Michigan Law Review

Volume 104 | Issue 1

2005

"Electronic Fingerprints": Doing Away with the Conception of Computer-Generated Records as Hearsay

Adam Wolfson
University of Michigan Law School

NOTE

"Electronic Fingerprints": Doing Away with the Conception of Computer-Generated Records as Hearsay

*Adam Wolfson**

INTRODUCTION

"Every statement has a dual nature, it is both a fact and the assertion of fact, and on the guise in which it appears depends whether it is original evidence or hearsay, the respectable Dr. Jekyll is received with a becoming respect, but the disrespectable Mr. Hyde is kicked ignominiously out of court."[1]

One night, in the hours just before daybreak, the computer servers at Acme Corporation's headquarters quietly hum in the silence of the office's darkened hallways. Suddenly, they waken to life and begin haphazardly sifting through their files. Several states away, a hacker sits in his room, searching through the mainframe via an internet connection. His attack is quick—lasting only a short five minutes—but the evidence of invasion is apparent to Acme's IT employees when they come in to work the next morning.

Nearly a year later, federal prosecutors bring suit in the federal district court against the person they believe to be the hacker. During the trial, several witnesses testify about the attack and its resulting damage. The only piece missing is the hacker's identity. In order to prove this, the prosecution wishes to introduce the mainframe's records of the attack, which document both the source of the invasion and the signature of the computer that conducted the entire event. A cursory check by computer specialists matched these records with the accused hacker's personal computer.

The prosecutors lay sufficient foundation to authenticate the records and then move to have them admitted into evidence.

"Objection!" states the defense counsel.

"On what grounds?" replies the judge.

"Hearsay, your Honor. The computer records the prosecution is attempting to introduce do not satisfy the business records exception under Federal Rule of Evidence 803(6). They were created in response to an attack, and were not maintained in the ordinary course of business. Consequently, they cannot be admitted under the Rules of Evidence and must be deemed inadmissible."

---

* J.D. candidate, December 2005, University of Michigan Law School. Special thanks to Professor Orin Kerr of George Washington University Law School for both help on the topic idea of this Note as well as his continuing input on its development throughout the writing process.

1. J.B.C. TREGARTHEN, THE LAW OF HEARSAY EVIDENCE 10–11 (1915).

The judge directs his attention to the prosecution.

"Counsel, are there any other exceptions these records fall under?"

"No, your Honor."

"Objection sustained."

This result may seem inequitable, but it is entirely possible given the current majority view on the nature of computer-generated records.

In order to understand this conception, it is important to first lay out what constitutes hearsay, the rationale for the rule, and the exceptions for computer-generated records. Hearsay is "a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted."[2] At its heart, the hearsay rule merely aims to exclude unreliable evidence at trial.[3] This "unreliability" is considered to be a product of several factors: (1) hearsay evidence is often not the best evidence of a fact because more direct statements or other evidence have far more probative value; (2) a hearsay statement is almost never made under oath; (3) other parties do not have a chance to cross-examine the maker of a hearsay statement; and (4) with a hearsay statement, the judge and jury do not get an opportunity to observe the demeanor of the declarant for credibility purposes.[4]

American courts do not admit hearsay because it generally creates an unreliable "chain of inferences" that is unacceptable when the aim of a trial is accurate fact finding.[5] Most inaccuracies are the result of "the four testimonial infirmities of ambiguity, insincerity, faulty perception, and erroneous memory."[6] Another danger hearsay raises is that it allows juries to take the statement in question out of context, which can completely change the

---

2. FED. R. EVID. 801(c). A "statement" is "(1) an oral or written assertion or (2) nonverbal conduct of a person, if it is intended by the person as an assertion." FED. R. EVID. 801(a). A "declarant" is "a person who makes a statement." FED. R. EVID. 801(b).

3. *See* Lilly v. Virginia, 527 U.S. 116, 131 (1999); IRVING YOUNGER, HEARSAY: A PRACTICAL GUIDE THROUGH THE THICKET 201 (1988) (stating that hearsay is only a rule against unreliable evidence); G. MICHAEL FENNER, THE HEARSAY RULE 4–5 (2003) ("Underneath it all, truth is the objective of the hearsay rule: The hearsay rule is about keeping out evidence that is so unreliable that it does not help us find the truth.").

4. ANDREW L.-T. CHOO, HEARSAY AND CONFRONTATION IN CRIMINAL TRIALS 11–13 (1996). These four factors are applicable in a variety of ways, each having more weight than the others depending on the case. Factors (1), (2) and (3) are the historical rationales for the rule. *Id.* at 11. Factor (4) has only recently risen to prominence as an accepted reason for upholding the rule as a whole. *Id.*

5. Laurence H. Tribe, *Triangulating Hearsay*, 87 HARV. L. REV. 957, 958 (1974). Tribe's analysis parallels that of CHOO, *supra* note 4, but goes a step further in describing the fallacies of eyewitness testimony in general. Tribe, *supra*, at 957–61. This, along with a triangular graph included in the article, helps to create a "heuristic device" for understanding the problems associated with admitting hearsay statements into evidence. *Id.*

6. Tribe, *supra* note 5, at 958. These four infirmities refer to the general problems with any set of in-court testimony. "Ambiguity" refers to statements that need clarification and can be misconstrued on a subsequent retelling. CHOO, *supra* note 4, at 84. "Insincerity," as the label implies, is the "deliberate lies" some declarants tell in order to alter others' perceptions of the facts. *Id.* "Faulty perception" and "erroneous memory" are both phenomena that occur as a matter of course in eyewitness testimony. *Id.* For further discussion of these "hearsay dangers," please see CHOO, *supra* note 4.

character of the assertion.[7] Because in-court analysis of testimony largely remedies these infirmities, we rightfully exclude hearsay evidence.[8]

With this logic in mind, it is clear why assertive documents and most types of records are textbook examples of hearsay. After all, a "statement" does not always have to be oral.[9] If the document is introduced because its proponent claims that the information contained therein is true, it is the written equivalent of an oral assertion and must therefore meet a valid hearsay exception.[10]

When introducing computer-generated documents, lawyers most commonly use the business records exception.[11] An extension of the historical "shopbook rule,"[12] this exception was a response to the advent of the corporate form, which created a heretofore unseen phenomenon: a trial where no physical person was being sued.[13] Since testimony of the corporation's inner workings necessarily incorporated voluminous business records, courts battled with the problem of a rigid hearsay rule that had no true on-point exceptions.[14] In 1936, the Commonwealth Fund Act[15] offered the first codification of the business records exception.[16] The Act's proponents argued that unaltered business records were unusually reliable because *businesses themselves* rely on these records for day-to-day operations.[17]

---

7. Williamson v. United States, 512 U.S. 594, 598 (1994).

8. *See* Tribe, *supra* note 5, at 960–61.

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

10. *Id.*; FENNER, *supra* note 3, at 10 (stating that conduct may be a "statement" if the actor intends it to be such).

11. FED. R. EVID. 803(6); Ronald J. Marzullo-La Russa, *Computer-Generated Evidence: Admissibility*, 20 REV. JUR. U.P.R. 121, 129 (1985).

12. RICHARD O. LEMPERT ET AL., A MODERN APPROACH TO EVIDENCE: TEXT, PROBLEMS, TRANSCRIPTS AND CASES 603 (3d ed. 2000) [hereinafter LEMPERT ET AL.]. According to LEMPERT ET AL.,

> [T]he "shopbook rule" is rooted in the early English custom that allowed a merchant doing business on account to enter his books into evidence to prove the defendant owed him money.
>
> . . .
>
> To ensure reliability, different jurisdictions required one or more of the following guarantees: (1) a "supplemental oath" taken by the merchant as to the justness of his accounts, (2) inspection by the court to determine if the books were fairly kept in the regular course of business, (3) testimony that the merchant kept honest books, and (4) proof apart from the books that at least some portion of the goods charged to an account had been actually delivered.

Id.; *see also* JOHN W. STRONG, 2 MCCORMICK ON EVIDENCE § 285, at 249–50 (5th ed. 1999) [hereinafter MCCORMICK].

13. *See* YOUNGER, *supra* note 3, at 111–13 (discussing the effect of the Industrial Revolution and increased need for business records on evidentiary necessities and rules).

14. *Id.*

15. Federal Business Records (Commonwealth Fund) Act, 28 U.S.C. § 1732 (2000).

16. FED. R. EVID. 803 advisory committee's note.

17. *Id.*; *see also, e.g.*, United States v. Snyder, 787 F.2d 1429, 1433–34 (10th Cir. 1986) ("The business records exception is based on a presumption of accuracy, accorded because the information is part of a regularly conducted activity, kept by those trained in the habits of precision, and customarily checked for correctness, and because of the accuracy demanded in the conduct of the nation's business.").

Congress, commentators, and courts agreed with this rationale's persuasiveness,[18] and the Act passed with minor controversy.[19]

The modern version of the exception deems a "memorandum, report, record, or data compilation" admissible if it is "kept in the course of a regularly conducted business activity."[20] This is a very broad rule[21] because the term "business" includes any "business, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit."[22] Examples of this broadness in practice include courts admitting as "business records" a blackjack dealer's tip log[23] and calendar notations of daily illegal drug sales.[24]

The other major exception under which computer records are admitted is the public records exception.[25] Under this exception, records must originate from "public offices or agencies"[26] and set forth (1) the activities of the office, (2) matters observed as part of office employees' jobs, or (3) factual findings resulting from an investigation conducted by the office.[27] This exception is predicated on the belief that (1) public records are just as trustworthy as business records because the government relies on them for proper functioning, (2) public employees usually record their activities properly, and (3) government employees are unlikely to remember details independent of the record.[28] Foundation of the records' admissibility, as with

---

18. FED. R. EVID. 803 advisory committee's note.

19. *Id.*

20. FED. R. EVID. 803(6). Courts have long held computer records admissible as business records, given the proper foundation. *See, e.g.*, United States v. Salgado, 250 F.3d 438, 452 (6th Cir. 2001) (requiring that computer records satisfy the business records exception); Hardison v. Balboa Ins. Co., 4 Fed. Appx. 663, 669 (10th Cir. 2001) (stating that computer records need to be verified pursuant to Federal Rule of Evidence ("FRE") 901); United States v. Moore, 923 F.2d 910, 914 (1st Cir. 1991) (holding that part of computer records introduced at trial were business records); United States v. Miller, 771 F.2d 1219, 1237 (9th Cir. 1985) (holding that computer records must satisfy the business records exception before being admitted); United States v. Glasser, 773 F.2d 1553, 1559 (11th Cir. 1985) (setting the situations in which computer records may be admitted as business records); Perma Research & Dev. v. Singer Co., 542 F.2d 111, 125 (2d Cir. 1976) (Van Graafeiland, J., dissenting) (explaining that the business records exception is legitimately applied to computer evidence). The foundation is laid when the party seeking to admit the records (1) introduces evidence that the computer program is sufficiently accurate for reliability purposes, and (2) establishes that the business relied on the records for day-to-day operations. *Salgado*, 250 F.3d at 453. The party need not provide expert testimony as to the mechanical accuracy of the program. *Id.* Instead, proper foundation and a witness on the stand who is a legitimate representative of the business *and* is familiar with the business' recordkeeping practices will suffice for business records purposes. *Id.* at 451–52; *Hardison*, 4 Fed. Appx. at 669; *Miller*, 771 F.2d at 1237.

21. 2 MCCORMICK, *supra* note 12, § 288.

22. 2 *Id.*

23. Keogh v. Comm'r of Internal Revenue, 713 F.2d 496 (9th Cir. 1983).

24. United States v. Lizotte, 856 F.2d 341 (1st Cir. 1988).

25. FED. R. EVID 803(8); Marzullo-La Russa, *supra* note 11, at 130–31.

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

27. *Id.*

28. FED. R. EVID. 803(8) advisory committee's note. The logical extension of this rationale is that public officials have an inordinately large number of records to maintain. It is nearly impossible to expect them to remember what would normally be just another number or figure entered into the ledger. Conse-

business records, may be established by a layperson representative of the government agency.[29]

A third conceivably applicable exception under which computer records may be admitted is the "residual" provision found in Federal Rule of Evidence ("FRE") 807 if there are sufficient "circumstantial guarantees of trustworthiness" and the piece of hearsay is offered as evidence of a material fact without causing undue prejudice against the opposing party.[30] A hearsay proponent who employs this exception must give opposing parties "a fair opportunity" to prepare for the evidence's inclusion in the record.[31] Unfortunately for parties who have no other recourse but FRE 807, this "catch-all" exception is seldom employed because judges are uncomfortable with its extremely powerful and flexible nature.[32]

Almost all federal courts,[33] and many state courts, regard all computer records as hearsay that may only be admitted under the business records[34] or public records exceptions.[35] These courts follow the dissent in *Perma Research v. Singer Co.*, a 1976 Second Circuit decision that considered the

---

quently, courts are willing to trust public records because (1) there is a presumption towards trusting government sans evidence to the contrary, (2) public officials have little incentive to lie when keeping their records, (3) these records are necessary for governmental functions and, as a result, are more likely to be accurate, and (4) there are very few other ways that the records would be admitted even though they have potentially high probative value. *See id.*

29. *See* United States v. Miller, 771 F.2d 1219, 1237 (9th Cir. 1985) (stating that custodians of computer records need not be intimately familiar with their programs in order to still offer proper foundation for the evidence).

30. FED. R. EVID. 807.

31. *Id.*

32. *See* CHARLES B. GIBBONS, FEDERAL RULES OF EVIDENCE WITH TRIAL OBJECTIONS 129–35 (2003); Russo v. Abington Mem'l Hosp., No. CIV.A.94-195, 1998 WL 967568, at *3 (E.D. Pa. Nov. 18, 1998) ("A catch-all rule such as Rule 807 must be sparingly invoked, lest its potential breadth swallow the carefully crafted narrowness of the enumerated exceptions."). Of the major cases involving computer records in federal courts, not one instance exists where such records were admitted under the residual exception. The only case—state or federal—that discusses the relationship between computer records and FRE 807, *Russo*, seems to suggest that computer records could legitimately be admitted under this Rule, but only after the proponent party demonstrates the records in question possess a *very high* level of trustworthiness. *See id.* at *3.

33. United HealthCare Corp. v. Am. Trade Ins. Co., 88 F.3d 563 (8th Cir. 1996); United States v. Pendergrass, 47 F.3d 1166 (4th Cir. 1995); Potamkin Cadillac Corp. v. B.R.I. Coverage Corp., 38 F.3d 627 (2d Cir. 1994); United States v. Cestnik, 36 F.3d 904 (10th Cir. 1994); United States v. Blackburn, 992 F.2d 666 (7th Cir. 1993); United States v. Moore, 923 F.2d 910 (1st Cir. 1991); United States v. Spine, 945 F.2d 143 (6th Cir. 1991); United States v. Hutson, 821 F.2d 1015 (5th Cir. 1987); United States v. Miller, 771 F.2d 1219 (9th Cir. 1985); United States v. Glasser, 773 F.2d 1553 (11th Cir. 1985); United States v. Kim, 595 F.2d 755, 762 (D.C. Cir. 1979); United States v. Liebert, 519 F.2d 542, 547 (3d Cir. 1975). The only two federal cases that take the opposite view are *United States v. Rollins*, No. ACM34515, 2004 WL 26780 (A.F. Ct. Crim. App. Dec. 24, 2003) and *United States v. Duncan*, 30 M.J. 1284 (N-M. Ct. Crim. App. 1990). The U.S. Supreme Court has not addressed the issue.

34. FED. R. EVID. 803(6). Computer-generated records introduced at trial are often printouts which purport to show that a party called a certain telephone number or used a certain credit card. *See, e.g.*, United States v. Salgado, 250 F.3d 438, 452 (6th Cir. 2001).

35. FED. R. EVID. 803(8). Federal courts have been quick to admit governmental computer records under this Rule. *See, e.g.*, United States v. Spine, 945 F.2d 143, 149 (6th Cir. 1991).

admission of computer simulations of anti-skid devices.[36] Noting various hearsay sources Perma Research's experts relied upon in analyzing the simulations' results and conclusions, Judge Van Graafeiland stated in his dissent that he was "not prepared to accept the product of a computer as the equivalent of the Holy Writ."[37] Further, he argued that computers' "ability to package hearsay and erroneous or misleading data in an extremely persuasive format" required that computer evidence satisfy a hearsay exception in order to be admitted.[38] Judge Van Graafeiland's solution contained two approaches: (1) for computer records submitted as business records, simply use the business records exception; and (2) when a computer program is used to produce information specifically for litigation, require the proponent party to make the computer program in question available to the opposing party before trial.[39]

Notably absent in Judge Van Graafeiland's analysis is the possibility that computer evidence might *not* represent human assertions and therefore not constitute hearsay. The issue of computer-generated data, such as the IP log at Acme Corp., was not addressed in the case. Considering *Perma* was decided in 1976, when personal computer technology was only beginning to develop,[40] it is likely that the court was not aware of such records.

Almost all federal courts and most state courts apply Judge Van Graafeiland's analysis to all computer records, regardless of source.[41] These courts are stuck in a hearsay rut; while they often rightly define the records as computer-generated—or, at least use the words "computer-generated"[42]—the final logical step on why self-generated records are *not* hearsay is never reached.[43]

---

36. 542 F.2d 111 (2d Cir. 1976). The case revolved around a dispute regarding two contracts for automotive anti-skid devices. One of the issues at trial was whether the devices performed properly, and Perma Research introduced computer simulations that presumably showed that the devices did not function well. On appeal, the Second Circuit reviewed the simulations and the experts themselves.

37. *Id.* at 121 (Van Graafeiland, J., dissenting).

38. *Id.* at 126 (Van Graafeiland, J., dissenting) (quoting Jerome J. Roberts, *A Practitioner's Primer on Computer-Generated Evidence*, 41 U. CHI. L. REV. 254, 279 (1974)).

39. *Id.* at 125 (Van Graafeiland, J., dissenting).

40. Ken Polsson, *Chronology of Personal Computers*, *at* http://www.islandnet.com/~kpolsson/comphist/ (last updated July 26, 2005).

41. *See* cases cited *supra* note 33 and accompanying text.

42. United States v. Salgado, 250 F.3d 438, 452 (6th Cir. 2001) ("[T]he admission of computer-generated toll and billing records made . . ."); United States v. Cestnik, 36 F.3d 904, 909 (10th Cir. 1994) ("[T]he government introduced computer-generated Western Union money transfer records."); United States v. Glasser, 773 F.2d 1553, 1559 (11th Cir. 1985) ("Computer generated business records are admissible under the following circumstances . . .") (list omitted); United States v. Fusero, 106 F. Supp. 2d 921, 924 (E.D. Mich. 2000) ("As the Court stated during the trial . . . computer-generated records . . . are admissible at trial pursuant to [FRE] 803(6).").

43. *See Cestnik*, 36 F.3d at 909 (holding computer-generated records admissible because they were used to show the amount and origin of fraudulent bank transfers *and* because they satisfied the business records exception); United States v. Linn, 880 F.2d 209, 216 (9th Cir. 1989) ("The record was generated automatically . . . as records of outgoing telephone calls regularly are . . . . In

Applying the hearsay exceptions outlined above to computer records means that business records generated in the regular course of business and governmental agency computer records will almost always be admitted at trial. Records that do not fit neatly into these categories, however, are left in an uncertain void where, depending on a court's view of the matter, they may be admitted or just as easily denied.[44] Fortunately, courts seem to implicitly recognize that many types of computer records should be allowed into evidence, and often find some way to admit such data under another hearsay exception.[45]

A minority of states employ a more nuanced view of computer records and take a vastly different stance on such records' admissibility.[46] Importantly, these states distinguish between computer-stored records and computer-generated records,[47] and maintain that computer-generated records

---

any event, telephone records are business records for the purposes of [FRE] 803(6)."); United States v. Miller, 771 F.2d 1219, 1237 (9th Cir. 1985) (holding that computer-generated records are potential hearsay because they constitute "writings"); United States v. Glasser, 773 F.2d 1553, 1559 (11th Cir. 1985) (setting out the various situations where computer-generated records are admissible, all of which are traditional exceptions to the hearsay rule); *Fusero*, 106 F. Supp. 2d at 924–25 (allowing computer-generated records into the record because they were kept in the ordinary course of business).

44. An example of the danger posed by submitting computer records to a hearsay analysis is found in *United States v. Blackburn*, 992 F.2d 666 (7th Cir. 1993). In that case, computer-generated records denoting the prescription of a pair of glasses left at the scene of a crime were found to not satisfy the business records exception because the records were compiled in preparation for litigation. *Id.* at 670. While the records were eventually admitted under the residual hearsay exception found in FED. R. EVID. 807, the fact that the court had to employ such a strained interpretation of the hearsay rule and its exceptions demonstrates the danger of such a treatment for computer-generated records.

45. *See* Molex, Inc. v. Wyler, No. 04 C 1715, 2005 WL 497812, at *4 (N.D. Ill. Feb. 17, 2005) (allowing email evidence under the state of mind exception to the hearsay rule); *In re* Homestore.com, Inc. Sec. Litig., 347 F. Supp. 2d 769, 781 (C.D. Cal. 2004) (holding that emails written by a party are admissible as party admissions under the hearsay rule); United States v. Boyce, 148 F. Supp. 2d 1069, 1082–83 (S.D. Cal. 2001) (holding computer-generated tax assessment forms created for litigation admissible under the public records exception to the hearsay rule); State v. Love, 576 S.E.2d 709, 711–13 (N.C. Ct. App. 2003) (admitting computer printouts of a witness's statement as recorded recollections).

46. *See* Orin S. Kerr, *Computer Records and the Federal Rules of Evidence*, U.S. ATT'YS' BULL., March 2001, at 25 (outlining the overall countermovement in some states to view computer-generated records as a separate form of evidence). As of this Note's publication, these states are California, *e.g.*, People v. Hawkins, 121 Cal. Rptr. 2d 627 (Ct. App. 2002), Illinois, *e.g.*, People v. Holowko, 486 N.E.2d 877 (Ill. 1985), Kansas, *e.g.*, State v. Schuette, 44 P.3d 459 (Kan. 2002), Louisiana, *e.g.*, State v. Armstead, 432 So. 2d 837 (La. 1983), Mississippi, *e.g.*, State v. Dunn, 7 S.W.3d 427 (Miss. Ct. App. 1999), Ohio, *e.g.*, Gray v. Fairview Gen. Hosp., No. 82318, 2004 WL 527936 (Ohio Ct. App. Mar. 18, 2004), Tennessee, *e.g.*, State v. Meeks, 867 S.W.2d 361 (Tenn. Crim. App. 1993), and Texas, *e.g.*, Ly v. State, 908 S.W.2d 598 (Tex. Ct. App. 1995). The only federal courts that have not followed the majority stance are the Air Force Court of Criminal Appeals, United States v. Rollins, No. ACM34515, 2004 WL 26780 (A.F. Ct. Crim. App. Dec. 24, 2003), and the U. S. Navy-Marine Corps Court of Military Review, United States v. Duncan, 30 M.J. 1284, 1288 (N-M. Ct. Crim. App. 1990).

47. *See Hawkins*, 121 Cal. Rptr. 2d at 642–43 (discussing various states' practices with regard to explicitly delineating between computer-stored and computer-generated records); *Armstead*, 432 So. 2d at 839–40 (setting out the terms "computer-stored" and "computer-generated" records and noting that computer-stored data must satisfy the business records exception, but computer-generated data is not dependent on the observations of humans and, therefore, cannot be hearsay).

cannot be hearsay because they are "not dependent upon the observations and reporting of a human declarant."[48] Computer-*stored* records, on the other hand, are deemed the electronic equivalent of handwritten documents.[49] Since they are created or maintained by a human, they are considered statements and must therefore satisfy a hearsay exception in order to be admitted.[50] Ironically, the non-hearsay stance fits logically into the majority of outcomes because it is the logic behind the hearsay rulings that is wrong, not the usual result. Therefore, instead of overruling prior cases, these courts simply need to recognize the distinction between computer-stored and computer-generated records.

This Note argues that the minority conception is the proper approach to judging computer-generated records' admissibility. The minority approach recognizes the true nature of this type of record and is in accordance with the overall purposes of the Federal Rules of Evidence: accuracy and truth in the fact-finding process.[51] Part I demonstrates that a distinction exists between computer-stored and computer-generated records. A majority of courts largely ignore this distinction despite contravening precedent from several state courts. Part II then explains why computer-generated records—as opposed to computer-stored records—should not be considered hearsay because these records do not fit into the definition of hearsay and they do not present the normal dangers associated with such statements. Part III advocates a test by which judges can distinguish between these two types of records. This Part also suggests ways in which federal and state judiciaries can reform faulty precedent and avoid the likely obstacles that will arise in such an endeavor.

I. The Distinction Between Computer-Stored and Computer-Generated Records and How It Is Ignored in Various Courts

While the split on this issue is quite distinct, it is surprising that more jurisdictions have not recognized or even addressed the possibility of different types of computer records being introduced at trial. This Section argues that there is an important distinction between various types of computer records that must be recognized by courts if they wish to practice consistency in applying the hearsay rule to proffered evidence, and that hearsay jurisdictions consciously ignore the demonstrated workability of the non-hearsay view.

The crucial distinction that courts should not ignore about computer records is that some records are computer-*stored* while others are computer-

48. *Armstead*, 432 So. 2d at 839–40.

49. *Duncan*, 30 M.J. at 1288.

50. *Id.* at 1288–89.

51. *See* Fed. R. Evid. 102 (setting forth accurate factfinding as one of the main purposes of the FRE).

generated.[52] In essence, computer-stored records are human assertions stored in an electronic format.[53] These records constitute "assertions" because they are "the by-product of a machine operation which uses for its input 'statements' entered into the machine by out of court declarants."[54] Examples of this type of record include: word processor files; spreadsheets, such as Microsoft Excel files; charts; graphs; and emails.[55] Accordingly, these records are "statements" and fit easily under the classic definition of hearsay.

Computer-generated records, on the other hand, are records that are "self-generated" by the computer.[56] This is a sometimes deceptively simple definition because human interaction often triggers the computer processes that create the records; however, the crucial factor is whether the record is a mark of computer activity or if it is the electronically-saved statements of a human user. A common example of this type of record is the trace report created by a telephone company computer when it monitors calls made to a specific phone number.[57] When a person dials that number, the computer automatically creates the report—no human must assert that the call was made in order for the record to be generated. Other examples include ATM receipts,[58] computer document "meta-data,"[59] and internet protocol ("IP") logs on computer networks.

The former, if introduced at trial, fall under the classic definition of hearsay while the latter can be likened to original evidence such as fingerprints, sound recordings, and photographs.[60] This distinction affects both how the records should be analyzed for admissibility as well as the methods attorneys must employ when introducing such records in the first place.[61] Therefore, courts must acknowledge the difference between computer-stored and computer-generated records in order to accurately judge a record's admissibility.

---

52. For further discussion on these two terms of art, please see *Armstead*, 432 So. 2d at 839–40.

53. *Id.* at 840.

54. *Id.* at 839.

55. Kerr, *supra* note 46; *Computer-Generated Evidence: The Hearsay Rule and Computerized Evidence*, 2 CRIM. PRAC. GUIDE 1, 1 (March 2001) [hereinafter CRIM. PRAC. GUIDE].

56. 2 MCCORMICK, *supra* note 12, § 294; CRIM. PRAC. GUIDE, *supra* note 55, at 1.

57. 2 MCCORMICK, *supra* note 12, § 294.

58. *See, e.g.*, United States v. Duncan, 30 M.J. 1284, 1289 (N-M. Ct. Crim. App. 1990).

59. *See, e.g.*, United States v. Rollins, No. ACM34515, 2004 WL 26780, at *9–10 (A.F. Ct. Crim. App. Dec. 24, 2003).

60. *Infra* notes 83–85 and accompanying text.

61. If a piece of evidence is not deemed hearsay under FED. R. EVID. 801, then the analyses for admitting it at trial fall on authentication, FED. R. EVID. 901, and the evidence's probative versus prejudicial value, FED. R. EVID. 403. If both of these qualifications are proven satisfactory to the judge, then the proffered evidence should be admitted. Importantly, even admissible hearsay must undergo these two steps. Therefore, the consequence of this distinction is that non-hearsay computer records do not have to undergo an additional step for being admitted at trial.

Almost all federal courts, and most state courts, doggedly ignore this distinction, maintaining a "hearsay conception" of *all* computer-generated records. While this hearsay conception appropriately recognizes that there are situations where computer evidence constitutes out-of-court assertions, opponents believe this view is oversimplified.[62] These same opponents aver that there are several powerful reasons to distinguish between the two types of records, and this is why the hearsay conception cannot be accepted by itself.

II. COMPUTER-GENERATED RECORDS SHOULD NOT BE CONSIDERED HEARSAY

Not only is the distinction between computer-stored and computer-generated records possible, it is supported by the language and purpose of the hearsay rules and vital to promote the policies of the Federal Rules of Evidence. This Section details the reasons for the non-hearsay view and argues that they are more persuasive than their hearsay counterparts.

First, the plain language of the hearsay rule suggests that computer-generated records cannot be considered hearsay because they are not made by a "person"[63] and cannot be "statements"[64] for the purposes of the rule.[65] Most courts have historically excluded from the hearsay rule "statements" made by animals and machines because the nature of their creation does not suggest any unreliability.[66] It is not clear why computer-generated records should be treated any differently.

State v. Armstead,[67] the hallmark case of this non-hearsay view, appropriately recognizes this fact and uses it in making the distinction between

---

62. Orin Kerr, previously of the Department of Justice's Computer Crime and Intellectual Property Section, argues that, as federal courts develop a more "nuanced" view on computer records, they will be able to see distinctions inherent in the evidentiary issues presented by the various types of record. Kerr, *supra* note 46, at 26. This ability to distinguish records, though, is not currently present in the way federal courts analyze computer records on the whole.

63. Federal Rule of Evidence 801(b) states, "A 'declarant' is a *person* who makes a statement." FED. R. EVID. 801(b) (emphasis added). Rule 801(c) then goes on to say, "'Hearsay' is a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted." FED. R. EVID. 801(c). *The Oxford English Dictionary* defines a "person" as "a human being regarded as an individual." CONCISE OXFORD DICTIONARY 1065 (10th ed. 2002). While far from a legal source, this dictionary's definitions are nonetheless taken as persuasive in U.S. courts. *See, e.g.*, Muscarello v. United States, 524 U.S. 125, 128 (1998). Generally, cases in the U.S. that have dealt with the issue of defining the term "person" were brought in order to incorporate either political or corporate bodies into the overarching definition, or were meant to clarify the term for tax purposes. *See, e.g.*, Ngiraingas v. Sanchez, 495 U.S. 182, 190 (1990) (compiling a history of various definitions of the corporate "person").

64. *See* FED. R. EVID. 801(a) (defining the term "statement").

65. *See, e.g.*, United States v. Duncan, 30 M.J. 1284, 1288 (N-M. Ct. Crim. App. 1990).

66. LEMPERT ET AL., *supra* note 12, at 522. Besides the fact that these types of "statement" are not made by a person, the typical reason that courts have excluded animal or machine statements from a hearsay analysis is because they are non-assertive. *See id.* at 517.

67. 432 So. 2d 837 (La. 1983).

computer-stored and computer-generated records.[68] In that case, instead of entertaining the defendant's claims that prosecutors failed to satisfy the business records exception, the court stated that the automatically generated telephone call logs at issue were not human statements of any kind.[69] After noting that computer-*stored* records are rightly treated as hearsay, the majority then pointed out that records that are not generated by human hands cannot be considered a statement within the normal bounds of the hearsay rule.[70] The underlying rationale of the rule, the court maintained, is to bar statements made without an oath that cannot be cross-examined.[71] Since self-generated records are merely a "record of [the computer's] operations," the court reasoned that they could not be statements at all.[72]

Several courts adopted *Armstead*'s interpretation by officially distinguishing between computer-stored and computer-generated records and implementing the appropriate rules for each.[73] The reasoning eventually broadened beyond just telephone records, and many different types of computer-generated output soon found acceptance in state courts.[74] Eventually, in *State v. Carter*, Louisiana went so far as to say that it would "defy logic" to conclude that authenticated computer-generated records could be anything but admissible evidence.[75]

Second, none of the traditional rationales for excluding hearsay[76] apply to computer-generated records. There is no direct testimony with higher probative value. It is impossible to increase the accuracy of computer-generated data by putting the computer under oath, cross-examining it, or observing its demeanor. Since computer-generated records are not statements, any worries about accuracy will be remedied by a simple authentication of the record and its contents. Furthermore, even if portions

---

68. *Id.*

69. *Id.*

70. *Id.* at 839–40.

71. *Id.* at 840.

72. *Id.*

73. *See, e.g.*, United States v. Rollins, No. ACM34515, 2004 WL 26780, *9–10 (A.F. Ct. Crim. App. Dec. 24, 2003); People v. Hawkins, 121 Cal. Rptr. 2d 627, 642–43 (Ct. App. 2002); People v. Holowko, 486 N.E.2d 877, 897 (Ill. 1985) ("[C]omputer-generated data are different .... The printouts ... are merely the tangible result of the computer's internal operations."); State v. Carter, 762 So. 2d 662, 678–80 (La. Ct. App. 2000); State v. Meeks, 867 S.W.2d 361, 375 (Tenn. Crim. App. 1993).

74. *See, e.g.*, *Hawkins*, 121 Cal. Rptr. 2d 627 (Cal. Ct. App. 2002) (admitting computer access logs used to show that the defendant downloaded confidential files at certain times); People v. Caffey, 792 N.E.2d 1163 (Ill. 2002) (permitting caller ID records into the record); Gray v. Fairview Gen. Hosp., No. 82318, 2004 WL 527936 (Ohio Ct. App. Mar. 18, 2004) (allowing into evidence self-generated CAD analyses of the plaintiff's mammogram); Ly v. State, 908 S.W.2d 598 (Tex. Ct. App. 1995) (admitting printouts of a criminal's movement outside of electronically-controlled boundaries).

75. *Carter*, 762 So. 2d at 678.

76. Williamson v. United States, 512 U.S. 594, 598 (1994); *supra* note 6 and accompanying text.

of such records are taken out of context,[77] the responding attorney can put them back in context by introducing the rest of the record. Considering that none of the rationales for the hearsay rule relate to authenticated computer-generated records, traditional justifications for excluding hearsay do not apply.

Third, the non-hearsay view, in line with hundreds of years of Anglo-American evidentiary precedent,[78] advocates distinctions based on the nature, trustworthiness, and probative value of each computer record at issue.[79] This is because lumping wide categories of evidence under the hearsay rule requires that they satisfy an exception to the rule, despite the fact that, as a category of evidence, they may be as reliable as any other non-hearsay items introduced at trial. Such a view is supported by both the hearsay rule's principal justifications and more recent additions to the corpus of evidentiary law.[80] Moreover, these principles accurately judge the probative weight that computer-generated records deserve.

Since the hearsay rule is predicated on the untrustworthiness of out-of-court statements,[81] the main concern is whether computer-generated records are trustworthy if properly authenticated. Several characteristics of these records lead to the conclusion that, indeed, they are trustworthy and undeserving of the hearsay label. Businesses, the government, and the average layperson utilize computer-generated records because they are reliable, and, more importantly, they offer an unbiased, accurate portrayal of certain exchanges that occur between computers and humans. Computer-generated records should thus be considered legally reliable[82] because of the nature in which they were created *and* because this same process eliminates any question of accuracy beyond a preliminary inquiry into the authenticity of the records themselves.

Any inaccuracies found in computer-generated records are not the type the hearsay rule is designed to catch. Whereas a Word document is a

---

77. *Williamson*, 512 U.S. at 598.

78. *See* 2 McCormick, *supra* note 12, § 53 (outlining the history of Anglo-American jurisprudence on judicial admissibility determinations).

79. *Id.*

80. American courts do not admit hearsay statements because they are inherently unreliable. Fenner, *supra* note 3, at 4–5. The hearsay rule "expresses the judicial system's preference for the real witness, rather than a witness who heard it from the real witness." *Id.* at 8 (citation omitted). (As will be discussed in Section III.A, *infra*, this Note's suggested "electronic fingerprints" test demonstrates why computer-generated records are, themselves, the "real witness.") Thus, probative evidence must be adequately authenticated, see People v. Houston, 679 N.E.2d 1244, 1249 (Ill. App. Ct. 1997), accurate, see State v. Farner, 66 S.W.3d 188 (Tenn. 2001), and easily introduced at trial, Fed. R. Evid. 401.

81. Tribe, *supra* note 5, at 958; *cf.* Lee v. Illinois, 476 U.S. 530, 543 (1986) (noting that hearsay statements are "presumptively unreliable").

82. Paul S. Milich, *Hearsay Antinomies: The Case for Abolishing the Rule and Starting Over*, 71 Or. L. Rev. 723, 745 (1992) ("Even before the hearsay rule was fully established, courts began finding specific situations in which hearsay should be admitted."); *see also* Fenner, *supra* note 3, at 135 (stating the traditional view that hearsay exceptions are for those types of hearsay statements that society at large deems unusually reliable).

mechanism for recording assertions made by a person, a computer-generated record, much like a photograph or sound recording, merely captures information about the state of the world at a particular moment.[83] Although these records may be inaccurate or misleading, as noted by Judge Van Graafeiland in *Perma Research*, the inaccuracies are best caught by the authentication process, rather than by cross-examining the computer itself.[84] Since the ultimate concern in admitting these types of evidence is authentication,[85] computer-generated records warrant the same treatment.

Fourth, classifying computer-generated records as hearsay may often frustrate the purpose of promoting accurate fact finding[86] for computer crimes like electronic terrorism, internet stalking, computer trespass, and electronic spoliation because it may prohibit highly relevant and trustworthy evidence regarding the crime.[87] While this is a justification based more on policy considerations than it is based on the hearsay rule or evidentiary rules, it suggests that the hearsay rule's justifications may be outweighed by countervailing interests. Furthermore, this rationale exhibits why it is so important to correctly classify computer-generated and computer-stored records: computers are used more and more in business and at trial;[88] evidentiary rules must keep pace.

Finally, the core of the hearsay position is based on an outdated conception of computers and the nature of the records they create, and the minority position is not. *Perma Research* was decided in 1976, and the majority of

---

83. *See* United States v. Rembert, 863 F.2d 1023, 1026–28 (D.C. Cir. 1988) (admitting photographs as valid reliable "silent witness[es]"); United States v. Slade, 627 F.2d 293, 301 (D.C. Cir. 1980) (holding sound recordings admissible evidence because they were reliable and relevant to the defendant's guilt); United States v. McMillan, 508 F.2d 101 (8th Cir. 1974); People v. Bowley, 31 Cal. Rptr. 471, 476 (Cal. 1963).

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

85. FED. R. EVID. 901(a); CRIM. PRAC. GUIDE, *supra* note 55, at 1; *cf.* United States v. Simpson, 152 F.3d 1241, 1250 (10th Cir. 1998) (holding that authentication of properly admissible computer records depends on the functioning of the program or process in question).

86. *See* Tribe, *supra* note 5, at 958 (noting that the reason hearsay evidence is excluded is because it impedes, rather than helps, factfinding).

87. The elements of each crime cited obviously rely heavily on computer evidence. For example, in a case for computer trespass, 28 U.S.C. § 2701(a) makes it illegal to access stored electronic communications if the user is either (1) unauthorized to do so, or (2) exceeds their authorization to do so. To extend the example, let us assume the victim in this suit is a business. 28 U.S.C. § 2701(a) (2000). If the business is unable to provide the records of the unauthorized access for any reason (such as deletion, corruption, or other destruction of the records), the only recourse may be to utilize records from the accused's computer itself. Since these records are not business records and are unlikely to fall under any other hearsay exceptions such as admissions, FED. R. EVID. 801(d). Similarly, in other cases like computer fraud, 18 U.S.C. § 1030(a)(4) (2000), or extortionate threats, 18 U.S.C. § 1030(a)(7) (2000), private individuals or businesses that do not have the proper records are likely unable to bring an adequate suit minus the ability to introduce the defendant's own computer records.

88. L. Neal Ellis, Jr. et al., *Recent Developments in Trial Techniques*, 35 TORT & INS. L.J. 677, 695 (2000); Paul W. Grimm & Claudia Diamond, *Low-Tech Solutions to High-Tech Wizardry: Computer-Generated Evidence*, 37 MD. B.J. 5, 6 (2004); Gary A. Munneke, *Legal Skills For A Transforming Profession*, 22 PACE L. REV. 105, 128 n.129 (2001).

subsequent foundational decisions were handed down twenty years ago.[89] Hearsay courts have not seen fit to question or reexamine these precedents.[90] This is not to say that these results are wrong. In fact, *Perma Research* and its progeny aptly recognize the danger of believing that all computer records are admissible and free from hearsay. The current hearsay conception, however, is based on a notion of computers that does not account for independent activity and recordkeeping, which are often free from any human interaction.[91] Simply delineating between the two types of records would allow these courts to keep their current precedent, but also include a view of computer records that rightly foregoes a hearsay analysis for trustworthy, reliable pieces of evidence contained in computer-generated records.

By contrast, the hearsay view is implicitly rationalized on the premises that uniformity in treatment of computer records is desirable,[92] the judicial process must be efficient, and computer records are ambiguously indefinable.[93] While these rationales technically provide the basis for a more smoothly-functioning judicial system as a whole, they are overridden in this case by the need for accurate factfinding and a consistent hearsay rule. The hearsay viewpoint's policy justifications simply cannot excuse the incorrect assumption that computer-generated records invariably constitute hearsay, especially when such records are highly probative and useful in ascertaining the truth.

A different source of the steadfast adherence to the business and public records exceptions might be the wording of the Rules of Evidence themselves. Both exceptions incorporate the words "data compilation[s]" into their definitions,[94] and almost all commentators take this to be synonymous with "computer records."[95] The hearsay view, however, seems to ignore that

---

89. *See, e.g.*, United States v. Miller, 771 F.2d 1219 (9th Cir. 1985); United States v. Glasser, 773 F.2d 1553 (11th Cir. 1985).

90. *See, e.g.*, United States v. Hornaday, 392 F.3d 1306, 1317 (11th Cir. 2004) (citing *Glasser*, 773 F.2d at 1557–58); Sea-Land Serv., Inc. v. Lozen Int'l, LLC, 285 F.3d 808, 819 (9th Cir. 2002) (citing *Miller*, 771 F.2d at 1237); United States v. Williams, 264 F.3d 561, 568 (5th Cir. 2001) (citing *Miller*, 771 F.2d at 1228); United States v. Stoudenmire, 74 F.3d 60, 64 (4th Cir. 1996) (citing *Glasser*, 773 F.2d at 1557).

91. See cases cited *supra* note 83 and accompanying text.

92. *See* BENJAMIN CARDOZO, THE NATURE OF THE JUDICIAL PROCESS 149 (1921) (noting that a judicial system can only do society's work if it practices a certain level of stare decisis because to do otherwise is to make law an uncertain and arbitrary practice); Carl Tobias, *A Divisional Arrangement for the Federal Appeals Courts*, 43 ARIZ. L. REV. 633, 656 (2001).

93. *See* Roberts, *supra* note 38, at 279 (discussing the inherent dangerousness computer evidence entails because it can combine hearsay and other inadmissible or erroneous data into an attractive evidentiary "package").

94. FED. R. EVID. 803(6) ("A memorandum, report, record, or data compilation, in any form . . ."); FED. R. EVID. 803(8) ("Records, reports, statements, or data compilations, in any form . . .").

95. *See* CRIM. PRAC. GUIDE, *supra* note 55; *see also* United States v. Briscoe, 896 F.2d 1476, 1494 (7th Cir. 1990) (noting that it is "well established that computer data compilations are admissible as business records under [FRE] 803(6)"); United States v. Hutson, 821 F.2d 1015, 1019 (5th Cir. 1987) ("Computer records are admissible if the requirements of Rule 803(6) have been met.").

this language does not mean computer records can *only* be admitted under these hearsay exceptions. The threshold question for applying FRE 803(6), after all, is whether the evidence in question is even hearsay.[96] It seems that courts get distracted by the fact that computer-generated records are printed on paper and look similar to human-created records,[97] despite the fact that the nature of their creation and content create an inference of trustworthiness strong enough to avoid a hearsay classification.

The only reason computers are viewed so distrustfully is because they *can* contain hearsay statements in "packaging" that otherwise looks like admissible evidence.[98] A means to distinguish between hearsay and non-hearsay computer records would easily resolve this concern.[99] In practice, drawing lines between these two types of record is not overly difficult. All that is needed is an approach that facilitates understanding of this important distinction.

III. A Proposed Method to Distinguish Between Computer-Stored and Computer-Generated Records: The "Electronic Fingerprints" Test

As established above, a gray area exists between computer-stored and computer-generated records, and it often confuses judges and attorneys alike.[100] As with many types of evidence, computer records may be classified differently depending on one's point of view. If the court analyzes each portion of a computer record, some parts may be considered computer-generated and consequently admissible under the various hearsay and evidence rules. For example, if a prosecutor hopes to admit a document found on a defendant's computer, the question becomes, must the file's metadata—

---

96. Fed. R. Evid. 803 ("The following [types of hearsay] are not excluded by the hearsay rule . . .") (list omitted).

97. *See, e.g.*, United States v. Miller, 771 F.2d 1219, 1237 (9th Cir. 1985) (calling computer records "writings" and stating that they will be admitted only if they satisfy the business records exception).

98. *Id.*

99. *See infra*, Part III.

100. Many hearsay jurisdiction cases properly identify records as computer-generated, yet then apply the hearsay rule and undertake a business records analysis. *See* United States v. Cestnik, 36 F.3d 904, 909 (10th Cir. 1994) (holding computer-generated records admissible because they were used to show the amount and origin of fraudulent bank transfers *and* because they satisfied the business records exception); United States v. Linn, 880 F.2d 209, 216 (9th Cir. 1989) ("The record was generated automatically . . . as records of outgoing telephone calls regularly are . . . . In any event, telephone records are business records for the purposes of [FRE] 803(6)."); United States v. Miller, 771 F.2d 1219, 1237 (9th Cir. 1985) (holding that computer-generated records are potential hearsay because they constitute "writings"); United States v. Glasser, 773 F.2d 1553, 1559 (11th Cir. 1985) (setting out the various situations where computer-generated records are admissible, and all of these situations are the traditional exceptions to the hearsay rule); United States v. Fusero, 106 F. Supp. 2d 921, 924–25 (E.D. Mich. 2000) (allowing computer-generated records into the record because they were kept in the ordinary course of business).

computer-generated, invisible "headers" of most computer files[101]—be inadmissible simply because the type of document itself is computer-stored data and, therefore, hearsay? If so, and records are viewed as wholes rather than as their constituent parts, they may be deemed inadmissible as a result.[102]

Under current precedent, jurists are frequently unable to distinguish between the two types of computer records because there is no test on which to base an accurate analysis.[103] A unified method for distinguishing computer-stored from computer-generated records would resolve this controversy. Without such a test, computer records, or parts thereof, that are logically admissible but do not satisfy a hearsay exception will be denied because they are improperly considered out-of-court statements under outdated notions of the nature of computers and hearsay itself.

In order to facilitate the recognition of the distinction between computer-stored and computer-generated records and to aid judges in the admission process of each type of record, this Part argues that courts should adopt a conception of computer records wherein records similar to "fingerprints" are considered admissible as original pieces of evidence. Section III.A outlines this "electronic fingerprints" test and describes how it may be used. Section III.B then notes potential obstacles to implementing the nonhearsay view and electronic fingerprints test, and it offers ways in which the transition can best be accomplished.

A. *The "Electronic Fingerprints" Test*

The "electronic fingerprints" test is premised on the distinction between computer-stored and computer-generated records, and it outlines an approach to help judges understand the *nature* of various computer records, which is especially useful when delineating between records that have elements of both classifications. Computer-generated records are likened to fingerprints in this test because of the way that they record the data in question.[104] This approach finds support in recent case law and academic

---

101. ALAN M. GAHTAN, ELECTRONIC EVIDENCE 7 (1999).

102. *Cf.* United States v. Blackburn, 992 F.2d 666, 670 (7th Cir. 1993) (holding that an otherwise valid computer-generated report was inadmissible because it was prepared for litigation rather than "in the course of regularly conducted business activity"); *see also*, People v. Chandler, No. 178600, 1996 WL 33357832, at *4 (Mich. Ct. App. Sept. 20, 1996) (upholding, as harmless error, the decision to exclude evidence that the accused's computer showed he was logged into his work network at the time of the victim's shooting).

103. See, e.g., United States v. Salgado, 250 F.3d 438 (6th Cir. 2001) (stating that computer records created by a computer itself are business records); Blackburn, 992 F.2d at 670 (finding a computer-generated report inadmissible because it "was not kept in the course of a regularly conducted business activity"); United States v. Glasser, 773 F.2d 1553 (11th Cir. 1985) (holding that computer-generated records created for litigation are inadmissible because they are hearsay and similarly unable to be authenticated).

104. Fingerprints are used as evidence because of their ability to accurately demonstrate a physical record of a human hand. Ed German, *The History of Fingerprints*, *at* http://onin.com/fp/fphistory.html (last updated May 8, 2005). Furthermore, they are often some of the

thought,[105] and it offers a lens through which courts may finally define the true nature of computer-generated output. Most importantly, however, the test presents an effective delineation process for courts, thereby helping them to avoid the illogical underpinnings that so plague current majority precedent on the subject.

The approach proceeds as follows. First, when computer records are introduced, a judge must ask if the *purpose* of the records is to establish the existence of a transaction by a mechanical or digital object, whether a computer, an ATM card, a telephone number, or some other tangible object. This is a threshold question based on judicial economy; it is easy to answer and gives an accurate view of the record's likely admissibility in one broad swath. If, for example, a prosecutor wishes to introduce an IP log in order to demonstrate that the defendant's computer signed on a network at specified times, this is presented in order to identify the computer conducting pertinent activity on an internet network; therefore, the records are relevant based on identification purposes.

Second, the judge must decide whether the piece of computer evidence constitutes an "electronic fingerprint" or, instead, an out-of-court statement. In order to accomplish this goal, the judge must evaluate the nature of the offered record itself. Specifically, the judge must ask if the record is an assertion or the preservation of an electronic transaction.[106] If the record is the result of a computer's sole operation, the purpose must be the presentation of the transaction in question.[107] If there was human interaction, what was

---

most probative evidence offered at trial. *See, e.g.*, K.S. v. State, 814 So. 2d 1190, 1192 (Fla. Dist. Ct. App. 2002) (stating that it is possible for prosecutors to rely solely on fingerprint evidence when establishing a defendant's guilt); Browning v. State, 91 P.3d 39, 42 (Nev. 2004) ("[D]efendant's guilt was overwhelming given that his fingerprints were at the crime scene . . . ."); People v. McKenzie, 768 N.Y.S.2d 816, 817 (N.Y. App. Div. 2003) ("Moreover, the fingerprint evidence, standing alone, established defendant's guilt beyond a reasonable doubt"). Therefore, considerable weight is given to these pieces of evidence. *Id.*

105. This concept of "electronic fingerprints" is not new; indeed, many commentators—both judicial and academic—already use the term to describe the remnants of a computer transaction. *See* Bernstein v. U.S. Dep't of Justice, 176 F.3d 1132, 1146 (9th Cir. 1999) ("Moreover, when we employ electronic methods of communication we often leave electronic 'fingerprints' behind . . . that can be traced back to us."); Richard L. Marcus, *Confronting the Future: Coping With Discovery of Electronic Material*, 64 LAW & CONTEMP. PROBS. 253, 264 (2001) ("As an initial matter, it would seem that these electronic 'fingerprints' should be no more immune to discovery than any other material that might be useful in making accurate determinations."); Robert H. McKirgan & Randy Papetti, *Cheating in the 21st Century*, LITIG., Summer 2001, at 49, 52 ("Unlike paper files, electronic files even when deleted often leave 'electronic fingerprints' that could reveal when the files were deleted.").

106. *See* FED. R. EVID. 801(c); United States v. Breland, 356 F.3d 787, 792 (7th Cir. 2004); McEuin v. Crown Equip. Corp., 328 F.3d 1028, 1038 (9th Cir. 2003); United States v. Sallins, 993 F.2d 344, 346 (3rd Cir. 1993); United States v. Rodriguez-Pando, 841 F.2d 1014, 1020 (10th Cir. 1988).

107. *See* United States v. Rollins, No. ACM34515, 2004 WL 26780, at *9 (A.F. Ct. Crim. App. Dec. 24, 2003) (denying the assertion that computer-generated records are hearsay because they are created independently of any human interaction).

the *assertive quality* of the interaction that created the record?[108] Essentially, this analysis is used to determine whether the record is an assertion or if it is the equivalent to the mark left behind when a person holds a tactile object. A hearsay analysis is only appropriate in the former case.

The cumulative result would be: (1) a threshold, traditionally judicial question, which—if answered "yes"—leads to; (2) a more searching technical question. If the answers tend toward less interaction or assertive intent, then the record should be classified as "computer-generated" and escape the hearsay label. If they tend toward assertive conduct—generally where there is significant human interaction—then they should be deemed "computer-stored" and go through general computer-related hearsay precedent set forward in federal cases. For example, if a prosecutor offers the defendant's online journal wherein the defendant admits that he signed on to a network at specified times, this obviously deals with human assertions, and, as a result, the court should apply a normal hearsay analysis.

Important to the "electronic fingerprints" approach is that judges analyze the specific part of the record being introduced as evidence under the previous two steps. This allows attorneys to break down the record into its constituent parts, which are usually a combination of computer-stored and computer-generated data.[109] For example, most computer-stored records such as Microsoft files and Photoshop images contain metadata,[110] which can be computer-generated. This metadata records a wide variety of data, such as when the file was last opened or modified, the user who accessed the file, the computer used, and any actions taken with respect to the file (such as printing or emailing it to another computer). A similar example is online journals, which contain both types of data combined into one. The site's user-created content may be rightfully excluded while the computer-generated logs of the website itself are admitted into the record. Because of computer evidence's highly unified presentation, judges and lawyers alike

---

108. *See* United States v. Duncan, 30 M.J. 1284, 1288–89 (N-M. Ct. Crim. App. 1990) (finding that records of keystrokes or computer-tracked information are not hearsay because the human interaction required to make such records is at a minimal level and is not assertive).

109. Interestingly enough, metadata has become a problem for some businesses because it often contains sensitive information that can be retrieved by electronic recipients of the file. An especially striking example recently involved England's Prime Minister, Tony Blair who unwittingly turned over Microsoft Word documents that contained sensitive information in their metadata. Richard M. Smith, *Microsoft Word bytes Tony Blair in the butt*, *at* http://www.computerbytesman.com/privacy/blair.htm (June 23, 2003). This data is also very important for normal Internet operation. For a discussion of metadata's purpose and definition with respect to Internet documents, see Warwick Cathro, *Metadata: An Overview* (August 1997), *available at* http://www.nla.gov.au/nla/staffpaper/cathro3.html (last updated Sept. 10, 1997).

110. *See* Staff, *AntiOnline Spotlight: Microsoft Metadata Forensics*, ENTERPRISE IT PLANET, Mar. 11, 2004, *at* http://www.enterpriseitplanet.com/security/features/article.php/3324701 (discussing the functions and prevalence of metadata in Microsoft files); Adobe, *Search results for "metadata,"* *at* http://busca.adobe.com/search?site=AdobeCom&client=AdobeCom&filter=0&output=xml_no_dtd&proxystylesheet=http%3A%2F%2Fwww.adobe.com%2Fspecial%2Fsearch%2Fadobecomsupport.xsl&restrict=Adobe_com_Train&q=metadata&x=0&y=0 (last visited Aug. 11, 2005).

can miss the crucial distinctions that make parts of the evidence admissible and other parts barred under the FRE and various court precedents.[111]

Finally, in the interests of creating as unified an approach as possible, the last step in this proposed approach is to err on the side of caution. If the answers to the questions posited above offer no clear determination of the records' classification, then judges should simply deem the record "computer-stored" and conduct regular hearsay analysis. In this narrow class of cases, courts should rely on the hearsay exceptions.

An example of the test's utility is found when various types of computer records are offered, much like fingerprints, to establish personal identity.[112] Typical examples of this in use are ATM records, phone records, computer metadata, and IP logs.[113] The common characteristic running through all of these instances is that they are used to identify the point of origin for an electronic transaction and do not reflect a human assertion. For example, phone company records demonstrate the incoming and receiving phone numbers of a telephone conversation;[114] IP logs display incoming computer signals and how an internet server organizes the flow of data to those computers;[115] and ATM records set down the ATM card used and the time and place of the transaction. Therefore, just as real fingerprints are the physical record of fingers touching objects, computer-generated records are the electronic record of computers or human users electronically "touching" other computers.[116]

The test thus relies on the premise that content, rather than form, should rule.[117] Furthermore, if an "electronic fingerprints" analysis deems the records to be computer-generated, then the only true question left over is whether they can also be authenticated. If so, and if there are no other valid objections to the evidence, then they should be admissible at trial.

The "electronic fingerprints" approach delineates the often confusing distinction between computer-stored and computer-generated records while still allowing truly ambiguous cases to be analyzed under a customary hearsay approach. Thus, under the test, courts retain their traditional

---

111. *See* FED. R. EVID. 105; Potamkin Cadillac Corp. v. B.R.I. Coverage Corp., 38 F.3d 627, 632 (2d Cir. 1994) ("A business record may include data stored electronically on computers and later printed out for presentation in court, so long as the 'original computer data compilation was prepared pursuant to a business duty in accordance with regular business practice.'") (quoting United States v. Hernandez, 913 F.2d 1506, 1512 (10th Cir. 1990)).

112. Stevenson v. United States 380 F.2d 590 (D.C. Cir. 1967); *cf.* State v. Dunn, 7 S.W.3d 427 (Mo. Ct. App. 1999) (wherein computer-generated telephone records were used to identify the house of origin for certain phone calls).

113. Kerr, *supra* note 46, at 26.

114. *See, e.g.*, *Dunn*, 7 S.W.3d at 432.

115. *See, e.g.*, United States v. Wagers, 339 F. Supp. 2d 934, 938 (E.D. Ky. 2004).

116. Roberts, *supra* note 38.

117. *See supra* notes 83–85 and accompanying text.

discretionary power with respect to questions of admissibility,[118] but also have an appropriate standard for determining admissibility at trial and judging plain error or erroneous rulings on computer evidence during appellate review. This standard will also provide guidance in an area which desperately needs cohesive thinking.

B. *Addressing Potential Problems with Reforming Current Majority Precedent—Adjusting to the Electronic Fingerprints Test*

Practically speaking, the question remains whether majority courts are willing to adapt to the non-hearsay view. While there are obstacles to this transition, none present such a barrier as to wholly prevent hearsay courts from changing their precedent. Any transition will necessarily be piecemeal, but this is certainly attainable despite any problems presented by current precedent and practice.

One major obstacle to reforming the hearsay position is that, even if judges are convinced to switch to the non-hearsay view, they may be leery of tampering with current precedent because they are unable to tell the difference between hearsay and non-hearsay computer records. This is not an overly distressing problem. Most notably, this is because it is a judge's job to make fine distinctions on evidence's admissibility.[119] The way to do this job and avoid the understandable fear stated above is to educate oneself on the nature of the evidence being introduced. To facilitate this process, trial judges should adopt the electronic fingerprints approach when analyzing computer records.

The second obstacle to reforming the hearsay position is the view that says, "If it ain't broke, don't fix it." It is true that, with valid authentication, most business records and public records will be admitted at trial.[120] Moreover, there are several other ways for most pieces of computer evidence to be admitted into evidence even if they are theoretically hearsay.[121] Regardless, computer-generated records should *still* be analyzed as non-hearsay evidence.

---

118. *See* FED. R. EVID. 104(a) (detailing trial courts' extremely broad discretion to determine evidence's admissibility).

119. *See* FED. R. EVID. 104(a) (giving broad powers to judges when determining evidence's admissibility).

120. *See* FED. R. EVID. 803(6), 803(8).

121. *See* Westfed Holdings, Inc. v. United States, 55 Fed. Cl. 544, 566 (Fed. Cl. 2003) (admitting the possibility that emails may be admissible as present-sense impressions if they are shown to be authentic and contemporaneous); Vermont Elec. Power Co. v. Hartford Steam Boiler Inspection & Ins. Co., 72 F. Supp. 2d 441, 449 (D. Vt. 1999) (holding that a party's emails are admissions for the purposes of the hearsay rule); People v. Bynum, 629 N.E.2d 724, 731–32 (Ill. App. Ct. 1994) (stating that computer graphs printed for trial by an expert witness were admissible as materials normally used by experts despite their status as hearsay); Kitterman v. Mich. Educ. Employees Mut. Ins. Co., No. 247428, 2004 WL 1459523, at *4 (Mich. Ct. App. June 29, 2004) (assuming that email correspondences of the defendant were admissible as recorded collections).

First, the current rule may mask the amount of computer evidence actually excluded. As some commentators point out, many pieces of potential hearsay evidence are not even introduced at trial because the proponent parties suspect they will be denied.[122] Thus, while most computer records are admitted at trial, this is likely a case of correlation, not causation. Put differently, attorneys are likely to only introduce computer records that they know will be admissible; to do otherwise would be to risk their credibility in front of the judge and jury and, consequently, potentially jeopardize their client's case. The status quo is therefore less convincing if argued solely on the approach's seeming functionality.

Second, the system is, in fact, broken. Computer-generated records simply cannot be hearsay, and the antiquated, *stare decisis*-fueled hearsay viewpoint refuses to recognize this fact. Courts regularly make fine distinctions on what is hearsay and what is not.[123] In order to continue this tradition, hearsay courts must make the effort to move beyond an imperfect logical basis for their evidentiary decisions.

These arguments demonstrate why it is baffling that hearsay courts have maintained the hearsay position for so long. Besides being internally inconsistent with several other important hearsay decisions,[124] the hearsay stance discredits the validity of evidence that is extremely probative, nonprejudicial, and reliable. The challenge that faces these courts is how to overcome inertia and arrive at a more coherent and logical position with respect to computer-generated records.

CONCLUSION

Reformation of the hearsay view will most likely be accomplished through small steps, the first of which is to simply establish a compelling reason for altering current practice. As this Note demonstrates, there are ample bases and reasons for federal—and similarly-aligned state—courts to correct decades of erroneous legal precedent.

Legal precedent must keep pace with technology. Computers play an increasingly large part at trial with each passing year.[125] This is so especially because computer-generated evidence is employed in a myriad of situations

---

122. *See, e.g.*, LEMPERT ET AL., *supra* note 12, at 534 n.41.

123. United States v. Ventresca, 380 U.S. 102, 118–20 (1965) (discussing whether a piece of evidence at trial was a personal observation, hearsay, or "hearsay on hearsay"); Adkins v. Brett, 193 P. 251, 252–53 (Cal. 1920) (recognizing that admissible declarations of mental state may nonetheless contain inadmissible hearsay recitals of fact); Breedlove v. State, 413 So. 2d 1, 6 (Fla. 1982) ("Merely because a statement is not admissible for one purpose does not mean it is inadmissible for another purpose.").

124. *See, e.g.*, Lilly v. Virginia, 527 U.S. 116 (1999); Shepard v. United States, 290 U.S. 96 (1933).

125. *See* Frank Tuerkheimer, *The* Daubert *Case and Its Aftermath: A Shot-Gun Wedding of Technology and Law in the Supreme Court*, 51 SYRACUSE L. REV. 803, 804–05 (2001).

that go well beyond simple business disputes.[126] Judges must therefore deal with the introduction of computer-stored and computer-generated evidence with ever-increasing frequency.

As society relies more and more on computers, it necessarily becomes more tech-savvy.[127] Similarly, so do its judges.[128] With approaches such as the electronic fingerprints test as well as judges' own experiences in a computer-filled society, understanding of what various pieces of computer evidence represent will flourish and lead to a more nuanced and ultimately correct process for admitting computer evidence at trial.

For the reasons discussed above, courts cannot go on simply assuming that all computer records are hearsay. Computer-generated records' methods of creation, purposes, and uses at trial all point to the conclusion that they simply are not human statements of any kind. In light of this fact, the question becomes where courts should go from here. An immediate transition to the non-hearsay viewpoint, facilitated by the electronic fingerprints test, is suggested. Barring this miraculous change in position, however, as previously stated, the least courts should do is reexamine the basis for their conclusions and move beyond the outdated *Perma Research* decision.

It may well be that courts differ on which computer-generated records are not hearsay and which constitute a human statement of one form or another. Such is a legal fact of life. However, if the hearsay versus non-hearsay analysis is present, then these courts will have made a step in the right direc-

---

126. GAHTAN, *supra* note 101, at 2. For example, computer evidence has been used, among other reasons, to substantiate allegations of sexual harassment, Knox v. Indiana, 93 F.3d 1327 (7th Cir. 1996), prove theft of trade secrets, First Tech. Safety Sys., Inc. v. Depinet, 11 F.3d 641 (6th Cir. 1993), verify the improper use of licensed software, Lauren Corp. v. Century Geophysical Corp., 953 P.2d 200 (Colo. Ct. App. 1998), and substantiate a wrongful termination of employment, Kelley v. Airborne Freight Corp., 140 F.3d 335 (1st Cir. 1998).

127. COMPUTER LAW 1–2 (Chris Reed & John Angel eds., 4th ed. 2000); Marc D. Goodman, *Why the Police Don't Care About Computer Crime*, 10 HARV. J.L. & TECH. 465, 467–72 (1997) (noting the need for tech-savvy police to respond to the increased numbers of children—and criminals—who are growing up surrounded by computers); John Grady & Jane Boyd Ohlin, *The Application of Title III of the ADA to Sport Web Sites*, 14 J. LEGAL ASPECTS SPORT 145, 147–48 (2004) (recognizing the trend for sports businesses to have cutting edge web sites because more and more sports consumers are highly cognizant of the technological realm); Dennis Kennedy, *Technology Trends: Do We Stand on the Threshold of the Next Legal Killer App?*, LAW PRAC. TODAY, Apr. 2004, at 5, *at* http://www.abanet.org/lpm/lpt/articles/tch04041.html (discussing litigation technology and modern attorneys' need to utilize and understand it).

128. Several judges have already taken the step of becoming more computer-savvy. Judge Richard Posner of the Seventh Circuit Court of Appeals, for example, started a "weblog" in 2004 with economist Gary Becker. *The Becker-Posner Blog*, *at* http://www.becker-posner-blog.com/ (last visited Aug. 11, 2005). This familiarity with computers has also become evident in written opinions. For example, in *United States v. Hill*, Judge Alex Kozinski stated, "As everyone who has accidentally erased a computer file knows, it is fairly easy to make mistakes when operating computer equipment." 322 F. Supp. 2d 1081, 1089 (C.D. Cal. 2004) (sitting by designation pursuant to 28 U.S.C. § 291(b)). Another such example is found in *In re Search of 3817 W. West End, First Floor Chicago, Illinois 60621*, in which the federal district court, of its own volition, suggested that a technical expert search computer files' "metadata" for pertinent information to the case. 321 F. Supp. 2d 953, 956 (N.D. Ill. 2004). As these cases (and Judge Posner's weblog) suggest, judges are gaining a more than passing knowledge of computers and their inner workings with each passing year.

tion. Computer records are not a class of evidence with a uniform face. If a court is able to make the logical step and recognize that various records differ in nature based on their characteristics, then the purpose of both the hearsay and the Federal Rules of Evidence will finally be realized, at least with respect to computer records.