidence).

[24] *See* MANUAL FOR COMPLEX LITIGATION § 21.446 (3d ed. 1995).

[25] *Id.*

1. The Volume of Electronic Evidence is Increasing Exponentially

10. One of the key differences between electronic data and traditional paper records is the sheer volume of electronic data and the speed with which electronic data is generated. *Ferber*, and its critical e-mail message, exemplifies this trend. Commentators estimate that in 1994 there were at least 20 million electronic e-mail users in the United States, more than half of whom had been on-line since 1990.[26] Commentators project that by the year 2000, that number will double to more than 40 million e-mail users worldwide, sending an estimated 60 billion messages annually and creating reams of electronic data with a mere click of a button.[27] Many of these records will be generated using employer-owned and employer-operated e-mail systems.[28]

11. E-mail is only one form of electronic evidence. Businesses, organizations, and individuals around the world generate computerized information at amazing speeds, often in lieu of traditional paper records and in circumstances where a paper record might not exist.[29] As one district court recognized, "[c]omputers have become so commonplace that most court battles now involve discovery of computer-stored information."[30]

2. Electronic Evidence Is Difficult to Discard

12. Another key difference between electronic and paper records is the uniquely durable nature of electronic evidence. Those who wish to discard paper records may simply throw out or shred the records. Those who wish to discard digital information do not possess such straightforward solutions. Contrary to popular belief, hitting the delete button does not destroy the computer records, nor is

---

[26] *See, e.g.,* Frank C. Morris, Jr., *E-Mail Communications: The Next Employment Law Nightmare*, CA 30 ALI-ABA 571, 573 (1995).

[27] *See, e.g., id.*

[28] *See id.* As of 1994, ninety percent of all companies with more than 1,000 employees had "some form of e-mail." *Id.*

[29] *See, e.g.*, 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, 2289 (1996) (noting the tremendous growth in the use of e-mail to conduct business and the "technological advances [that] have created a new type of 'virtual office' where paper records" are disappearing and documents increasingly are stored in electronic form).

[30] Bills v. Kennecott Corp., 108 F.R.D. 459, 462 (D. Utah 1985).

it the digital equivalent of throwing out or shredding a hard copy document.[31] Instead, the computer may "mark" the files as space that can be "overwritten" with new information in the future.[32] Deleting a file also may command the computer to mark the record for storage in a "back-up" or archive system, where the machine will save the record for a period of time.[33] Whether the information is marked for overwriting, archived, or dealt with in some other manner, computer experts often can recover supposedly "deleted" information long after the computer user thought it had been destroyed.[34] Thus, electronic data can appear unexpectedly, with the potential to generate litigation or dramatically impact its results.

13. For many, the Iran-Contra affair substantiated the durable nature of electronic evidence. Oliver North and National Security Adviser John Poindexter discovered that deleting a computer file is not the equivalent of shredding a document when computer technicians searched computer back-up tapes and discovered electronic mail messages that had been deleted from e-mail systems used by the Executive Office of the President ("EOP") and the National Security Council ("NSC").[35] E-mail messages also were used by the Tower Commission, congressional investigators looking into the Iran-Contra affair, and by the Department of Justice in connection with its prosecution of Manuel Noriega.[36]

14. Prompted in part by the Iran-Contra scandal and the planned purge of certain material from White House computers during the transition from the Reagan to the Bush Administration, the National Security Archive and other organizations and individuals served on the NSC and the EOP Freedom of Information Act ("FOIA") requests for all relevant materials stored on the electronic communications systems since their installation.[37] These individuals and

---

[31] *See* Davis, *supra* note 23, at 53.

[32] *Id.*

[33] *Id.*

[34] *Id.*

[35] *See* Armstrong v. Bush, 721 F. Supp. 343, 345 n.1 (D.D.C. 1989); Armstrong v. Executive Office of the President, 1 F.3d 1274, 1280, 1283 (D.C. Cir. 1993) (per curiam); s*ee also* Robert Garcia, *"Garbage In, Gospel Out": Criminal Discovery, Computer Reliability and the Constitution*, 38 U.C.L.A. L. REV. 1043, 1083-84 (1991);Philip G. Schrag, *Working Papers As Federal Records: The Need for New Legislation to Preserve the History of National Policy*, 46 ADMIN. L. REV. 95, 109 (1994); Martha Middleton, *A Discovery: There May be Gold in E-Mail*, NAT'L L.J., Sept. 20, 1993, at 1 (calling the Iran-Contra affair the most "frequently cited example of the ramification of electronic media discovery"); Lawrence J. Magid, *As North Learned, Deleted Files are Retrievable*, L.A. TIMES, Aug. 10., 1987, at (Business) 4.

[36] *Armstrong*, 1 F.3d at 1283 n.7.

[37] *See Armstrong*, 721 F. Supp. at 347; *Armstrong*, 1 F.3d at 1280; *See also Opening the*

organizations also filed suit seeking a declaratory judgment that the electronic documents were presidential and/or federal records, and an injunction prohibiting their destruction.[38]

15. The district court concluded that certain items stored in the NSC's computer system were records subject to the Federal Records Act ("FRA")[39] and held that the EOP and NSC's guidelines relating to the preservation of those records were contrary to law under the FRA and arbitrary and capricious.[40] In a lengthy opinion, the Court of Appeals of the District of Columbia affirmed the trial court's ruling that the NSC and EOP guidelines for managing such documents did not comport with the FRA and held that the e-mail communications on the computer systems and back-up tapes constituted "federal records," which the EOP and the NSC could not destroy except in accordance with the FRA.[41]

16. The appellate court reached this conclusion in part because it held that there were "fundamental and meaningful" differences between the electronic e-mail records sought by the plaintiffs and the hard copy printouts of the e-mail messages, required the EOP and NSC to handle the e-mail messages according to the FRA.[42] For example, the court found that although hard copy printouts retained the text of the messages, the e-mail records contained information the hard copy printouts did not, including distribution lists, directories, and acknowledgments of receipts.[43] The court observed that without preserving the *electronic* record, "essential transmittal information relevant to a fuller understanding of the context and import of an electronic communication will simply vanish."[44] Recognizing the importance of electronic copies of documents, the court remanded to the district court to determine whether the NSC guidelines properly distinguished between federal records, subject to both FOIA requests and the FRA's preservation requirements, and/or Presidential records, which are exempt from FOIA requests and subject to a less-

---

Government's Mail: Public Access to National Security Council Records, 35 B.C. L. REV. 1145, 1182-89 (1994).

[38] *See Armstrong*, 1 F.3d at 1280.

[39] The Federal Records Act is a collection of statutes which govern the handling and destruction of documents and records by federal agencies. Federal Records Act, 44 U.S.C. §§ 2101-17, 2901-09, 3101-07, 3301-24 (1996).

[40] Armstrong v. Executive Office of the President, 810 F. Supp. 335, 345-348 (D.D.C. 1993). The court also held the United States Archivist had breached his statutory duty to prevent the destruction of federal records. *See id.* at 342.

[41] *See Armstrong*, 1 F.3d at 1287.

[42] *See Armstrong,* 1 F.3d at 1287.

[43] *See id.* at 1277, 1280.

[44] *Id.* at 1280.

demanding preservation requirement under the Presidential Records Act.[45] The court observed that no court had ever "definitely resolved" the question of whether the NSC is an "agency", and thus, subject to the FOIA[46] and held the record before it did not contain sufficient facts for it to decide that question.[47]

17. On remand, the district court held that the NSC was an agency subject to the FOIA and directed the NSC to comply with both the disclosure requirements of the FOIA and the document preservation rules of the FRA, except in the limited circumstances when a high level official of the NSC acts solely to advise and assist the president.[48] In such cases, the court held that the Presidential Records Act, rather than the FRA, applied.[49] Not surprisingly, the NSC appealed the trial court's determination.[50] In another lengthy opinion, the Court of Appeals reversed the trial court, holding that the NSC was not an agency[51] and thus, did not have to comply with either the FOIA or the FRA.[52] The court, however, did not reconsider its decision that an agency's general electronic records and associated backup tapes could be subject to the FRA.[53]

18. In response to the *Armstrong* decisions, the National Archives Records Administration ("NARA") released new guidelines for the preservation and archiving of certain types of federal e-mail.[54] The NARA also amended its *Managing Electronic Records* handbook to include additional information on identification and retention requirements for federal e-mail records.[55] The NARA's efforts are not,

---

[45] *Id.* at 1296; *see also id.* at 1280.

[46] *Id.* at 1296.

[47] *Id.*

[48] *See* Armstrong v. Executive Office of the President, 877 F. Supp. 690, 700-04, 705-06 (D.D.C. 1995).

[49] *See id.* at 705-06.

[50] *See* Armstrong v. Executive Office of the President, 90 F.3d 553, 555 (D.C. Cir. 1996).

[51] *See id.* at 567.

[52] *See id.*

[53] *See id.* at 556-57.

[54] *See* Electronic Records Management, 36 C.F.R. § 1234 (1996). The regulations outline standards for the creation, use, preservation, and disposition of electronic records. *Id.* §§ 1234.20-1234.34. They also address the selection and maintenance of electronic records, including factors in choosing records for long-term storage. *Id.* § 1234.30(a),(b). Finally, they outline procedures for retaining and disposing of electronic data. *Id.* §§ 1234.32, 1234.34.

[55] *Id.* § 1234.24.

however, complete. The NARA continues to work on providing guidance to federal agencies on how to deal with electronic records.[56]

3. Electronic Evidence Often Contains Informal Materials that do not Exist in Paper Form

19. Other key differences between electronic evidence and paper records are how, when, and why people record information in electronic form. As numerous litigants and commentators have found, people routinely use computers, particularly e-mail, to send draft, informal, or "uncensored" messages they would never "put in writing."[57] As a result, computerized records often contain insights into "corporate knowledge and behavior" and "off-the-cuff" remarks that people would never record on paper.[58] Such remarks are often damaging in litigation.[59]

20. In one well-known securities fraud case, Siemens Solar Industries ("Siemens") sued Atlantic Richfield Co. ("ARCO") for allegedly concealing flaws in a solar power subsidiary that ARCO sold to Siemens.[60] After the sale, Siemens discovered e-mail messages in ARCO's computer system suggesting that ARCO knew at the time of sale that the new technology was not commercially viable.[61] For example, in one e-mail message sent prior to the sale, an ARCO employee commented that "the whole basis of our plan is almost invalid due to the fact that we have been operating under the wrong assumption for ten years."[62] Although the court ultimately dismissed Siemens' securities claims because the statute of limitations had expired,[63] the case illustrates how and why computerized records often contain damaging information that would otherwise be unlikely to surface in paper production.[64]

---

[56] *See Court Enables National Archives to Proceed with Electronic Records Plans* (last modified Sept. 30, 1998) <http://www.nara.gov/nara/pressrelease/nr98-149.html>.

[57] Dreyer, *supra* note 29, at 2289 (citations omitted).

[58] *Id.* at 2289-90; Middleton, *supra* note 35, at 40; *see also* Morris, *supra* note 26, at 586.

[59] *See* Dreyer, *supra* note 29, at 2289; Middleton, *supra* note 35, at 40; Morris, *supra* note 26, at 586-87.

[60] Siemens Solar Indus. v. Atlantic Richfield Co., [1993-1994 Transfer Binder] Fed. Sec. L. Rep. (CCH) ¶ 98,167, at 99,162 (S.D.N.Y. Mar. 16, 1994).

[61] *See Siemens*, [1993-1994 Transfer Binder] Fed. Sec. L. Rep. (CCH) at 99,163.

[62] Morris, *supra* note 26, at 586-87.

[63] *See Siemens,* [1993-1994 Transfer Binder] Fed. Sec. L. Rep. (CCH) at 99,167.

[64] In another well-known case, attorneys discovered an e-mail that Officer Lawrence Powell

21. More recently, employees of Morgan Stanley sued the company for employment discrimination based upon an electronic mail message containing "jokes" about the purported speech patterns of African-Americans.[65] As in the *Siemens* case, it is unlikely that such a "joke" would appear in an official company memorandum or in a more traditional record. The court, however, decided that one racist e-mail was insufficient grounds for finding a hostile work environment and dismissed the complaint.[66]

4. Electronic Evidence is Easy to Manipulate

22. Another important difference between electronic and paper records is the ease with which users may manipulate and exchange electronic information as compared to paper data. One notorious example involved Silicon Valley rivals Borland International ("Borland") and Symantec Corporation ("Symantec").[67] The Borland and Symantec dispute centered around the alleged conduct of Gordon Eubanks, Symantec's president, and Eugene Wang, a former Borland general manager and vice president who had since joined Symantec.[68]

23. Concerned that Wang might have leaked confidential Borland information to outsiders before resigning, Borland executives reviewed Wang's e-mail files shortly after Wang left.[69] Upon finding several messages to Eubanks containing allegedly confidential information, Borland contacted the local police, who then brought in the district attorney's office.[70] A subsequent police search at the

---

sent shortly after his altercation with Rodney King. *See* United States v. Koon, 34 F.3d 1416, 1425 (9th Cir. 1994), *aff'd in part, rev'd in part*, 116 S. Ct. 2035 (1996). In that e-mail, which was sent via the Los Angeles Police Department Mobile Digital Terminal system, Officer Powell commented, "[O]oops," and, "I havent [sic] beaten anyone this bad in a long time." *Id.*

65 Owens v. Morgan Stanley & Co., Inc., No. 96 CIV. 9747(DLC), 1997 WL 403454, at *1 (S.D.N.Y. July 17, 1997); Monique Wise, *N.Y. Firm Sued Over Racial Jokes*, BOSTON GLOBE, Jan. 14, 1997, at C3.

66 *See Owens*, 1997 WL 403454, at *2. The court also based its dismissal on the plaintiff's failure to allege the prima facie elements of an intentional discrimination claim. *See id.* at *3. The plaintiffs were given the option to file an amended complaint. *See id.* at *4.

67 *See* People v. Eubanks, 927 P.2d 310 (Cal. 1996).

68 *See Eubanks*, 927 P.2d. at 312; *see also* Gina Smith, *Betrayal in Silicon Valley*, CAL. LAW., Apr. 1993, at 46, 46.

69 *See Eubanks*, 927 P.2d at 312.

70 *See id.*

homes of both Wang and Eubanks found additional allegedly incriminating materials.[71]

24. In the wake of the searches, Borland sued Eubanks, Wang, and Symantec for the theft of trade secrets[72] and the state filed criminal trade secret charges.[73] Although the court eventually dismissed the criminal charges,[74] and the parties settled Borland's civil suit,[75] Eubanks and Wang were under indictment for more than four years.[76]

25. Perhaps motivated by the Symantec-Borland controversy and other similar cases, President Clinton signed into law the Economic Espionage Act of 1996 ("EEA").[77] The EEA makes the theft of trade secrets by any means, including downloading or uploading computer files, a federal crime.[78] The EEA also provides prison sentences[79] and financial penalties[80] for acts of economic espionage and contains provisions designed to maintain the confidentiality of trade secrets in court proceedings.[81]

III. LEGAL FRAMEWORK GOVERNING ELECTRONIC EVIDENCE

A. Background

---

[71] *See* Smith, *supra* note 68, at 48.

[72] *See id.* at 48.

[73] *See Eubanks*, 927 P.2d at 312.

[74] *See* G. Pascal Zachary, *Symantec CEO is Cleared in Suit About Secrets*, WALL ST. J., Nov. 25, 1996, at B6.

[75] *See Borland Secret Suit Ends*, N.Y. TIMES, Feb. 17, 1997, at 47.

[76] *See* Zachary, *supra* note 74. Symantec attorneys delayed proceedings for so long that the district attorney finally made a motion to dismiss the case, citing "changes in California laws covering trade secrets, the departure of [an employee] from Borland, and the staleness of the information at issue." *Id.* In addition, Symantec lawyers questioned Borland's payment of $13,000 for costs of the government's investigation. *See Eubanks*, 927 P.2d at 312; *see also* Zachary, *supra* note 74. These questions resulted in an appeal to the California Supreme Court. *See Eubanks*, 927 P.2d at 312.

[77] *See* Economic Espionage Act of 1996 § 101, 18 U.S.C.A. §§ 1831-39 (West Supp. 1998).

[78] *Id.* § 1832(a).

[79] *See id.* §§ 1831, 1832.

[80] *See id.* §§ 1831, 1832.

[81] *See id.* § 1835.

26. Although questions concerning electronic evidence have received much attention lately, the legal framework governing the discovery and use of electronic evidence at trial actually dates back to the late 1960s and early 1970s, when businesses began to use computers in larger numbers. By 1970, the Advisory Committee, which drafts the Federal Rules of Civil Procedure, recognized that existing discovery rules did not adequately address if, and under what circumstances, litigants could discover digital information.[82] Consequently, the Committee sought to amend the definition of "document" in Federal Rule of Civil Procedure 34(a) to include electronic data.[83] As finally adopted by Congress, amended Rule 34(a) defined "document" to include "data compilations from which information can be obtained, translated, if necessary, by the respondent through detection devices into reasonably usable form."[84]

27. The Advisory Committee intended the amendments to Rule 34(a) to bring the Federal Rules of Civil Procedure into the computer age.[85] The Advisory Committee observed:

> The [newly] inclusive description of "documents" is revised to accord with changing technology. It makes it clear that Rule 34 applies to electronic data compilations from which information can be obtained only with the use of detection devices, and that when the data can as a practical matter be made usable by the discovering party only through the respondent's devices, respondent may be required to use his devices to translate the data into usable form. In many instances, this means that the respondent will have to supply a print-out of computer data.[86]

28. Although the Advisory Committee intended to make electronic data discoverable, the Committee recognized that identifying and producing relevant electronic data could impose severe burdens on the producing party.[87] Consistent with traditional discovery principles, the Committee observed that courts have the power under Rule 26(c) of the Federal Rules of Civil Procedure to consider the

---

[82] *See* 8A CHARLES ALAN WRIGHT ET. AL., FEDERAL PRACTICE AND PROCEDURE § 2218 (2d ed. 1994).

[83] *See id.*

[84] FED. R. CIV. P. 34(a)(1).

[85] *See* WRIGHT, *supra* note 82, § 2218.

[86] FED. R. CIV. P. 34(a) advisory committee notes.

[87] *See id.*

burden and expense on the parties in deciding whether to compel the production of electronic data.[88]

B. Trends

29. In the years since the amendment to Rule 34(a), courts and litigants have clashed over the reasonableness of the burden and the expense of discovering computer-based information. For example, in *In re Brand Name Prescription Drugs Antitrust Litigation,* litigants disagreed about the "reasonable cost" of searching for and producing potentially relevant e-mail.[89] The dispute centered around e-mail communications among the defendant's employees.[90] Both sides agreed that the records were discoverable.[91] The plaintiffs argued that they were entitled to the e-mail records because the records were relevant and available; they had been stored in back-up form on the defendant's computer system.[92] The defendant responded that the plaintiffs should pay the approximately $50,000 it would cost to search the 30 million pages of computer data required to satisfy plaintiffs' request.[93]

30. The court rejected the defendant's arguments and ordered the defendant to produce the relevant e-mail at the defendant's expense.[94] The court acknowledged that the question of who should pay for the retrieval and production of computer-stored records was "complicated."[95] Although recognizing that "it seems unfair to force a party to bear the lofty expense attendant to creating a special computer program for extracting data responsive to a discovery request," the court nonetheless observed that when "a party chooses an electronic storage method, the necessity for a retrieval program or method is an ordinary and foreseeable risk."[96] The court held that the "normal and reasonable translation of electronic data into a form usable by the discovering party should be the ordinary and foreseeable burden" borne by the

---

88 *See id.*

89 In re Brand Name Prescription Drugs Antitrust Litig., No. 94 C 897 MDL 997, 1995 U.S. Dist. LEXIS 8281, at *1 (N.D. Ill. June 13, 1995).

90 *See id.*

91 *See id.*

92 *See id.* at *1-2.

93 *See id.*

94 *See id.* at *8.

95 *Id.* at *5.

96 *Id.*

producing party unless "extraordinary hardship" would result.[97] The court also held that a contrary holding would undermine the "guiding principle" that information stored with new technology should be as accessible as traditionally discoverable documents.[98]

31. In addition to the question of who should bear the costs of production, courts and litigants have disagreed about whether computerized information must be produced in a particular format. In one widely cited case, *National Union Electric Corp. v. Matsushita Electric Industrial Co.,* the court ordered a party to create and produce a computer-readable magnetic tape copy of information previously produced in hard-copy form.[99] The conflict arose when the defendant served interrogatories asking for detailed information about the plaintiff's products and, in response, the plaintiff produced a lengthy computer printout.[100] The defendants argued that they could not effectively analyze the printout unless they entered it manually into their computer system, an expensive and time-consuming task.[101] To avoid such time and expense, the defendants asked the court to order the plaintiff to create and produce a computer-readable tape containing the information previously produced in hard-copy form.[102] Although the defendants' offered to pay for the cost of producing the magnetic tape, the plaintiff refused to do so.[103]

32. Citing the amended definition of documents in Federal Rule of Civil Procedure 34(a) and the accompanying Advisory Committee notes, Judge Harold Becker ordered the plaintiff to create a computer-readable magnetic tape.[104] Judge Becker noted that "the only difference between what defendants already have [the hard-copy computer printout] and what they request [the computer-readable tape] is that a computer cannot read what [the plaintiff] has already produced," and thus the difference was "mechanical, not qualitative."[105] Accordingly, the court required the

---

97 *Id.* at *5-6.

98 *See* id. at *5.

99 National Union Elec. Corp. v. Matsushita Elec. Indus. Co., 494 F. Supp. 1257, 1258, 1262 (E.D. Pa. 1980).

100 *See id.* at 1258.

101 *See id.*

102 *See id.* at 1258-59.

103 *See id.*

104 *See id.* at 1262-63. Judge Becker also cited a number of cases in which courts compelled the production of computerized records. *See id.* at 1261.

105 *Id.* at 1260.

plaintiff to produce the data in its "usable form," the computer-readable tape, even though plaintiff previously had produced the information in print.[106]

C. Litigants Who Fail to Produce Electronic Evidence Risk Sanction

33. Because electronic data is discoverable under federal and state rules of procedure, litigants who fail to produce electronic evidence risk court sanctions. In *Crown Life Insurance Co. v Craig,* for example, the Seventh Circuit upheld the imposition of sanctions against a litigant who failed to produce relevant computer records.[107] Craig asked Crown to produce certain categories of documents, which Crown produced in hard-copy form followed by an affidavit stating that it had turned over all relevant materials.[108] During an earlier deposition, however, a Crown employee referred to relevant computer records that were not produced.[109] Craig sought to compel production of the records, but Crown repeatedly refused, claiming that the data remained in raw form and was inaccessible at the time of Craig's request.[110] Crown also argued that it was not required to produce the records because Craig had requested only "written documents."[111]

34. Faced with Crown's use of, but refusal to produce, the computer records, the court upheld the trial court's ruling prohibiting Crown from using or relying upon the information contained in the computer records.[112] The court of appeals held that Crown had a duty to produce the records, regardless of their form, and that Craig's request for written documents, with its request for various other forms of

---

106 *Id.* at 1262 (quoting FED. R. CIV. P. 34(a)); *see also* Anti-Monopoly, Inc. v. Hasbro, Inc., 94 CIV. 2120, 1995 WL 649934, at *1 (S.D.N.Y. Nov. 3, 1995) ("The law is clear that data in computerized form is discoverable even if paper 'hard copies' of the information have been produced, and that the producing party can be required to design a computer system to extract the data from its computerized business records, subject to the Court's discretion as to the allocation of the costs of designing such computer program."); Haworth, Inc. v. Herman Miller, Inc., No. 1:92 CV 877, 1995 WL 465838, at *1 (W.D. Mich. Apr. 20, 1995) (holding that under Federal Rule of Civil Procedure 34(a), respondent to a discovery request bears the burden of translating computer data into a form that the requesting party can use).

107 Crown Life Ins. Co. v. Craig, 995 F.2d 1376, 1377, 1380-84 (7th Cir. 1993).

108 *See id.* at 1378-80.

109 *See id.* at 1379.

110 *See id.* at 1379-81.

111 *Id.* at 1382.

112 *See id.* at 1384.

information, provided an adequate basis for the production of the computer records at issue.[113]

IV. USE OF ELECTRONIC EVIDENCE AT TRIAL

35. Just as the federal and state rules of procedure apply to electronic data, so too do the federal and state rules of evidence.[114] Proponents of the use of electronic evidence at trial typically encounter two obstacles to the admission of electronic data into evidence; hearsay[115] and foundation objections. As *Ferber* demonstrates, proponents of electronic evidence may put forth a number of creative arguments to overcome such objections, including arguments based on the present sense impression,[116] business records,[117] public records,[118] and the catch-all exceptions to the hearsay rule.[119]

36. Most often, litigants seek to introduce electronic records into evidence using the business records exception to the hearsay rule.[120] Under this rule, courts may admit into evidence any "memorandum, report, record, or data compilation, in

---

[113] *See id.* at 1383.

[114] *Cf.* MANUAL FOR COMPLEX LITIGATION, *supra* note 24, § 21.446.

[115] The Federal Rules of Evidence's definition of hearsay includes any "statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted." FED. R. EVID. 801(c)*; see also* Dreyer, *supra* note 29, at 2299 (citations omitted) (asserting that the hearsay rule is one of the most common barriers to the admissibility of electronic evidence).

[116] *See* FED. R. EVID. 803(1).

[117] *See* FED. R. EVID. 803(6).

[118] *See* FED. R. EVID. 803(8).

[119] *See* FED. R. EVID. 803(24), 804(b)(5).

[120] As a general rule, a court may admit a record into evidence pursuant to the business records exception to the hearsay rule if the record was: (1) made by someone with personal knowledge, or from information provided by someone with both personal knowledge and a duty to report; (2) made in the regular course of business, at or near the time the recorded event occurred; and (3) the business regularly makes such records. *See generally* FED. R. EVID. 803(6). In many instances, the party arguing in favor of the business record exception must demonstrate that the records were or are: "(1) kept pursuant to a routine procedure designed to assure their accuracy[;] (2) . . . created for motives that tend to assure accuracy (e.g., not including those prepared for litigation)[;] and (3) . . . not themselves mere accumulations of hearsay" falling within the ambit of the business records exception to the hearsay rule. United States v. Cestnik, 36 F.3d 904, 909-10 (10th Cir. 1994) (citations and internal quotations omitted).

any form" that satisfies the foundation requirements.[121] According to the Advisory Committee notes, "[t]he expression 'data compilation' is used as broadly descriptive of any means of storing information other than the conventional words and figures in written or documentary form. It includes, but is by no means limited to electronic computer storage."[122]

37. When the Advisory Committee first stated that a business record could include computer-based information, at least one commentator expressed concern that the term "data compilation" would incorporate "the entire process of computer system from the reception of data . . . to the final printing-out of the information."[123] Today however, most courts do not harbor such fears.[124] As one court noted, "'it is immaterial that the business record is maintained in a computer rather than company books', assuming that the proponent lays a proper foundation for admissibility under the business records exception to the hearsay rule."[125]

38. In addition to the business records exception, courts and litigants also rely on the public records exception to the hearsay rule.[126] Almost twenty years ago, the Ninth Circuit in *United States v. Orozco* held that certain government computer records qualified as "public records," and, therefore, were properly admitted into evidence by the trial court.[127] Recently, the Ninth Circuit in *Hughes v. United States* held that Internal Revenue Service documents generated by a computer were admissible as public records.[128]

39. Finally, courts and litigants frequently rely on the "catch-all" exceptions to the hearsay rule to overcome hearsay objections to otherwise reliable electronic evidence. In *Palmer v. A.H. Robins Co.,* the Colorado Supreme Court admitted

---

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

122 FED. R. EVID. 803(6) advisory committee's notes.

123 Colin Tapper, *Evidence From Computers*, 8 GA. L. REV. 562, 604 (1974).

124 *See, e.g.*, *United States v. Goodchild*, 25 F.3d 55, 60-62 (1st Cir. 1995) (admitting under Fed. R. Evid. 803(6) computer printouts memorializing telephone conversations); *Cestnik*, 36 F.3d at 909-910 (admitting computer generated money transfer records into evidence as business records); *United States v. Brisco*, 896 F.2d 1476, 1493-1495 (7th Cir. 1990) (admitting computerized telephone records as business records).

125 United States v. Catabran, 836 F.2d 453, 457 (9th Cir. 1988) (quoting United States v. Georgia, 420 F.2d 889, 893 n.11 (9th Cir. 1969)); *see also* Dreyer, *supra* note 29 at 2301-2314 (containing a detailed discussion of the admissibility of e-mail under the business records exception to the hearsay rule).

126 *See, e.g.,* Hughes v. United States, 953 F.2d 531, 539-40 (9th Cir. 1992) (citations omitted).

127 United States v. Orozco, 590 F.2d 789, 793-94 (9th Cir. 1979).

128 *Hughes*, 953 F.2d at 540.

computer records into evidence under the common law "general hearsay exception," explaining that the data, while not a business record, was sufficiently reliable to be admitted into evidence.[129]

40. In deciding whether to admit the electronic data into evidence, courts must confront concerns about the reliability, accuracy, and authenticity of computer records.[130] For example, the *Manual for Complex Litigation* (the "*Manual*") notes that the accuracy of computerized records may be impaired as a result of computer programming errors, equipment malfunction, and data entry errors.[131] The *Manual* also acknowledges that the volume of relevant electronic data may impair a court's ability to verify the information's integrity.[132]

41. In response to such concerns, some older decisions required litigants using computer-based evidence to offer a more extensive foundation than that required for conventional records.[133] Thus, in *United States v. Scholle*, the court held that a proponent of electronic evidence must delineate "the original source of the computer program . . . and the procedures for input control including tests used to assure accuracy and reliability" as part of the foundation to ensure the reliability of the evidence.[134] Other commentators have suggested that courts should require proponents of computer evidence to provide detailed foundation evidence that the proffered electronic evidence is the product of standard industry computer practices.[135]

---

[129] Palmer v. A.H. Robins Co., Inc., 684 P.2d 187, 202 (Colo. 1984); *cf.* Karme v. Commissioner, 673 F.2d 1062,1064-65 (9th Cir. 1982) (admitting foreign bank records that appeared trustworthy, but did not constitute business records).

[130] *See* MANUAL FOR COMPLEX LITIGATION, *supra* note 24, § 21.446; *see also* CHRISTOPHER B. MUELLER & LAIRD C. KIRKPATRICK, 4 FEDERAL EVIDENCE § 446 (1994) ("Some allowance accommodation is required because of the differences between the conventional account book and the electronic medium of the computer.").

[131] MANUAL FOR COMPLEX LITIGATION, *supra* note 24, § 21.446.

[132] *Id.*

[133] *See, e.g.*, United States v. Scholle, 553 F.2d 1109, 1125 (8th Cir. 1977) (requiring more extensive foundation for computer storage); United States & Fidelity Guaranty Co. v. Young Life Campaign, Inc., 600 P.2d 79, 81 (Colo. App. 1979) (noting that the foundation for computer records, while similar to that for other business records, requires "special application").

[134] *Scholle*, 553 F.2d at 1125.

[135] *See generally* Rudolph Peritz, *Computer Data and Reliability: A Call For Authentication Of Business Records Under The Federal Rules Of Evidence*, 80 NW. U. L. REV. 956 (1986). Professor Peritz also suggests that proponents of computer-based evidence should be required to demonstrate, through expert testimony, that the computer program at issue functions reliably and accurately. *See id.* at 961.

42. More recently, courts have rejected the notion that proponents of electronic evidence must meet heightened foundation requirements in every case. In *United States v. Vela,* the Fifth Circuit upheld the trial court's admission of electronic evidence even though the proponent's foundation witness did not identify the type of computers used to generate the records and did not verify that the computers were in proper operating condition.[136] The court explained that "[t]he failure to certify the brand or proper operating condition of the machinery involved does not betray a circumstance of preparation indicating any lack of trustworthiness."[137] The court suggested that the opponent could argue that the records were unreliable and unbelievable after the records were admitted.[138]

V. PRACTICAL ADVICE FOR LAWYERS USING ELECTRONIC EVIDENCE

43. Whatever theory of admissibility courts and litigants use, the unique characteristics of electronic evidence—its volume, durability, frequently uncensored nature, and ease of transmission and manipulation by users—make it a critical source of information. Attorneys may wish to consider a few basic steps to prepare for discovery and use of such information at trial. For example, attorneys may wish to advise clients to inventory potential sources of electronic evidence and establish an electronic records management policy. Such a policy might include guidelines for the preservation of various types of company data and the periodic purging of nonessential records.

44. Lawyers may also wish to advise clients of the peculiar characteristics of electronic records, namely e-mail. In so doing, clients can minimize the risk of improper e-mail communications. Attorneys may also wish to advise clients to implement a computer and/or e-mail policy designed to guard against improper or unauthorized use of the computer systems. Finally, attorneys should develop plans for the discovery and use of electronic data in litigation. Such a plan might include discovery requests and depositions designed to unearth relevant electronic data and a trial strategy that incorporates and capitalizes on the potential treasure trove of electronic information.

---

[136] United States v. Vela, 673 F.2d 86, 90 (5th Cir. 1982); *see also* United States v. Moore, 923 F.2d 910, 914 (1st Cir. 1991) (finding that the head of the bank's customer loan department is a competent foundation witness for computerized consumer loan records compiled by an independent service bureau which is connected to the bank via telephone); United States v. Bonallo, 858 F.2d 1427, 1436 (9th Cir. 1988) (rejecting the argument that computer records are inherently untrustworthy, and, thus, inadmissible, because they can be altered); People v. Lugashi, 252 Cal. Reptr. 434, 440-443 (Cal. Ct. App. 1988) (admitting computer records under the business records exception to the hearsay rule does not require testimony from a computer expert as to the computer's technical reliability).

[137] *Vela*, 673 F.2d at 90.

[138] See *id.*

45. Regardless of the options selected, lawyers and litigants who fail to plan for the discovery of electronic data risk overlooking key pieces of evidence and encountering potentially damaging disclosures. The days of the "paper trail" have ended.