# ELECTRONIC DISCOVERY AND DIGITAL EVIDENCE: ARTICLE: TESTABLE RELIABILITY: A MODERNIZED APPROACH TO ESI ADMISSIBILITY

Summer, 2014

**Reporter**
12 Ave Maria L. Rev. 213 *

**Length:** 43815 words

**Author:** Steven W. Teppler+

+ Steven W. Teppler leads the Abbott Law Group's information governance and electronic discovery practice. Steven's litigation practice focuses on electronic discovery, including production, preservation, and spoliation issues. His experience includes federal and state court litigation matters both against, and on behalf of, Fortune 500 companies, as well as probate and family law disputes where electronic discovery is critically implicated. He has practiced law since 1981, is admitted to the bars of New York, the District of Columbia, Florida, and Illinois and advises private and public sector clients about risk, liability, and compliance issues unique to information governance (i.e., from instantiation through management, preservation, and disposition). Steven is an adjunct professor at Ave Maria Law School, teaching electronic discovery, and also lectures nationwide on evolving theories of information governance and electronic discovery. Mr. Teppler is also a founding co-chair of the Florida Bar's Business Law Section eDiscovery Committee, and is a co-drafter of the 2012 electronic discovery amendments to the Florida Rules of Civil Procedure.

## Text

**[*213]**

This Article examines the proposition that all digital data sought to be introduced and admitted as evidence should be subject to a heightened showing of reliability and testability. This objective could be reached by either: (1) considering all digital data as hearsay pursuant to *Federal Rule of Evidence (FRE) 807*; (2) creating a new evidence rule requiring such a showing as a predicate to admissibility; or (3) the emergence of express decisional authority. This Article also analyzes the inadequacy of the current approaches to dealing with the hearsay exception used to offer computer-generated information into evidence. The author proposes that until the FRE are revised to reflect the highly mutable and untestable nature of digital evidence, such evidence should be treated as hearsay and subject to application of Rule 807, and in accordance with Rule 807, deemed inadmissible unless an affirmative showing of reliability and testability is successfully asserted.

Summary

Subject to certain exceptions not pertinent to this discussion (unfair prejudice, confusion of the issues and the like), all relevant evidence is generally considered admissible once a proper foundation has been laid pursuant to Rule 901.

**[*214]** Once authenticated, the FRE provide for the exclusion of hearsay evidence. [1] Hearsay evidence is defined as "a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to

---

[1] *Fed. R. Evid. 802*.

prove the truth of the matter asserted," [2] and is generally inadmissible unless it falls either under an enumerated exception or is considered "residual." [3] The business records exception and the "residual" hearsay rule are generally applicable to digital data but adopt differing approaches to trustworthiness or reliability. [4] Rule 803(6)'s "Records of Regularly Conducted Activity" exception (more commonly referred to as the "business records" exception) provides for exception status subject to a rebuttable near-presumption, while the residual hearsay exception set forth in Rule 807 appears to require an affirmative showing of reliability or trustworthiness. [5] These exceptions [6] to the hearsay rule provide for widely disparate assessments of trustworthiness.

Since digital data is inherently mutable and not testable by inspection, it is generally not demonstrably trustworthy (e.g., reliable) under most data generating regimes. [7] The Rules sidestep the digital data's inherent unreliability by providing only a low bar to attaining admissibility by operation of the business records exception, that is, by a literal adherence to current requirements, and which tends to reflect an assessment that is proffered but not performed. [8] Accordingly, this approach pays homage to, **[*215]** but falls short of its intended objective of reliability because the Rules (and most judicial authority) do not properly address reliability issues arising from the inherently mutable nature and concomitant untestability of native digital data. [9] Although this shortcoming has been documented since at least as early as the 1970's, the FRE have not been amended to demand of a party seeking to admit digital data that degree of reliability properly reflective of the frailty of digital evidence, except for the December 2011 amendment expressly incorporating the term "electronically stored information" into Rule 101(b). [10]

---

[2] Id. 801(c) (restyled Dec. 1, 2011).

[3] See id 803 (exceptions regardless of declarant's availability); id. 804 (exceptions when declarant is unavailable); id. 807 (residual hearsay).

[4] Compare Rule 803(6) (business records exception), with Rule 807 (residual hearsay).

[5] See Cross v. Amtec Med., Inc., No. 3:09-CV-00168-*HTW-LRA, 2012 WL 4603396, at 7 n.2 (S.D. Miss. Sept. 20, 2012)* (referring to Rule 803(6) as the "Business Record's Exception to the Hearsay Rule"). In order to admit evidence under the Rule 807 residual hearsay exception, a court must find that the evidence satisfies the prerequisites of trustworthiness, notice, necessity, and materiality, and must also determine that the purposes of the rules and justice will be served by admission of the evidence. See *United States v. Phillips, 219 F.3d 404, 419 n.23 (5th Cir. 2000)* (The residual hearsay exception is to be "used only rarely, in truly exceptional cases." (citation omitted)); *Herdman v. Smith, 707 F.2d 839, 841-42 (5th Cir. 1983)*; John W. Strong et al., McCormick on Evidence § 324 (5th ed. 1999).

[6] For purposes of this article, Rule 807 will be discussed as another hearsay exception. Unlike the Business Records Exception, Rule 807 includes an additional procedural requirement imposed on the offering party (notice and opportunity to be heard by opponent) together with a showing by the offering party that such evidence is "more probative on the point for which it is offered" than other evidence reasonably procurable by the proponent. Compare Rule 807, with Rule 803(6).

[7] See George Paul, Foundations of Digital Evidence 21 (2008); see also PixArt Imaging, Inc. v. Avago Tech. Gen. IP (Singapore) Pte. Ltd., No. C 10-*00544 JW, 2011 WL 5417090, at 10 (N.D. Cal. Oct. 27, 2011)* ("The residual hearsay exception is not to be used as a "broad hearsay exception, but rather is to be used rarely and in exceptional circumstances.'" (quoting *Fong v. Am. Airlines, Inc., 626 F.2d 759, 763 (9th Cir. 1980))*.

[8] See Paul, supra note 7, at 131-49; see also Stephen Mason, Electronic Evidence: Disclosure, Discovery & Admissibility, ch. 4 (2007).

[9] At least one recent opinion addressing hearsay has indicated that reliability is the hallmark for admissibility of evidence: "The rules of evidence, not the Confrontation Clause, are designed primarily to police reliability." *Bullcoming v. New Mexico, 131 S. Ct. 2705, 2720 n.1 (2011)* (Sotomayor, J., concurring).

[10] *Fed. R. Evid. 101(b)(6)* ("[A] reference to any kind of written material or any other medium includes electronically stored information."). It should be noted that, as in the Federal Rules of Civil Procedure, the Federal Rules of Evidence do not provide a definition for the term "electronically stored information." See also id. 1001(d) (providing, in pertinent part, that "for Electronically Stored Information, "original' means any printout - or other output readable by sight - if it accurately reflects [that] information," but neither defining electronically stored information, nor addressing the inherent mutability of computer generated information).

Until the FRE are revised to directly address the mutable nature of this new species of evidence, an interim solution may be made by considering all digital data to be hearsay, and that an affirmative showing of reliability pursuant to Rule 807 must be demonstrated if admissibility is to be sought.

Although three United States Circuit Courts of Appeals have rejected the comprehensive application of the hearsay rule to all digital data, [11] it is contended that well-established authority from the Second Circuit provides the constitutional basis for deeming all digital data as hearsay. Moreover, and despite the mostly orthogonal arguments made in opposition, the undisputedly mutable and untestable nature of digital data itself compels the conclusion that all digital data is hearsay. Finally, this article examines the potential implications of the application of the hearsay exclusionary rule to digital evidence used in both the criminal and civil context.

Until the FRE are revised to address information in digital format, the prevailing trustworthiness-by-presumption standard set forth in Rule 803(6), together with recent judicial authority, will continue to provide the proper **[*216]** standards for determination of authentication. This Article argues that the admissibility of digital data should be pre-conditioned on some affirmative showing of reliability required by the residual hearsay rule. [12]

## I. Background

Digital data, or computer-generated information, is known by many names; one such name, "Electronically Stored Information" (ESI), is the term adopted in the 2006 amendments to the Federal Rules of Civil Procedure (FRCP). [13] Interestingly, the legal community has not come to any agreement (or even a proposal) that defines ESI in non-tautological terms; however, an international standard promulgated by the International Standards Organization (ISO) has offered a non-tautological definition of electronically stored information. [14] Accordingly, for purposes of uniformity and irrespective of instantiation format or however stored, the terms "computer generated information," "ESI," "digital information" and "digital data" are used interchangeably in this article.

---

[11] See, e.g., *United States v. Lamons, 532 F.3d 1251, 1263-64 (11th Cir. 2008)* (machine generated raw data not "statements" and not testimonial hearsay); *United States v. Moon, 512 F.3d 359, 362 (7th Cir. 2008)* (raw data generated by lab machines not out-of-court statements subject to confrontation clause); *United States v. Hamilton, 413 F.3d 1138, 1142 (10th Cir. 2005)* (computer generated "header information" not hearsay); *United States v. Khorozian, 333 F.3d 498, 506 (3d Cir. 2003)* (header information generated by a fax machine not hearsay); *United States v. Blazier, 69 M.J. 218, 224 (C.A.A.F. 2010)* ("It is well-settled that under both the Confrontation Clause and the rules of evidence, machine-generated data and printouts are not statements and thus not hearsay - machines are not declarants - and such data is therefore not "testimonial.'").

[12] Standing in contrast to Rule 803(6) is the "Residual Exception" to the hearsay rule articulated in Rule 807, which requires a showing of "equivalent circumstantial guarantees of trustworthiness." ***Fed. R. Evid. 807***. The application of Rule 807 is not the norm, as the intent of Congress in enacting Rule 803(24) (predecessor to Rule 807) was to account for unforeseen evidentiary scenarios, and generally to be used "rarely, and only in exceptional circumstances." *United States v. Peneaux, 432 F.3d 882, 893 (8th Cir. 2005)*.

[13] See Summary of the Report of the Judicial Conference Committee on Rules of Practice and Procedure (2005), available at *http://www.uscourts.gov/uscourts/RulesAndPolicies/* rules/Reports/ST09-2005.pdf. The Supreme Court transmitted the proposed rules to Congress in April 2006. Congress did not enact legislation to reject, modify, or defer the pending rules within the time prescribed by28 U.S.C. § 2074, and the new rules became effective December 1, 2006. Carl Roberts, The 2006 Discovery Amendments to the Federal Rules of Civil Procedure, Law Practice Today (Aug. 2006), *http://apps.americanbar.org/lpm/lpt/articles/tch08061.shtml*.

[14] Electronically Stored Information, or ESI, is defined as "data or information of any kind and from any source, whose temporal existence is evidenced by being stored in or on any electronic medium." Int'l Org. for Standardization, ISO/IEC FCD 27040: Information Technology - Security Techniques - Storage Security 3.16 (proposed ISO standard) (Oct. 31, 2013) (on file with author) (internal citation and emphasis omitted). This includes, without limitation, "traditional e-mail, memos, letters, spreadsheets, databases, office documents, presentations and other electronic formats commonly found on a computer. ESI also includes system, application and file associated metadata such as timestamps, revision history, file type, etc… . Electronic medium can take the form of, but is not limited to, storage devices and storage elements." Id. (internal citations and emphasis omitted).

The vast majority of information currently generated is digital in nature. [15] It therefore follows that the vast majority of information sought to be introduced as evidence will also be digital in nature, and this trend is reflected both in the December 2006 amendments to the FRCP as well as the **[*217]** hundreds of interpretive decisions that have issued almost unabated since that time.

Digital data is inherently malleable or mutable. [16] The inherently mutable nature of computer-generated data creates new issues that have a significant and detrimental effect on reliability, authentication, and ultimately on the issue of admissibility. This mutability, in turn, exposes the inherent frailty of digital data sought to be introduced as evidence. [17]

With few exceptions to date, these issues remain largely ignored by both the bench and the bar, and are directed into unsuitable definitions or relegated to obsolescent analyses. The reason for this ignorance or misapprehension is likely the result of a basic misunderstanding of the nature of both computer-generated information and the variable nature of the computing environment by which such information is generated. The result of this general misunderstanding can be seen in the current mixture of judicial approaches to the admissibility of digital evidence. [18]

**[*218]** The FRE use the term "data compilation," but never refer to or directly address ESI, or digital data, as evidence. The evidence rules predate by decades the 2006 electronic discovery amendments to the FRCP, and so it is not surprising that the FRE make no mention of ESI. [19] Despite the approach of the fortieth anniversary of near

---

[15] See Peter Lyman & Hal R. Varian, How Much Information?, tbl. 1.2, http://www2.sims. berkeley.edu/research/projects/how-much-info-2003/.

[16] Bruce H. Nearon, Jon Stanley, Steven W. Teppler, & Joseph Burton, Life After Sarbanes-Oxley: The Merger of Information Security and Accountability, *45 Jurimetrics J. 379, 387 (2005)*.

[17] It has also long been accepted that computer output is not infallibly reliable. Noting that computers are more than merely "calculators … with a giant "memory,"' a 1976 dissenting opinion stated: "As courts are driven willy-nilly into the magic world of computerization, it is of utmost importance that appropriate standards be set for the introduction of computerized evidence." *Perma Research & Dev. v. Singer Co., 542 F.2d 111, 124 (2d Cir. 1976)* (Van Graafeiland, J., dissenting). Judge Van Graafeiland went on to quote a contemporaneous law review article:

Although the computer has tremendous potential for improving our system of justice by generating more meaningful evidence than was previously available, it presents a real danger of being the vehicle of introducing erroneous, misleading, or unreliable evidence. The possibility of an undetected error in computer-generated evidence is a function of many factors: the underlying data may be hearsay; errors may be introduced in any one of several stages of processing; the computer might be erroneously programmed, programmed to permit an error to go undetected, or programmed to introduce error into the data; and the computer may inaccurately display the data or display it in a biased manner. Because of the complexities of examining the creation of computer-generated evidence and the deceptively neat package in which the computer can display its work product, courts and practitioners must exercise more care with computer-generated evidence than with evidence generated by more traditional means.

*Id. at 125* (quoting Jerome J. Roberts, A Practitioner's Primer on Computer-Generated Evidence, 41 U. Chi. L. Rev. 254, 255-56 (1974)). Further, the judge pointed out that, "There are those knowledgeable in the field of computerization who believe that new evidentiary rules will be required to channel and control the use of this new medium." Id. The prescience of Judge Van Graafeiland's dissenting comments in Perma Research has been borne out by the ensuing decades of ill-informed and often contradictory judicial authority, and is so timely that this dissent might have been issued yesterday.

[18] Compare ***St. Clair v. Johnny's Oyster & Shrimp, Inc., 76 F. Supp. 2d 773, 775 (S.D. Tex, 1999)*** (digital data taken from the internet described as "voodoo information"), with *D & H Auto Parts, Inc. v. Ford Marketing Corp., 57 F.R.D. 548, 552 (E.D.N.Y. 1973)* ("In relying upon data processing by a machine, there should be no more necessity for oral testimony concerning the reliability of the machine operations than that of the manual procedure supplanted, whether it be bookkeeping, order preparation, or mathematical computation."). See Steven W. Teppler, Digital Evidence as Hearsay (Part 1), EDDE J., Summer 2010, at 18, 19 n.6.

ubiquity, however, the term "computer" remains notably missing from the FRE. Moreover, even the authentication provisions of Rule 901 refer generally to the accuracy of a "process or system" in producing an "accurate result" [20] without indicating whether the process or system is a computer, or whether the result is computer-generated information.

The term "data compilation" makes one of its rare appearances in Article VIII of the FRE, and is expressly included as a record of a regularly conducted activity under the business records exception to the hearsay rule. [21] Judicial authority generally supports the proposition that computer-generated information is a subset of the umbrella term "data compilation" for purposes of analysis under the business records exception. [22]

A second appearance of the term "data compilation" appears in Rule 901(b), but curiously, only from within the context of authenticating "Ancient Documents." [23] A final reference to "data compilation" is found in **[*219]** Rule 1001, which generally requires that an original is required to prove the content of a writing, recording, or photograph. [24] "Writing and recordings" are defined, in pertinent part, to include "letters, words or numbers, or their equivalent, set down by handwriting, typewriting, printing, photostating, photographing, magnetic impulse, mechanical or electronic recording, or other forms of data compilation." [25]

Digital Data as "Source" Data

The vast majority of information generated today is originated as electronic or computer-generated data. [26] It therefore follows that that digital data will become the main source of evidence used in modern litigation. Despite

---

[19] Other jurisdictions are beginning to recognize the need for updating their evidence laws to require more robust authentication for computer-generated information. See South Australian Law Reform Institute, Computer Says No: Modernisation of South Australian Evidence Law to Deal with New Technologies (2012), available at http://www.law.adelaide.edu.au/reform/publications/reports/.

[20] Fed. R. Evid. 901(b)(9).

[21] ***Id. 803***(6). Curiously, the "Residual Hearsay" rule makes no mention of data compilations. See ***id. 807***.

[22] See United States v. Croft, 750 F.2d 1354, 1364 (7th Cir. 1984) ("It is well-settled that computer data compilations may constitute business records for purposes of Fed. R. Evid. 803(6) and may be admitted at trial if a proper foundation is established." (citation omitted)); United States v. Hayes, 861 F.2d 1225, 1228 (10th Cir. 1988); 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.'"); Health Alliance Network, Inc. v. Cont'l Cas. Co., 245 F.R.D. 121, 129 (S.D.N.Y. 2007).

[23] Fed. R. Evid. 901(b)(8). Digital data clearly falls within the ambit of Rule 901(b)(8). Charles Alan Wright & Victor Vincent Gold, Federal Practice and Procedure § 7113(b)(8) (2000) ("The scope of Rule 901(b)(8) extends to "a document or data compilation in any form.' The Advisory Committee's Note suggests that "data compilations' includes "data stored electronically or by other similar means.'"). An ever-increasing volume of digital data is now, or will soon become, greater than 20 years old. Assertions of "ancient document" status intended to fast-track authentication pursuant to Rule 901(8), when coupled with parallel assertions of invoking the ancient documents exception to the hearsay rule pursuant to Rule 803(16), will tend to increase the likelihood of unreliable and untrustworthy digital data admitted into the evidence ecosystem.

[24] Fed. R. Evid. 1001.

[25] Id.

[26] See James E. Short et al., How Much Information? 2010 Report on Enterprise Server Information 7 (2011), available at http://hmi.ucsd.edu/pdf/HMI_2010_EnterpriseReport _Jan_2011.pdf ("In 2008, the world's servers processed 9.57 zettabytes of information, almost 10 to the 22nd power, or ten million million gigabytes. This was 12 gigabytes of information daily for the average worker, or about 3 terabytes of information per worker per year. The world's companies on average processed 63 terabytes of information annually.").

this massive shift in species of evidence from physical (paper and ink) to digital, there has been a relative paucity of judicial authority, and certainly no emergent majority view, dealing with the vagaries inherent to computer-generated information and the directions for its admissibility into evidence.

As early as the late 1970's, courts have written about the need to amend the FRE to address the unique evidentiary issues presented by the inherently mutable nature of computer-generated data. [27] Unfortunately, the Rules do not directly address the unique authentication or admissibility issues arising from this massive shift from evidence in physical format to evidence in digital format. [28] It might have been hoped that the 2006 amendments to the FRCP would accelerate corresponding amendments to the FRE. [29] To date, **[*220]** however, this hope remains unfulfilled. Until such time, as it is, attorneys and judges will continue to deal with inconsistent and, at times, contradictory evaluative admissibility frameworks for digital evidence.

Adding to this unwieldy and inconsistent framework is a general lack of understanding of what constitutes computer-generated information, and what constitutes "source information." Source data of all computer-generated information is binary in nature, and the data processed, viewed, printed out, or stored is composed of ordered sets of zeroes and ones. [30] These binary data are acted upon (processed) by other ordered sets of binary data comprising the operating system and other data processing software applications to produce what are commonly referred to as a data files. [31] "Source" data is, therefore, always comprised of zeroes and ones that are then processed, or rendered, by the operating system and various applications to produce files.

These files are generally further processed by other applications to produce images that can be viewed on a screen, or can be viewed by printing the data to paper. [32] Nevertheless, the source data for either an image viewed on a screen or a computer-generated paper printout are the binaries, or the ordered sets of zeroes and ones, that comprise the true, or source, data used to produce the screen image or paper printout. [33] The data (or information) actually read or perceived by a human reader (or members of a jury) should therefore be considered the last "view" in a set of "views of views" and not the "source" or origination data. [34] In other words, while a person might read,

---

[27] See 2 McCormick on Evidence § 294 (6th edition, 2006); *Commonwealth v. Klinghoffer, 564 A.2d 1240, 1243-44 (Pa. 1989)* (Larsen, J., dissenting). As stated earlier, in a noted 1976 dissent, Justice Van Graafeiland presciently pointed to the need to amend the rules of evidence to address the admissibility issues presented by computer-generated information. *Perma Research & Dev. v. Singer Co., 542 F.2d 111, 124-26 (2d Cir. 1976)* (Van Graafeiland, J., dissenting). It is unfortunate that more than three decades later, no such amendments have been adopted, and the current inconsistent approach to authentication and admissibility is the direct result of that failure to amend.

[28] See 2 McCormick on Evidence, supra note 27, at § 294.

[29] These amendments included changes to *Fed. R. Civ. P. 16(b)(5)*, 26(a)(1)(B), 34(a), 34(b), 37 and 45(a)(1)(C). Roberts, supra note 13.

[30] *Bruce H. Nearon et al., supra note 16*.

[31] Id. at 388.

[32] Id.

[33] Paul, supra note 7, at 21.

[34] Teppler, supra note 18, at 22 n.18:

There is much confusion as to the term "original' as it applies to computer-generated data. The phrase "first instantiation' (which implies "origin') rather than "original' is used with good reason, and exemplifies one of the challenges in adapting the application of the F.R.E. to computer-generated information. The commonly used definition for original is incompatible with the concept of "initial' "first' or "earliest' with "only.' This definition has no inherent value [from within a digital evidence context]. "Original' digital data files can be reproduced in exact bit for bit copies. Unlike paper "originals' there may never be "only one' original. Data files may in fact, be "duplicate originals' created at different times. First instantiation, or origin, however, refers to the characteristics of the source of the data, the environment (including controls) and provenance of the initial creation of digital data. Thus, the adoption and substitution of the term, "first instantiation' for "original' is suggested as more appropriate [because it most

**[*221]** hear, or see computer-generated data, it is impossible to read, hear, or see source computer-generated or origination data. [35] In order to perceive source computer data as native data, it is necessary to read and interpret the language (e.g., "C," "C++," "Python," "Objective-C," or "Visual Basic") in which that data is written. In order to interpret the language in which data is written, it is necessary in turn to understand the language in which it is written. The ultimate aim in understanding or examining computer-generated information is to understand the assertions, or speech, of the computer programmers (all of whom are human, and all of whom are declarants) who by object code or source code provide the instructions to computers to make conditional statements.

II. Admissibility Generally

The procedural schema in the United States:

Requires the parties to present trial evidence pursuant to rules that make it clear when proof has been formally proffered before it is introduced and then may be considered by the trier of fact in resolving fact issues. The proponent needs to know how to introduce evidence, the opponent must know when to object, and the judge needs to know when to rule. The rules of practice concerning presentation of evidence, offers of proof, and objections all are designed to secure this result. [36]

To this end, the FRE provides the contextual framework (further interpreted by case law) in accordance with which counsel may offer evidence or challenge, impeach, or rebut such evidence. The FRE, together with case law precedent, provides guidelines for a court in determining evidentiary rulings.

**[*222]** The provisions of the FRE lend themselves to a flow chart of actions that must be taken by a party offering digital data into evidence, and decisions to be made by a judge, before any such admission into evidence.

[SEE FIGURE IN ORIGINAL]

The decision points of this flow chart are not fixed, and, subject to existing precedent, the FRE provides a judge with the discretion to determine the admissibility of an item of evidence. Evidence, whether a thing, record, **[*223]** photograph, or testimony, is not admitted automatically into trial for scrutiny by a jury or judge. [37] For reasons not pertinent to this discussion (including but not limited to privilege and substantial unfair prejudice), computer-generated information sought to be admitted (and otherwise admissible) may be excluded (or not permitted to be used) at trial. [38] Accordingly, while any point reached along the FRE flow chart discussed in this Article may be

---

accurately fits within the purview of the F.R.E depiction of "original"]. It should also be noted that the adoption of this term also permits a disambiguation of the term "time' for digital data creation. While "first instantiation' can have only one time reference as it relates to data creation, "original' data can be created at many different times.

Id. In Lorraine v. Markel Am. Ins. Co., then-Chief U.S. Magistrate Judge (and now U.S. District Judge) Paul Grimm of the District of Maryland identified this issue in dicta in what is perhaps the seminal decision on authentication and admissibility:

Because it is so common for multiple versions of electronic documents to exist, it sometimes is difficult to establish that the version that is offered into evidence is the "final" or legally operative version. This can plague a party seeking to introduce a favorable version of its own electronic records, when the adverse party objects that it is not the legally operative version, given the production in discovery of multiple versions.

*Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 547 (D. Md. 2007)*.

[35] An example of unreadable binary code is 01101010101101101100010100111010101001110100101 01.

[36] 1 McCormick on Evidence § 51 (6th ed. 2006) (footnotes omitted).

[37] See *Lorraine, 241 F.R.D. at 538* ("Whether ESI is admissible into evidence is determined by a collection of evidence rules that present themselves like a series of hurdles to be cleared by the proponent of the evidence. Failure to clear any of these evidentiary hurdles means that the evidence will not be admissible." (footnote omitted)).

favorably met, admission is not necessarily guaranteed by laying a proper foundation for authentication, nor is admissibility guaranteed by the applicability of a hearsay exception.

Generally, therefore, all relevant evidence that is not privileged or deemed to cause substantial unfair prejudice is admissible. [39] Once the initial hurdles of relevancy and the like have been met by a party offering the evidence, evidence must be authenticated by some means that satisfy Rule 901(a)'s requirement that evidence "is what [its] proponent claims," or, as more commonly stated, that "evidence is what it purports to be." [40]

"Traditional" Authentication

In order for evidence to be admissible, it must be identified or authenticated by extrinsic evidence in a manner that complies with Rule 901(a). Non-limiting examples of methods of authentication are set forth in Rule 901(b). Such methods include the testimony of a witness or witnesses with knowledge, expert opinion, distinctive characteristics "and the like," or the efficacy of a particular method or process in producing an accurate result. [41] The test used is minimalist by design, and this minimalist approach has been embraced by the majority view in what is known as the "rationality test." [42] The "rationality test" provides that authentication requirements will **[*224]** be met so long as it would be rational for a jury to find that the evidence is authentic. [43] The hurdles presented by these subsections to Rule 901(b) to authentication are therefore low and easily traversed. [44] Accordingly, this low bar to authentication also facilitates the admissibility of inherently unreliable ESI as evidence. [45]

"Traditional" Hearsay

---

[38] There are several other reasons for exclusion of such evidence. See *Fed. R. Evid. 104(a)* (preliminary questions); id. 402 (relevance); id. 403 (prejudice, waste of time); *id. 501* (privilege).

[39] Id. 401; id. 402; id. 403.

[40] *Id. 901*(a); *United States v. Caldwell, 776 F.2d 989, 1001-02 (11th Cir. 1985)* ("Authentication or identification under rule 901 merely involves the process of presenting sufficient evidence to make out a prima facie case that the proffered evidence is what it purports to be. Once that prima facie showing has been made, the evidence should be admitted, although it remains for the trier of fact to appraise whether the proffered evidence is in fact what it purports to be.").

[41] *Fed. R. Evid. 901(b)(1)*, (3), (4), (9).

[42] See *MDU Res. Group v. W.R. Grace & Co., 14 F.3d 1274, 1282 n.12 (8th Cir. 1994)* ("However the issue is phrased, the analysis is the same. Rule 901(a) provides that the authentication requirement "is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.' To satisfy this requirement, MDU needed only to demonstrate a rational basis for its claim that the evidence is what MDU says it is.").

[43] See *United States v. Safavian, 435 F. Supp. 2d 36, 38 (D.D.C. 2006)* ("The question for the Court under Rule 901 is whether the proponent of the evidence has offered a foundation from which the jury could reasonably find that the evidence is what the proponent says it is… . The Court need not find that the evidence is necessarily what the proponent claims, but only that there is sufficient evidence that the jury ultimately might do so." (internal quotation marks and citation omitted)).

[44] *Lexington Ins. Co. v. W. Pa. Hosp., 423 F.3d 318, 328 (3rd Cir. 2005)* ("We have repeatedly noted that "the burden of proof for authentication is slight.'"); *Conner v. City of Jackson, Tenn., No. 08-1146, 2009 WL 3429690, at 3 (W.D. Tenn., Oct. 19, 2009)* ("[A] party need only put forth enough evidence that a reasonable juror could find the document is what it is purported to be." (citation omitted)); *CA, Inc. v. Simple.com, Inc., 780 F. Supp. 2d 196, 223 (E.D.N.Y. 2009)* ("[Authentication] requires little more than a prima facie showing of authenticity: it "does not erect a particularly high hurdle.'" (citation omitted)).

[45] The issues arising from this minimalist approach to digital data authentication have lain dormant for the last half-century or more: "The common law approach to authentication of documents has been criticized as an "attitude of agnosticism,' as one which "departs sharply from men's customs in ordinary affairs,' and as presenting only a slight obstacle to the introduction of forgeries in comparison to the time and expense devoted to proving genuine writings which correctly show their origin on their face." *Fed. R. Evid. 901* advisory committee's note (citations omitted).

While Rule 901 addresses authentication as a pre-condition to admissibility, Rule 801 refers to the exclusion of hearsay evidence even if the party offering the evidence lays a proper foundation for authentication. Accordingly, Article VIII effectively imposes a post-authentication requirement that a hearsay determination be made as a second pre-condition to admissibility. In order to be admissible, therefore, the evidence offered must first be authenticated or it is excluded.

Even if authenticated, the evidence is typically excluded if deemed hearsay, unless the evidence falls under an articulated exception to the hearsay rule. [46] Hearsay, which is defined as a "statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted," is generally not admissible. [47] There are, however, certain exceptions to the hearsay rule, where, under certain conditions, a court is permitted (but not required) to **[*225]** admit evidence that would otherwise constitute inadmissible hearsay. [48] One major exception is provided by Rule 803(6), which is titled "Records of Regularly Conducted Activity," but is typically referred to as the "Business Records Exception." [49] "Residual Hearsay," embodied in Rule 807 (and formerly a Rule 803 exception) permits admissibility of other types of hearsay based upon "equivalent circumstantial guarantees of trustworthiness." [50] Once authenticated, evidence may be deemed hearsay and inadmissible, or it may be deemed hearsay but qualify as an exception to the hearsay exclusionary rule, in which case the evidence maintains its admissible status.

The result of that process, which is common to the operation of both Rule 901 (authentication) and Rule 801 (hearsay), is to permit or preclude evidence at a hearing or trial. The authentication provisions of Rule 901 and the hearsay exclusionary provisions of Rule 801 may therefore be considered to occupy sequential yet co-equal status as pre-conditions to admissibility. [51] Finally, the Rules permit post-admission introduction before a jury of relevant evidence pertaining to "weight or credibility." [52]

Lack of Uniformity in the Judicial Approach

There is no uniformity of approach in lower court decisions towards the issue of authentication and admissibility of computer-generated information offered as evidence for trial. [53] The issue is complicated by the absence of any United States Supreme Court guidance as to whether digital data is inadmissible hearsay, or not. This lack of Supreme Court guidance has not **[*226]** escaped judicial notice. [54] Some courts appear to view all computer-

---

[46] See *Fed. R. Evid. 803*; ***id. 807***.

[47] ***Id. 801***(c).

[48] ***Id. 803***.

[49] See, e.g., Cross v. Amtec Med., Inc., No. 3:09-CV-00168-*HTW-LRA, 2012 WL 4603396 at 7 n.2 (S.D. Miss. Sept. 30, 2012)* ("*Rule 803(6) of the Federal Rules of Evidence*, commonly known as the "Business Record's Exception to the Hearsay Rule … .'").

[50] ***Fed. R. Evid. 807***.

[51] One important distinction between the authentication process and the hearsay assessment process is that while Rule 901(b) provides non-limiting authentication options, Rule 802 provides for the express exclusion of hearsay evidence not articulated as an exception in Rule 803, or that does not comply with the express language of Rule 807.

[52] *Fed. R. Evid. 104(e)*.

[53] Compare ***St. Clair v. Johnny's Oyster & Shrimp, Inc., 76 F. Supp. 2d 773, 774-75 (S.D. Tex. 1999)*** (viewing the internet as "one large catalyst for rumor, innuendo, and misinformation," stating that there was "no way" the plaintiff could "overcome the presumption that the information he discovered on the Internet [was] inherently untrustworthy," and excluding the information as hearsay, characterizing it as "voodoo information taken from the Internet"), with *Perfect 10, Inc., v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146 (C.D. Cal. 2002)* (following Ninth Circuit's relaxed authentication and admissibility requirements, court found declaration sufficient to authenticate print-outs of web site).

generated information as hearsay, perhaps saved from exclusion by qualifying under the business records exception. [55] Other courts do not consider certain categories of computer-generated data as hearsay, [56] or require only a Rule 901(b)(9) showing that the evidence is an accurate result from a system or process. [57] In more recent decisions, however, a number of courts have tended to consider a higher degree of evidential reliability, even for laying a foundation under Rule 901. [58]

One court's approach to internet-posted evidence indicates a marked disinclination to admit computer-generated information by labelling such data "voodoo information" incapable of finding a basis for admission even under the "most liberal" interpretation of the hearsay exception rules. [59] The court in the St. Clair case places much emphasis on its understanding (some of it presumably apocryphal) of computer-generated data:

Anyone can put anything on the Internet. No web-site is monitored for accuracy and nothing contained therein is under oath or even subject to independent verification absent underlying documentation. Moreover, the Court holds no illusions that hackers can adulterate the content on any web-site from any location at any time. For these reasons, any evidence procured off the Internet is adequate for almost nothing, even under the most liberal interpretation of the hearsay exception rules found in Fed. R. Civ. [sic] P. 807. [60]

Other judicial authority accords a greater degree of presumptive trustworthiness or reliability to computer-generated information and is friendlier to its admission as evidence. A Federal District Court in California, relying on a Ninth Circuit precedent, eschewed the St. Clair **[*227]** approach in favor of admitting print-outs of computer logs from a website. [61] Although the court in Perfect 10 acknowledged that there is a reduced evidentiary standard to be applied in preliminary injunction motions, it nevertheless ruled certain printouts of web pages admissible after considering the declaration of the party offering the printouts together with the circumstantial authenticity of the content (internet domain address and the date of the print-outs). [62] Nevertheless, neither the St. Clair nor the Perfect 10 decisions provide any substantive basis for concluding that computer-generated information is, or is not, hearsay. Indeed, these decisions are representative of the disparate approaches to categorize computer-generated information as hearsay or non-hearsay for purposes of admission into evidence at trial. To date, the Supreme Court has not offered an opinion on the issue. [63]

It may be safely assumed that an abundance of digital evidence arising in today's commercial and complex litigation is placed into the hearsay exception category as business records. Thus, once authenticated, the next hurdle for

---

[54] See Hawkins v. Cavalli, No. C03-3668 PJH, 2006 WL 2724145, at 12 (N.D. Cal. Sept. 22, 2006).

[55] ***St. Clair, 76 F. Supp. 2d at 775***.

[56] *United States v. Hamilton, 413 F.3d 1138, 1142 (10th Cir. 2005)* (file header information accompanying pornographic images uploaded to the Internet not considered an assertion or statement by a declarant and held not hearsay).

[57] *U-Haul Int'l Inc. v. Lumbermens Mut. Cas. Co., 576 F.3d 1040, 1045 (9th Cir. 2009)* (testimony regarding process used to create computer summaries held sufficient basis for authentication pursuant to *Fed. R. Evid. 901(b)(9)*).

[58] See, e.g., *In re Vee Vinhnee, 336 B.R. 437, 442, 446 (B.A.P. 9th Cir. 2005)*; *In re Vargas, 396 B.R. 511 (Bankr. C.D. Cal. 2008)*; *Lorraine v. Markel Am. Life Ins. Co., 241 F.R.D. 534, 542-43 (D. Md. 2007)*; *State v. Swinton, 847 A.2d 921, 941-42 (Conn. 2004)*; *Rodd v. Raritan Radiological Assoc., 860 A.2d 1003, 1012 (N.J. Super. Ct. App. Div. 2004)*.

[59] ***St. Clair, 76 F. Supp. 2d at 773***.

[60] ***Id. at 774-75***. Although the court cited to the Federal Rules of Civil Procedure, it is probable that the reference to Rule 807 is actually to Federal Rules of Evidence.

[61] *Perfect 10, Inc., v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1155 (C.D. Cal. 2002)*.

[62] *Id. at 1154, 1165*.

[63] Hawkins v. Cavalli, No. C03-3668 PJH, 2006 WL 2724145, at 12 (N.D. Cal 2006).

admissibility necessitates satisfying that exception's testimonial evidence requirements relating to contemporaneity, knowledge, and regularity (of conduct and practice) requirements. [64] By categorizing computer-generated information only as a subset of business records, judges have thus been able to avoid the central issues that are uniquely inherent to the authentication of computer-generated information. The Pennsylvania Supreme Court recently acknowledged that:

Judicial decisions to date have largely skirted the edge of the problem because they have been concerned mainly with computerized records made in the regular course of business… . Routinely prepared records, admitted pursuant to business records acts such as *28 U.S.C. § 1732* are well recognized exceptions to the hearsay rule, because their regular use in the business of the company insures a high degree of accuracy. Proof of day-to-day business reliance upon computerized records should therefore make less onerous the burden of laying a proper foundation for their admission. [65]

The Klinghoffer court considered that computer-generated information that was not categorized as a business record as hearsay, but (unlike the court in St. Clair), admitted the evidence on the condition of meeting the **[*228]** "circumstantial guarantees of trustworthiness" set forth in the residual hearsay provisions of Rule 807:

Where, however, a computer is programmed to produce information specifically for purposes of litigation, an entirely different picture is presented. Its product, which is hearsay and conclusory, is not admissible under *28 U.S.C. § 1732* or similar state statutes… . Under such circumstances, a court should not permit a witness to state the results of a computer's operations without having the program available for the scrutiny of opposing counsel and his use on cross-examination… Moreover, such availability should be made known sufficiently in advance of trial so that the adverse party will have an opportunity to examine and test the inputs, program and outputs prior to trial. [66]

Indeed, one court notes that the "requirements for authenticating a business record are identical to those for laying a foundation for its admissibility under the hearsay exception." [67]

The implications arising from these findings of interchangeability appear to illustrate the poorly articulated need to incorporate a requirement to show digital data trustworthiness or reliability (otherwise typically a finding made from within the context of a hearsay determination), into an express or free-standing precondition to the admissibility process. [68]

It is clear that computer-generated information that is not a business record might consist of a digital photograph of an accident scene taken by a bystander, a computer-generated document containing a home inventory for insurance purposes, or a non-business related e-mail containing allegedly defamatory matter. None of these examples can be easily (if at all) included in the business records category, and it is not surprising that there is no authority directly addressing these examples and evaluating whether they are hearsay or not (although this digital data could be offered into evidence pursuant to Rule 807 provided that the proponent complies with its additional

---

[64] *Fed. R. Evid. 803(6)*.

[65] *Commonwealth. v. Klinghoffer, 564 A.2d 1240, 1242-43 (Pa. 1989)*.

[66] *Id. at 1243* (citations omitted).

[67] *FDIC v. Carabetta, 739 A.2d 301, 308 (Conn. App. Ct. 1999)*.

[68] In one of the seminal decisions on the admissibility of digital evidence, Chief Magistrate Judge Paul Grimm of the U.S. District Court for the District of Maryland advances the argument that trustworthiness is an evaluative factor in both authentication and hearsay admissibility assessments. "The requirement of authentication and identification also insures that evidence is trustworthy, which is especially important in analyzing hearsay issues. Indeed, these two evidentiary concepts often are considered together when determining the admissibility of exhibits or documents." *Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 542 (D. Md. 2007)*.

procedural requirements). Moreover, it appears that the drafters' express intent was to make Rule 801 a limiting definition (and a limiting evidentiary **[*229]** exclusion rule) such that if species of evidence did not fit clearly into one of the definitions of hearsay, it was not to be considered hearsay [69]: "The definition [of hearsay set forth in Rule 801] does not in terms say that everything not included within the definition is not hearsay, but that was the intended effect of the rule, according to the Advisory's Committee's Note." [70]

There can be little doubt that vast amounts of non-business records digital information are generated each year. Such digital data, if considered hearsay, will be admissible if at all, only pursuant to Rule 807. With this exponential increase in non-business digital data, the need is clear for the adoption of a uniform and well-articulated approach to the admissibility of computer-generated information.

III. Hearsay, Digital Data, and the "Declarant"

An increase of what at least one court describes as a lack of understanding of computer-generated evidence is emblematic of a new and critical complication that arises out of attempts to define computer-generated information. [71] This complication involves semantics, specifically those relating to the concept of hearsay. Hearsay is defined as a "statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted." [72] A "statement" is defined in part as a person's oral or written assertion intended to be an assertion. [73] A "declarant" is defined as "a person who makes a statement." [74] The FRE provide, therefore, that hearsay does not exist without a declarant, and that the pre-condition to being a declarant is that a declarant must be a person. Problems in semantics arise from the meaning and application of the term "declarant" as it appears in the various hearsay provisions of the FRE. A literal interpretation of Rule 803 is that a declarant may not be computer **[*230]** data or a computer program because neither data nor a computer program is a person. [75]

Indeed, three circuits and at least two district courts have held that where a machine generates data without the assistance of a person, there is neither a "statement" nor a "declarant," and therefore, no hearsay. [76] Some courts

---

[69] The residual hearsay rule (formerly an exception) operates only in certain limited circumstances. See *United States v. Phillips, 219 F.3d 404, 419 n.23 (5th Cir. 2000)* ("The [residual hearsay] exception is to be "used only rarely, in truly exceptional cases.'").

[70] *United States v. Hamilton, 413 F.3d 1138, 1143 (10th Cir. 2005)* (quoting John W. Strong, McCormick on Evidence § 246, at 97 (5th ed. 1999)). It is perhaps with good reason that the Supreme Court of Connecticut noted that the divergent views on computer-generated evidence arise in large part from the lack of understanding by those at the bar and the bench. *State v. Swinton, 847 A.2d 921, 939-40 n.25 (Conn. 2004)*.

[71] *Swinton, 847 A.2d at 939-40 n.25*.

[72] *Fed. R. Evid. 801(c)* (restyled Dec. 1, 2011).

[73] ***Id. 801***(a).

[74] ***Id. 801***(b) (restyled Dec. 1, 2011).

[75] See *Stevenson v. State, 920 S.W.2d 342, 343 (Tex. Ct. App. 1996)* (holding that an intoxilyzer was not a declarant and information generated by it was not a statement, and thus, not hearsay).

[76] *United States v. Washington, 498 F.3d 225, 231 (4th Cir. 2007)* ("Raw data generated by the machines do not constitute "statements,' and the machines are not "declarants.'"); *United States v. Hamilton, 413 F.3d 1138, 1142 (10th Cir. 2005)* (holding that file header information accompanying pornographic images uploaded to the internet was not hearsay); *United States v. Khorozian, 333 F.3d 498, 506 (3d Cir. 2003)* (holding that header information automatically generated by fax machine was not hearsay because "nothing "said' by a machine … is hearsay."). See also *United States v. Crockett, 586 F. Supp. 2d 877, 885 (E.D. Mich. 2008)* (holding that printouts of crime laboratory mass spectrometer and gas chromatograph testing results were not hearsay, because the instruments were not "persons," and thus not declarants, so they could not make "statements" for hearsay purposes); Hawkins v. Cavalli, No. C03-3668 PJH, 2006 WL 2724145 at 12 (N.D. Cal 2006) (holding that computer printouts of

have distinguished between computer-"generated" and computer-"stored" information in making a hearsay determination. [77] That line of decisional authority underscores the lack of understanding of how computers work, as all computer information is always first generated. Thus, there can be no storage of computer information without generation (or instantiation) occurring as a necessary precondition. Computer-generated information may then be stored, transmitted, or even deleted, but it must exist before it is stored, and in order to exist it must be generated. This issue is related to the distinction between "original" data, and origination, source, or first instantiation, of computer generated information. Accordingly, an analysis in relation to "generated" and "stored" data is agonistic, strained at best, [78] **[*231]** and creates a distinction without a difference, although some might wish the matter was otherwise. [79]

One Approach: Treat Digital Data as Hearsay

There is a plausible argument that can be made in support of the proposition that all digital data constitutes some type of hearsay. Certain assumptions must first be made. First, computer generated information of any type, whether output, operating system or application files or data, and even the metadata, are statements made by a computer programmer or like person through the means of a computer language. [80] These statements, or assertions, are conditional statements, which in essence provide instructions to a computer that, given a certain set of conditions, the computer is told to make a statement on behalf of the computer programmer. [81] That statement

---

computer access records were not hearsay "because a human was not responsible for setting and coordinating the computer's recording of access dates. Rather, the access dates were completely computer-generated with no human input").

[77] See 1st Fin. SD, LLC v. Lewis, No. 2:11-CV-00481-*MMD-VCF, 2012 WL 4761931, at 2 (D. Nev. 2012)* ("Metadata is generated automatically by the software that creates a file, not an individual user. For that reason, it cannot be excluded as hearsay"). The 1st Financial court, in dicta, noted that the alteration of metadata may transform it into hearsay: "Of course, Defendants may challenge the authenticity of the metadata by providing some evidence of alteration, e.g., arguing that the metadata was deliberately altered by an individual, thereby properly characterizing it as hearsay." Id. at 3. See also *Hawkins, 2006 WL 2724145, at 12*.

[78] This strained distinction between computer-stored and computer-generated information was highlighted in a recent federal bankruptcy court decision addressing the issue:

Two different standards exist for electronic business records. Records which are not created by a computer but are merely stored on one are not subject to the particular reliability concerns that arise with records generated by a computer. As a result, they are subject to the lesser standard set forth in Midfirst Bank, which states that computer records, with limited exceptions not applicable here, must merely meet the requirements of Rule 803(6) and do not require additional authentication… . Records that are generated by a computer using data compiled or created by the computer present questions regarding reliability and accuracy which require a higher standard for authentication. Thus, records created by this method are subject to the standard suggested by Imwinkelreid and must meet each of the factors.

*In re McFadden, 471 B.R. 136, 161 (Bankr. D.S.C. 2012)* (citation omitted).

[79] The author has experienced first-hand attempts to delineate between ESI "generated," and ESI "stored" in a litigation matter. The author's client represented the plaintiff, and requested from the defendant electronically stored information, in native data format, with all associated metadata, and as generated by defendant in the conduct of its everyday activities. The defendant produced documents in TIFF, rather than in native data format, claiming that while it might have "generated" such information in "live" or native format, it "stored" such information only as TIFF format files. The difference between generated and stored here is significant. The "generated" ESI here would have provided searchable content and metadata. The TIFF files produced were not searchable, and contained no metadata. In this instance, the "first instantiation" of data could only be the data as generated, and not as ultimately stored. The matter settled before the issue was determined by the court.

[80] One of the first modern computer languages is COBOL (Common Business Oriented Language), which was introduced in 1959. Jiehong Li & Rona Abraham, COBOL 1 available at *http://www.csee.umbc.edu/courses/graduate/631/Fall2002/COBOL.pdf*. Modern computer languages abound, and include, "C," "C++," "Objective-C," "Visual Basic," and "Python." See List of Programming Languages, Wikipedia, *http://en.wikipedia.org/wiki/List_of_programming* _languages (last visited Sept. 5, 2013).

may be another instruction, or it may be computer-generated information, output by the computer. [82] It is important to understand that the computer only generates information it is instructed to make on behalf of the person **[*232]** instructing it to make a statement. [83] Contrary to popular opinion, and generally unless there is some hardware malfunction, computers do not make mistakes, nor do they generate any information not instructed by a human programmer to make. In these instances, if a mistake is made, it is not the computer that makes a mistake, but the result of a mistaken statement (i.e., an instruction or assertion) that a computer is told by the programmer to make - whoever the programmer may be (that is, a third person may cause malicious software to be downloaded on to a computer, and the computer will thus take instructions from this software). [84]

The Hamilton case provides an example of how a court can get the concept of computer language wrong, and thereby draw conclusions not supported by logic. There, the judge determined that a file header cannot be considered a statement made by a person who transmits that file to another computer over the Internet. [85] The Hamilton court, accordingly, ruled that there is no hearsay because there is no person making a declaration as required by Rule 801(b). [86] However, the commands (contained in a computer program) to create a file header, to transmit a file, to receive a file, to generate a log of file creation, transmission or receipt activities, and to enter or not enter information into a log file, are all statements and may be considered to be a declaration of a person, that person being a programmer instructing a computer to make such statement in his or her stead; in other words, as an agent for the declarant. The instructions generally provide for the following analysis: When a certain condition or conditions are met, I (the computer programmer or system administrator) want you (the computer) to say "this" and nothing else, on my behalf.

This means that a computer and computer program will only produce information within the ambit of the instructions contained in the source code of the application, or program, and the application or program will only **[*233]** produce information intended to be created by the declaration of the creator of that application or program. The truth of that assertion (i.e., the asserted statement of a programmer) may only be ascertained through an examination of the source code written by that programmer. Therefore, an argument can be made that there is, and must always be, a person-declarant for any computer-generated information. To find that computers autonomously generate information independent of direct human instruction, (as did the Tenth Circuit in Hamilton and the United

---

[81] See Conditional (Computer Programming), Wikipedia, http://en.wikipedia.org/wiki/ Conditional_%computer_programming%29 (last visited Sept. 5, 2013).

[82] This is demonstrated in the case of State of Connecticut v. Julie Amero, where the police officer for the prosecution insisted that the color of a hyperlink proved that the accused had clicked on a pornographic web site because it was red, when, in fact, the web designer entered code to the web page, making it red when viewed. For an exhaustive analysis of this case, see Stephen Mason, International Electronic Evidence, at xxxvi-lxxv (2008).

[83] The traditional approach to hearsay evidence has been more concerned with the elimination of secondhand evidence provided by a witness who for some reason is not available to be cross-examined in court. This approach fails utterly when faced with the inherent traits unique to digital evidence. While it is true that digital evidence is ultimately generated by a computer, it is also the result of the speech, or declaration, of at least one computer programmer, speaking in a particular language, and translated by the computer into human readable output. Although the computer is not human, the information it generates represents the declaration of its programmers, as to what human readable output, or statement, should be generated. Steven W. Teppler, Digital Evidence as Hearsay (Part 2), EDDE J., Winter 2011, at 32 n.2.

[84] Even a computer "crash" or malfunction, is not the result of a mistake by the computer. Rather, it is the result of language written into a program. That language is called a "bug," or fault that is deliberatively written in computer language, by the programmer or coder making that statement, and embodied in the executable compiled therefrom. Crash (Computing), Wikipedia, http://en.wikipedia.org/ wiki/Crash_(computing) (last visited Oct. 13, 2013).

[85] See *United States v. Hamilton, 413 F.3d 1138, 1142 (10th Cir. 2005)*.

[86] Id.

States District Court for the Central District of California in Hawkins) comes perilously close to anthropomorphism, and would impart sentience into computing devices that simply (and at least at present) does not exist. [87]

Moreover, the statement made by a programmer to a computer that instructs the computer to make another statement, such as a file header or other metadata, illustrates the computer programmer's desires and intent to make his or her statement through that computer's processes. It is not, as so presciently put by Judge Van Graafeiland, merely a calculation made by a machine with a "giant memory." [88] For instance, the file header contains specific information, including a statement made by programmer that he or she desires to convey if certain conditions are met, including a statement of time. Note that ultimately, programmers, administrators and human users of a computer are making statements. Persons make these statements, and these statements can easily be deemed as declarations falling within the purview of the hearsay rule if the intended result of these assertions is content to be read or viewed by a recipient. To date, no authority expressly adopts this position. [89] If, however, the objective is to provide for reliability, uniformity **[*234]** and consistency in relation to the authentication and admissibility of digital data, the treatment of computer-generated information generally as hearsay, accompanied by a requisite affirmative showing of reliability in the content, rather than in output, would be a major step in reaching this aspiration.

Determining What Is Hearsay

Judicial authority appears to divide computer-generated information into three categories for the purpose of distinguishing what is hearsay. The first category refers to the creation of computer-generated information input into a computer solely by a person. The second category refers to that class of computer-generated information input into a computer in part by a person, and in part by a computer application. The third category refers to computer information generated without direct human input or assistance. [90] A person creating a memorandum using a word processing application may exemplify the first category. The second category is exemplified by a person creating a form for a computer to arrange and complete. An example of the third category of computer-generated information exists where a computer creates a record of a transaction with another computer. These categories will be examined from the perspective of the traditional approach, and the complications and contradictions either created or left unresolved by that approach will be considered. A fourth potential category, for which there has been no

---

[87] The late Alan Turing is considered by many to be the father of modern binary computing, and he described a "test' for computer independence of thought, or sentience. The Turing Test is a proposal for a test of a machine's capability to demonstrate thought. See A. M. Turing, Computing Machinery and Intelligence, 59 Mind 433, 433-34 (1950). It proceeds as follows: a human judge engages in a natural language conversation with two other parties, one a human and the other a machine; if the judge cannot reliably tell which is which, then the machine is said to pass the test. It is assumed that both the human and the machine try to appear human. In order to keep the test setting simple and universal (to explicitly test the linguistic capability of the machine instead of its ability to render words into audio), the conversation is usually limited to a text-only channel such as a teletype machine, as Turing suggested, or more recently, IRC or instant messaging. Teppler, supra note 83, at 33 n.3.

[88] *Perma Research & Dev. v. Singer Co., 542 F.2d 111, 124 (2d Cir. 1976)* (Van Graafeiland, J., dissenting) ("Statements like those of the District Judge that a computer is "but calculators [sic] with a giant memory and the simulations the computer produces are but the solutions to mathematical equations in a logical order' represent an overly-simplified approach to the problem of computerized proof which should not receive this Court's approval." (internal quotation marks omitted)).

[89] Such analyses are most likely to be found in dissenting opinions, and even then little consideration is given to the analysis. The dissenting opinion from an unpublished Virginia case considers the issue with the intensity of a Klieg light, but ultimately disregards the categorization of computer-generated information into "hearsay" and "non-hearsay": "It is unlikely that computer-generated evidence will be offered into evidence for some purpose other than "to prove the truth of a matter asserted,' and thus is hearsay." *Watlington v. Commonwealth, No. 2332-99-3, 2000 WL 1672871, at 3* (Benton, J., dissenting) (emphasis added) (quoting Randy Snyder, Note, Assuring the Competency of Computer-Generated Evidence, 9 Computer L.J. 103, 104 (1989)). Teppler, supra note 83, at 33 n.5.

[90] For a similar analysis, see Mason, supra note 8, at xiii.

judicial analysis, has recently emerged as a consequence of computer programs that "listen and respond" to questions in natural language and with a "voice" that closely mimics a "real" human.

First Category: The Memorandum "Created" by a Human

A memorandum created by a person if offered for the truth of its content, is generally considered hearsay whether or not it is also considered a business record. [91] If the memorandum sought to be admitted is a business record, the provisions of Rule 803(6) must be satisfied. [92] Rule 803(6) **[*235]** requires that either the author of the memorandum must give evidence to provide corroborative testimony, or a "custodian or other qualified witness" must testify that the "data compilation" was "made at or near the time by a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the … data compilation." [93] Notably, the phrasing of 803(6)(e) creates a near presumption of reliability. This presumptive trustworthiness arises out of what is typically a very light burden on the proponent asserting the exception. [94]

There are significant problems with the Rule 803(6) analysis. [95] All computer-generated information has metadata, or data about data, generated in association with the generation of the content itself. The question that then arises is whether the data compilation comprising the memorandum includes the content of the memorandum, and the metadata associated with that memorandum. It must be correct that the additional data is included with the content. [96] That metadata, which is also computer-generated information, can contain a plethora of information, including source data, time and date information, a digital signature, routing information, date of creation, the last time it was viewed, modifications, the approval of a purported person who reviewed the content, and even the application and version of the application with which the content was created. [97] It is asserted **[*236]** by some that the generation

---

[91] See United States v. Cinergy Corp., No. 1:99-cv-1693-LJM-JMS, 2009 WL 6327419, at 3 (S.D. Ind. Apr. 24, 2009).

[92] The memorandum is both a Rule 803(6) memorandum and a "data compilation." The difference is that a memorandum has some semantic meaning ascribed to it, transforming it into "information." For the purpose of this example, however, the terms are used interchangeably. Teppler, supra note 83, at 34 n.7.

[93] *Fed. R. Evid. 803(6)* (alteration in original).

[94] See, e.g., *In re McFadden, 471 B.R. 136, 160 (Bankr. D.S.C. 2012)* ("Rule 803(6) merely requires, for records to be admissible as business records, the witness must be familiar with the company's record keeping system. Mr. Goss, as a record custodian for Saxon, clearly meets that test. His testimony established that he has custody of Saxon's records and is familiar with how they are obtained, modified, and stored." (citation omitted)).

[95] If the memorandum is considered not to be a business record, another traditional approach might still deem the contents of the memorandum hearsay (if offered for its truth), and therefore anyone offering it will be required to comply with the pre-condition regarding admissibility under the residual hearsay requirements set out in Rule 807. Unlike the admission of a business record, however, the operation of Rule 807's "equivalent circumstantial guarantees" language would require an affirmative showing of trustworthiness. The application of Rule 807's more robust reliability requirements should be considered a reasonable substitute for the near-presumption of trustworthiness now provided by Rule 803(6)'s Business Records exception, particularly where mutable computer generated information may consist of untestable erroneous computer information regularly generated, as a regular practice, and in the usual course of activity.

[96] An even more problematic possibility exists where a person digitally signs an entire data compilation, including metadata. The digital signature is a representation of a statement by the purported signer, and the metadata by definition forms a part of that statement, even though first instantiated by an "automated" computer process.

[97] Metadata is not only evidence about evidence, but is evidence itself. Log files, master file tables, e-mail headers and the like are all evidence of digital events that occur within a computer, and these digital events may, by themselves be factual rather than merely contextual and used to prove an assertion or claim. For example, the time of an event associated with a memorandum may appear in at least two areas outside the memorandum that a human is able to view. These times should not differ, but may well do so in the event of time-based data manipulation. Without access to such metadata, a party would not have the ability to test the consistency of the asserted time of relevancy (if not the reliability of the time itself). A second example

of this data is made without the input or assistance from a person. [98] In accordance with decisional authority and Rule 801(b), this information could not be considered hearsay, even if it otherwise might be considered a business record. Thus, while the content of the memorandum might be hearsay (whether or not a business record), the associated metadata responsible for all aspects of its existence and format inexplicably is not. If the content is a person or declarant, and metadata is anything but a person or declarant, it is suggested that a two-step authentication process for such computer-generated data ought to be considered. The content of the memorandum, which is hearsay, would first require determination under the provisions of Rules 803(6) or 807. The metadata associated with the memorandum, however, would only require authentication under the provisions of Rules 901(b)(1) or 901(b)(9). Under this analysis, the memorandum metadata created by a person and input into a computer could never be considered to be created only by a person, and therefore, purely hearsay under either Rules 803(6) or 807. Not surprisingly, the same analysis may be used where a person creates a form to be filled out by other people using various forms of software.

In other words, while the content of the memorandum would be considered hearsay, and subject to analysis as to whether it was hearsay and **[*237]** therefore to be excluded, or an exception and therefore admitted, the metadata associated with the content would need only to be authenticated, and not subject to any hearsay analysis, in order to be admissible. Since the reliability and accuracy of metadata in some instances may be of greater evidentiary significance than the content (e.g., in instances where the metadata, but not the content, has been altered or deleted), [99] issues of reliability should attach concurrently to both the content and the metadata. In reality, therefore, computer-generated information in categories one and two are the same, and should be treated in an identical manner.

The element of time significantly complicates any hearsay analysis. Critical to any evidentiary analysis is an association of time with the relevant evidential event. At issue in this example will be what time is referred to as it is associated with the memorandum. It could be the time that the document was created by the purported author of the memorandum; the time stated within the content of the memorandum (which may differ from the time the document is recorded as being created); or the time that the memorandum was created according to the metadata information (i.e., file properties or file header). In addition, other questions that might be posed include the time typed into the memorandum, and whether this constitutes part of the "declaration" by a "person" at the "time" of the declaration. A further issue is the time value contained in the metadata, and whether it is a statement by the person who "told" (i.e., programmed) the computer to state a specific time on his or her behalf. Arguably, it may be necessary to reconcile the "time" contained in the content, or hearsay portion of the data compilation as being admissible as a part of a "declaration" by a "person" with a different "time" statement (and statement it is) contained

---

supporting the production of metadata in evidence exists in the case of "hybrid documents" or documents of one format embedded within documents of another format. For instance, it is easy to bring together a Microsoft Excel document into a Microsoft Word document. In such cases, the Excel(R) spreadsheet could clearly be considered metadata to the Word(R) document. The Excel(R) document, potentially containing relevant evidence, would be rendered totally invisible and undetectable to the reader perusing the document using Word(R). If a producing party converted the hybrid Word(R) document to PDF format, the format conversion process would strip all the Excel(R) information. The production of all relevant metadata is therefore critical to the efficacy of the discovery process itself. Teppler, supra note 83, at 35 n.9.

[98] *United States v. Hamilton, 413 F.3d 1138, 1142 (10th Cir. 2005)* (holding automatic generation of downloaded file header information not hearsay: "In other words, the header information was generated instantaneously by the computer without the assistance or input of a person. As concluded by the district court, this uncontroverted fact clearly places the header information outside of Rule 801(c)'s definition of "hearsay.' In particular, there was neither a "statement' nor a "declarant' involved here within the meaning of Rule 801."). Other courts have adopted the Tenth Circuit's reasoning in Hamilton, see *United States v. Washington, 498 F.3d 225, 233 (4th Cir. 2007)* ("In only one circumstance is a computer-generated assertion not considered the statement of a person: when the assertion is produced without any human assistance or input."); see also *United States v. Crockett, 586 F. Supp. 2d 877, 885 (E.D. Mich. 2008)* (following Hamilton, holding mass spectrometer readouts and printouts machine, and not human generated, and therefore not statements).

[99] These alterations, modifications, or deletions may well be made by a person.

in metadata, which arguably need only be subject to the 901(b)(9) "accurate result" rule because such information would not be considered hearsay. [100]

If these two "times" differ substantially, and if reliability and testability is the new watchword for admissibility of computer-generated evidence, there are a number of possible permutations: (1) The computer-generated content with the more "reliable" time is admissible, and that the computer-generated information content considered "less reliable" is excluded; (2) that the entire data compilation, including content and metadata, must be excluded; or (3) that the entire data compilation is admissible. It is **[*238]** respectfully submitted that none of these options can be preferred, because the current criteria for categorizing and evaluating computer-generated information are contradictory, cumbersome, and ill suited to accomplish the task. For example, the first choice would mean a court excludes metadata and admits content, or admits metadata but excludes content, both of which would defeat any possibility of establishing the provenance of the computer-generated information offered as evidence. Excluding or admitting the entire data compilation might obviously serve to further the purpose of one party, or be more judicially expedient, but it would also thereby detract from the integrity of the evidentiary process, and the efficacy of trial proceedings in general.

Characterizing all computer-generated information as hearsay, and imposing an affirmative testable reliability requirement to an exception to the exclusionary rule, or requiring the admissibility of all computer-generated information to be conditioned on Rule 807's "equivalent circumstantial guarantees of trustworthiness," would help avoid these artificially created distinctions.

Second Category: Digital Data Generated in Part with Human Assistance

As discussed above, no computer data can be created or generated by a human without some associated data or metadata, generated by the computer itself. Accordingly, and in this way, computer-generated information described in the first and second categories are identical. The problems posed by this digital data category are underscored by recent introduction of the "Siri" application by Apple, Inc. [101] The "voice" one hears in response to a query sounds like a human voice. Siri's "voice" is actually computer-generated information sourced from an unknown place, then processed, perhaps many times, and rendered into audio output closely approximating human conversational language. [102]

**[*239]** If a person not a party to the Siri "conversation" hears Siri respond to a query, but the conversation is not known to involve a computer, is what is heard by that third party hearsay? Likely not (at least under the current evidence rules and decisional authority), as the declarant in this example would not be a "person" making a statement. If it is revealed that the conversation was with a computer application named Siri, and Siri made the response, is the response then not considered hearsay and admissible for its truth after a simple Rule 901(b)(9) "accuracy of result" authentication foundation has been properly made? What if the Siri conversation involves the use of an iPhone application that measures the degree of mobility impairment, and Siri states in response to a

---

[100] As discussed supra, a third possibility is for a court to consider metadata as hearsay, as the declaration of a person in the position of a computer system or network administrator, a computer programmer, and the like. In that case, the admissibility of both the memorandum (if deemed hearsay) and its associated metadata would be predicated upon complying with the appropriate requirements of admissibility provided under Rule 803(6) or Rule 807.

[101] Siri is a network based "intelligent personal assistant that helps you get things done just by asking." Siri Frequently Asked Questions, Apple, *http://www.apple.com/iphone/features/Siri-faq.html* (last visited Sept. 6, 2013). Siri is an application offered by Apple that listens, interprets and responds to queries in natural language: "Talk to Siri as you would to a person. Say something like "Tell my wife I'm running late' or "Remind me to call the vet.' Siri not only understands what you say, it's smart enough to know what you mean. So when you ask "Any good burger joints around here?' Siri will reply "I found a number of burger restaurants near you.' Then you can say "Hmm. How about tacos?' Siri remembers that you just asked about restaurants, so it will look for Mexican restaurants in the neighborhood. And Siri is proactive, so it will question you until it finds what you're looking for." Siri: Your Wish Is Its Command, Apple, *http://www.apple.com/ios/siri/* (last visited July 22, 2013).

[102] See Siri: Your Wish Is Its Command, supra note 101.

query: "Your ability to maintain your balance is substantially impaired," and law enforcement attempts to admit the testimony of the third party listener to Siri's response as evidence of impairment after an automobile accident? [103] What result if, in a civil matter, the human participant to the Siri conversation is heard to state: "Please affix my digital signature to that email contract" but the email cannot be located? Apple disclosed that it mines data and stores both the content as well as the information associated with each Siri interaction, including time, duration, location, and query and response. [104] Is what Apple stores considered metadata, or is it information generated by a computer without the assistance of a human? Is this information considered generated or merely "stored"? It may be both, underscoring the distinction without a difference between "generated" and "stored" evidence categorization approach adopted by courts today. [105]

Third Category: Digital Data Generated Without a Human Being

In this category, metadata created during the generation of computer information, such as a file header (or data about data) created during an upload of an image file to a remote computer, has been held not to be hearsay because, using a strict application of the hearsay rule, there was no "person" making a declaration.

**[*240]** As the court points out in U.S. v. Hamilton:

The district court in this case correctly concluded that the header information that accompanied each pornographic image was not hearsay. Of primary importance to this ruling is the uncontroverted fact that the header information was automatically generated by the computer hosting the newsgroup each time Hamilton uploaded a pornographic image to the newsgroup. In other words, the header information was generated instantaneously by the computer without the assistance or input of a person. As concluded by the district court, this uncontroverted fact clearly places the header information outside of Rule 801(c)'s definition of "hearsay." In particular, there was neither a "statement" nor a "declarant" involved here within the meaning of Rule 801. [106]

Here, a cogent argument appears to be made to the effect that the computer-generated information created by a remote computer during the process by which the remote computer receives computer-generated information transmitted to it from another computer is not a statement of a person, and therefore, not hearsay. In this instance, both metadata information (file header, IP address) as well as the content created by the remote computer might be considered not to be hearsay and subject only to the "accurate result" requirement of Rule 901(b)(9). The argument against this logic and in favor of determining the data transmitted to be hearsay, is that the receiving computer is carrying out the stated intent or declaration of some person who instructed the computer to make the assertion on his or her behalf (e.g., a programmer) to carry out some request (and provided that certain conditions are met) that the receiving computer was told by the sending computer as agent for that person, which in turn was requested by a statement or declaration of the person or sender.

It is suggested that all computer-generated information is hearsay of some sort. The "differences" between human-generated computer information and non-human-originated computer-generated information are illogical, and create categorizations that are merely distinctions without differences. Moreover, these artificial "differences"

---

[103] In this instance, the issue would be whether Siri's response could be considered testimonial hearsay, and therefore, subject to Sixth Amendment Confrontation Clause protections. See *Crawford v. Washington, 541 U.S. 36, 61-62 (2004)*; *Melendez-Diaz v. Massachusetts, 129 S. Ct. 2527, 2531 (2009)*.

[104] See Robert McMillan, Apple Finally Reveals How Long Siri Keeps Your Data, Wired (Apr. 19, 2013, 6:30 AM), *http://www.wired.com/wiredenterprise/2013/04/siri-two-years/*; see also Jonathan Burg, Siri + Apple Know a Lot About You, Who Cares About Privacy?, Jon Burg's Future Visions (Oct. 19, 2011, 2:24 AM), *http://www.jonburg.com/future/2011/10/siri-apple-know-a-lot-about-you-who-cares-about-privacy.html*. Other providers of "free" online services who engage in similar behavior may include Microsoft, Google, Facebook, Twitter, Instagram, and Flickr.

[105] See, e.g., *In re McFadden, 471 B.R. 136, 161 (Bankr. D.S.C. 2012)*.

[106] *United States v. Hamilton, 413 F.3d 1138, 1142 (10th Cir. 2005)*.

underscore the need for a more unified and technology-oriented approach to evaluating computer-generated information offered as evidence based on testable reliability.

**[*241]**

IV. Constitutional Issues: Digital Data as Speech

In a recent decision from the Second Circuit, the court determined that computer language, including object code as well as source code, was "speech" for purposes of the First Amendment. [107]

Object code, source code, and even a developer's remarks from uncompiled code have been held to comprise "speech" for First Amendment purposes. [108] Accordingly, if computer-generated information is held to be "speech" for First Amendment purposes, one should question why such speech has been deprecated to the status of "non-speech" for hearsay purposes. This dichotomy raises serious implications in criminal proceedings.

Crawford v. Washington - Testimonial Hearsay and the Sixth Amendment

The Supreme Court's seminal decision in Crawford v. Washington generally holds that a Sixth Amendment right to cross-examination will arise where testimonial hearsay is used to establish an element of a crime or used **[*242]** to convict. [109] Consider the application of this to computer-generated information used to convict or to establish an element of a crime. When considered, for example, with respect to the output of a blood alcohol testing appliance or other electronically stored evidence, the issue of whether ESI is hearsay takes on new and increased significance. If such computer-generated evidence (the blood alcohol testing device as a computer) is testimonial hearsay, a defendant will be entitled to cross examine the source code and object code in order to help establish his or her innocence.

---

[107] Having concluded that computer code conveying information is "speech' within the meaning of the First Amendment, we next consider, to a limited extent, the scope of the protection that code enjoys." *Universal City Studios, Inc. v. Corley, 273 F.3d 429, 449-50 (2d Cir. 2001)*. "But the fact that a program has the capacity to direct the functioning of a computer does not mean that it lacks the additional capacity to convey information, and it is the conveying of information that renders instructions "speech' for purposes of the First Amendment. The information conveyed by most "instructions' is how to perform a task.'" *Id. at 447-48*. "Programmers use snippets of code to convey their ideas for new programs; economists and other creators of computer models publish the code of their models in order to demonstrate the models' vigor." *Id. at 448 n.21*. The court further noted:

Reinforcing the conclusion that software programs qualify as "speech' for First Amendment purposes - even though they instruct computers - is the accelerated blurring of the line between "source code' and conventional "speech.' There already exist programs capable of translating English descriptions of a program into source code. These programs are functionally indistinguishable from the compilers that routinely translate source code into object code. These new programs (still apparently rudimentary) hold the potential for turning "prose' instructions on how to write a computer program into the program itself. Even if there were an argument for exempting the latter from First Amendment protection, the former are clearly protected for the reasons set forth in the text. As technology becomes more sophisticated, instructions to other humans will increasingly be executable by computers as well.

*Id. at 448 n.22* (citations omitted). "Code, because it uses a notational system comprehensible by humans, is communication that qualifies as speech." *Id. at 449 n.24*.

[108] See *Universal City Studios, Inc. v. Reimerdes, 82 F. Supp. 2d 211, 219 n.29 (S.D.N.Y. 2000)* ("Defendants asserted at oral argument that DeCSS, or some versions of it, contain programmer's comments, "which are non-executable appendages to lines of executable code.' … Such comments are protected by the First Amendment." (citation omitted)).

[109] See *Crawford v. Washington, 541 U.S. 36 (2004)*. The Supreme Court articulated the testimonial hearsay Confrontation Clause issue in a decision rendered subsequent to Crawford and Melendez: "As a rule, if an out-of-court statement is testimonial in nature, it may not be introduced against the accused at trial unless the witness who made the statement is unavailable and the accused has had a prior opportunity to confront that witness." *Bullcoming v. New Mexico, 131 S. Ct. 2705, 2713 (2011)*.

Computer code and output has the ability to "speak" for someone, and at times this "someone" may be a coder or programmer. In an exhibit to a software patent issued by the U.S. Patent and Trademark Office, one patentee included his uncompiled source code as an exhibit. [110] In a criminal matter, as a defendant, it might be necessary to know how the computer code in a device that was instrumental in providing evidence that a crime was committed, might have so failed. Under the doctrine articulated in Crawford v. Washington, the defendant would be guaranteed the right under the Sixth Amendment to cross examine the program code, or "speech" of the programmer, and perhaps even the programmer. If, however, the computer code, or computer-generated information, was deemed not to be hearsay, the right to examine either the computer source code (or its programmer) that helps convict (perhaps more correctly stated as "who helps convict") might not be guaranteed.

The Supreme Court expanded the application of the Crawford doctrine in 2009 and appears to be edging toward an understanding that a computer might in fact be the agent of a declarant uttering testimonial hearsay, thereby enabling the defendant the right of cross-examination under the Sixth Amendment Confrontation Clause. In Melendez-Diaz v. Massachusetts, the Court determined that a drug-testing examiner's certificate (considered equivalent to an affidavit) was both accusatory and testimonial, thus permitting cross-examination. [111] The Court reasoned that such certificates were created with the sole intent to be used as evidence at trial, and that under Massachusetts law, the sole purpose of the certificate was to provide prima facie evidence of composition, quality and net weight. [112] This **[*243]** evidence was clearly both testimonial and accusatory, and that the petitioner was entitled to "confront" the persons giving this testimony. [113] The Court further held that such certificates are the functional equivalent of "live, in-court testimony." [114]

At the heart of the court's extension of the Crawford doctrine is the notion of reliability that can be tested. The Court found that the aim of the Confrontation Clause is to ensure evidentiary reliability, but nonetheless confirms that the guarantee is procedural rather than substantive. The Melendez-Diaz decision is also important because it expressly associates evidence reliability with testability. [115]

The Melendez-Diaz decision provides a tantalizing hint, and perhaps only a hint, that the Court might entertain an appeal based on the Confrontation Clause in connection with the reports (not maintenance reports) created by Breath-a-lyzer (blood alcohol testing) appliances. [116] The Melendez-Diaz Court also recognized the potential for manipulation of evidence. [117] On appeal, an argument might be made that the output of the appliance (i.e., a

---

[110] U.S. Patent No. 5,619,571 (filed June 1, 1995).

[111] *129 S. Ct. 2527, 2542 (2009)*.

[112] *Id. at 2532*.

[113] Id. But see *Williams v. Illinois, 132 S. Ct. 2221, 2240 (2012)* (5-4 decision) (holding that the testimony of forensic specialist did not violate petitioner's confrontation rights because the laboratory's report was not offered into evidence to prove the truth of the matter asserted). In his decisive concurrence, Justice Thomas stated that the report was not offered to prove truth, accordingly not "testimonial," and therefore, not subject to Sixth Amendment Confrontation Clause application. *Id. at 2256* (Thomas, J., concurring).

[114] The "certificates' are functionally identical to live, in-court testimony, doing "precisely what a witness does on direct examination.'" *Melendez-Diaz, 129 S. Ct. at 2532* (citations omitted).

[115] To be sure, the Clause's ultimate goal is to ensure reliability of evidence, but it is a procedural rather than a substantive guarantee. It commands, not that evidence be reliable, but that reliability be assessed in a particular manner: by testing in the crucible of cross-examination… . Dispensing with confrontation because testimony is obviously reliable is akin to dispensing with jury trial because a defendant is obviously guilty. This is not what the Sixth Amendment prescribes." *Id. at 2536* (citations omitted).

[116] See *id. at 2536 n.5* ("Some forensic analyses, such as autopsies and breathalyzer tests, cannot be repeated, and the specimens used for other analyses have often been lost or degraded.").

computing device) is ultimately both accusatory and testimonial; that the code, or language used to create the accusatory output will be considered testimonial hearsay, and accordingly that a defendant that is accused of having a higher-than-legal blood alcohol level based on such appliances, will be afforded the right to examine the code under the Sixth Amendment Confrontation Clause. Future decisions could prove interesting, because the **[*244]** report of the Breath-a-lyzer itself may well be deemed a type of testimonial hearsay, invoking the application of the Confrontation Clause. [118]

It appears that perhaps in future decisions, the reliability of computer-generated information (testable accuracy and trustworthiness) may be made a freestanding precondition for admissibility, rather than a factor to be accorded post-admission weight by a trier of fact. In the absence of a new evidence rule directed to the admissibility of digital evidence, the characterization of digital information as hearsay pursuant to Rule 807 would at least require some affirmative demonstration of testable reliability of content (as distinguished from reliability of process and output) as a precondition for admissibility.

Computers that Accuse

An example of the confusion arising from the failure to determine whether digital data is hearsay or not, is perhaps best exemplified by recent opinions in criminal cases. These decisions focus on the admissibility of information generated by what are commonly known as "Breath-a-lyzer' machines, or computers that measure an automobile driver's breath-alcohol levels. [119] A court in Texas has held that "the intoxilyzer instrument is a computer, not a person. By definition, therefore, the intoxilyzer is not a declarant… . Because the intoxilyzer is not a declarant, the data it generates is not a statement and cannot be hearsay." [120]

A few recent cases have undertaken a different analysis. One Florida court has required that under the Florida full information law, [121] the source code used in a Breath-a-lyzer machine must be produced for examination by the state. The court stated, in pertinent part, that:

An instrument or machine that can be used by the State to establish the guilt of an accused subjecting them to mandatory fines, mandatory loss of driving privileges, and loss of freedom (sometime mandatory) should be made available to the defense for open inspection … [The disclosure of] full information should include the software that runs the instrument. To construe the statute otherwise is tantamount to granting the state authority to use confidential information (i.e., the software code) to establish the guilt **[*245]** of a criminal defendant … . The software is an integral part of the intoxilyzer [sic]. Unless the defense can see how the intoxilyzer [sic] breathalyzer works … , it remains as stated by the Court in Muldowny and more recently by Judge Ralph E. Erikkson as being nothing more than a "mystical machine" used to establish an accused's guilt. State v. Lentz, 12 Fla. L. Weekly Supp. 806(a) (18th Judicial Circuit, Seminole County, April 29, 2005). [122]

The Florida court did not address the hearsay issue, but the analysis clearly indicates that computer code can be used to establish guilt. The device at issue in State v. Lentz does not retain any samples of the breath provided by a

---

[117] See *id. at 2536* ("Forensic evidence is not uniquely immune from the risk of manipulation."). It should therefore come as no surprise that evidentiary issues associated with computer-generated information typically involve some degree of forensic acquisition and analysis.

[118] The Bullcoming Court expressly identified, but expressly declined to rule on this issue: "We do not decide whether, as the New Mexico Supreme Court suggests, a State could introduce (assuming an adequate chain of custody foundation) raw data generated by a machine in conjunction with the testimony of an expert witness." *Bullcoming, 131 S. Ct. 2705, 2722 (2011)*.

[119] See, e.g., State v. Jack Irish, Case No. 2006-CT-02109 SC (Fla. Sarasota Cty. Ct. 2006).

[120] *Stevenson v. State, 920 S.W.2d 342, 343 (Tex. Ct. App. 1996)*.

[121] *Fla. Stat. Ann. § 316.1932(1)(f)(4)* (West Supp. 2013).

[122] State v. Jack Irish et al., Case No. 2006-CT-02109 SC (Fla. Sarasota Cty. Ct. 2006).

suspect driver, and the only evidence is the information processed by the appliance. [123] It is clear that the computer information generated by the Intoxilyzer therefore accuses (or exonerates) a defendant, and this information is "spoken" by the code contained in the device. The code conveys information, and that information is the programmer's statement, or declaration. For example, a recent patent issued by the United States Patent and Trademark Office included some uncompiled source code that contained a rather pointed comment that might lead an attorney during cross-examination to further explore a program's data output reliability and testability. [124] This information, which is the assertion, and declaration, of a person made out-of-court, and which would otherwise have been used for the truth of its content, would not be discovered if only the computing device (here the Intoxylizer) or the compiled code were produced for examination. [125] Accordingly, the only "testimony" for blood alcohol level can come from the Intoxilyzer itself, or more specifically, the code that speaks to that information. [126]

The issue as to whether computer-generated information is or is not hearsay may eventually be resolved under the standard articulated in Crawford v. Washington. In that opinion, the Supreme Court held generally that the use of testimonial hearsay automatically invokes a defendant's Sixth **[*246]** Amendment right to confrontation. [127] A future case might present a series of facts that includes the use of computer-generated information, not generally considered hearsay (such as file metadata or the output of an Intoxilyzer-type computing appliance) but which may nonetheless be considered testimonial. If computer-generated information is held to be testimonial hearsay, and afforded Confrontation Clause protection permitting the examination of source code, it would not take a quantum leap in analysis to find that that computer source code, as a species of evidence, is also hearsay from within the context of civil litigation, requiring a heightened showing of reliability and testability.

## V. Reliability of Digital Data Today

The mutability characteristic of digital data renders it inherently unreliable, and this mutability includes "wiping" or expunging, modifying, altering or otherwise changing digital data. [128] To thoroughly expunge data from a single computer requires more than merely downloading and running a wiping utility. There are many locations on the hard disk that might either contain a pointer to an earlier version of data, or a copy of data that might otherwise be considered irretrievable. [129] For instance, the operation of an automatic file backup in a word processing application may save one or a number of recent versions of a document. [130] Moreover, evidence of the existence

---

[123] State v. Lentz, 12 Fla. L. Weekly Supp. 806a (Fla. Seminole Cty. Ct. Apr. 29, 2005).

[124] U.S. Patent No. 5,619,571 (filed June 1, 1995) ("If this fails, we are fd.").

[125] It should be pointed out that an officer who administers the Intoxilyzer test does not determine or assess whether a suspect driver has a blood alcohol level above the limit set by law.

[126] But see *United States v. Washington, 498 F.3d 225, 227 (4th Cir. 2007)* (holding that a toxicology laboratory testing machine data output was not the out of court statement of the laboratory technician, and appearing to eschew the notion that computer-generated information is testimonial hearsay, and therefore not subject to Crawford's Sixth Amendment confrontation rights). Note that this decision holds merely that the testing machine's output is not the statement of the laboratory technician, and does not address whether the machine's statement is the statement of the program (and programmer) that generated the data.

[127] *Crawford v. Washington, 541 U.S. 36, 68-69 (2004)*.

[128] *Nearon et al., supra note 16*.

[129] Such information includes metadata. See *Aguilar v. Immigration & Customs Enforcement Div. of the U.S. Dep't of Homeland Sec., 255 F.R.D. 350, 354 (S.D.N.Y. 2008)* ("Metadata, frequently referred to as "data about data,' is electronically-stored evidence that describes the "history, tracking, or management of an electronic document.' It includes the "hidden text, formatting codes, formulae, and other information associated' with an electronic document." (citation omitted)).

[130] Such information is frequently found in what is known as "system metadata." See id. ("System metadata "reflects information created by the user or by the organization's information management system.' This data may not be embedded within the file it describes, but can usually be easily retrieved from whatever operating system is in use. Examples of system metadata include data concerning "the author, date and time of creation, and the date a document was modified.'" (citation omitted)).

of digital data (and what happened to it during its life cycle) may be found in a master file table or other logging operation that takes place without the knowledge of the user. [131] In addition, a simple erasure or deletion typically does not expunge data, but only removes the "pointer" to the data, and the data itself remains accessible unless and until overwritten (in whole or in part) by newly generated data. [132] In a networked system, a **[*247]** user may think she is expunging data at a workstation, only to find that the network server automatically copies, archives, or backs up all data generated by the workstation. That said, the distinction between expunging data and the mutable nature of data may best be explained by presuming that mutable digital data relates to the difficulty of proving persistent data integrity (some technologists might describe this as proving "statefulness"), rather than whether it does or does not exist.

This characteristic should be considered when determining reliability. Digital data that is, under the current admissibility schema, almost totally dependent upon corroborative testimony may have little, if anything, to do with the authenticity of the content sought to be admitted. The criteria to ascertain admissibility of computer-generated information must, it is suggested, require a demonstration of heightened reliability and testability. In addition, it must do so in a manner that does not merely mirror the techniques for evaluating physical evidence.

The modern requirement for reliability appears to suggest the merger of the "accurate result" test embodied in Rule 901(b)(9), the "trustworthiness" test enumerated in Rule 803(6), with the "equivalent circumstantial guarantees" test enumerated in Rule 807. Hints of this merger have appeared as early as 1987: "The principal precondition to admission of documents as business records pursuant to *FRE 803(6)* is that the records have sufficient indicia of trustworthiness to be considered reliable." [133] Other courts have, in more recent decisions, included the concept of reliability into determining admissibility where digital data, whether considered hearsay or not, is being offered into evidence. [134] E-mail (and, presumably, such truncated communications as "tweets" and text messages) has emerged as a significant mode of electronic communication. Although still considered by many **[*248]** courts to be a casual communication, some jurists are beginning to require demonstration of enhanced reliability. [135] A more

---

[131] Id.

[132] That mere deletion of a file does not remove the file itself, but merely a pointer to it, has been expressly recognized by at least one U.S. Circuit Court of Appeals. See *Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 419 (7th Cir. 2006)* ("Ordinarily, pressing the "delete' key on a computer (or using a mouse click to delete) does not affect the data sought to be deleted; it merely removes the index entry and pointers to the data file so that the file appears no longer to be there, and the space allocated to that file is made available for future write commands. Such "deleted' files are easily recoverable. But Citrin loaded into the laptop a secure-erasure program, designed, by writing over the deleted files, to prevent their recovery. IAC had no copies of the files that Citrin erased." (citation omitted)); see also *Dedalus Found. v. Banach, No. 09 Civ. 2842 (LAP), 2009 WL 3398595, at 3 (S.D.N.Y. Oct. 16, 2009)* (citing to the Seventh Circuit decision in Citrin: "The Court explained that merely pressing the delete key on a computer does not remove data but rather "removes the index entry and pointers to the data file so that the file appears no longer to be there.'").

[133] *Potamkin Cadillac Corp. v. B.R.I. Coverage Corp., 38 F.3d 627, 632 (2d Cir. 1994)*; see also ***Saks Int'l, Inc. v. M/V Exp. Champion, 817 F.2d 1011, 1013 (2d Cir. 1987)***.

[134] See *In re Vee Vinhnee, 336 B.R. 437, 445 (B.A.P. 9th Cir. 2005)* ("This ever-expanding complexity of the cyberworld has prompted the authors of the current version of the Manual for Complex Litigation to note that a judge should "consider the accuracy and reliability of computerized evidence' and that a "proponent of computerized evidence has the burden of laying a proper foundation by establishing its accuracy.'"); see also *Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 542 (D. Md. 2007)*.

[135] See It's My Party, Inc. v. Live Nation, Inc., Civil No. JFM-09-547, *2012 WL 3655470, at 5 (D. Md. Aug. 23, 2012)* ("Email, however, is typically a more casual form of communication than other records usually kept in the course of business, such that it may not be appropriate to assume the same degree of accuracy and reliability. As email is more commonly used to communicate business matters both internally and externally, however, more formal paper records are becoming more unusual. Nevertheless, I decline to accept a blanket rule that emails constitute business records; more specificity is required regarding the party's recordkeeping practices to show that a particular email in fact constitutes a reliable business record.").

rigorous standard for requiring heightened reliability for electronic communications appears to have raised the bar for exclusion under the "business records" exception to the hearsay rule. [136]

The basis for determining the reliability of computer-generated information differs greatly from that of physical evidence. Although the provenance of the evidence must still be established, the requirements in respect of digital data are not the same as physical evidence. Simply put, it is not old wine in new bottles. On the one hand, it is possible to observe the process by which a human controls and applies pen to paper, and forensic tests can be performed to assist in and corroborate witness testimony in **[*249]** connection with a determination as to the authenticity of the document. On the other hand, it is not certain (and certainly without access to and testing of interpretation, or translation of the source or origination data and code) how a computer is programmed to speak for its programmers or content creators. This lack of knowledge means the reliability of the data cannot be realistically ascertained without some measure of testability.

Whether couched in terms such as "trustworthiness" or "accurate result," the concept of reliability remains a central prerequisite leading to the admissibility of evidence. To the detriment of modern jurisprudence, however, the evolution of the concept of reliability as a precondition to admissibility of digital data has not kept up with the revolution in information technology. Nevertheless, there has been some slow but steady judicial recognition of the reliability issues that are unique and inherent to digital data. Some recent judicial authority appears to indicate a sputtering trend away from revisiting the approach to digital data pre-conditions to admissibility, but whether it takes the form of a revision of the rules for authentication, hearsay, or the implementation of a freestanding rule in favor of a more general and flexible concern for reliability remains unclear. [137]

There has been some recognition of this in state decisional authority. In a seminal 2004 opinion, the Supreme Court of Connecticut announced its new approach to computer-generated evidence, declaring reliability as an essential pre-condition of admissibility. [138] The Swinton opinion held, in pertinent part, that a trial court improperly admitted

---

[136] See In re Deepwater Horizon, No. 2179, 2012 WL 85447, at 3 (E.D. La. Jan. 11, 2012):

The individual elements required to trigger the exception's applicability show that there is no categorical rule that emails originating from or received by employees of a producing defendant are admissible under the business records exception. First of all, the email must have been sent or received at or near the time of the event(s) recorded in the email. Thus, one must look at each email's content to determine whether the email was created contemporaneously with the sender's acquisition of the information within the email. Second, the email must have been sent by someone with knowledge of the event(s) documented in the email. This requires a particularized inquiry as to whether the declarant - the composer of the email - possessed personal knowledge of the information in the email. Third, the email must have been sent or received in the course of a regular business activity, which requires a case-by-case analysis of whether the producing defendant had a policy or imposed a business duty on its employee to report or record the information within the email. Fourth, it must be the producing defendant's regular practice to send or receive emails that record the type of event(s) documented in the email. This would require proof of a policy of the producing defendant to use email to make certain types of reports or to send certain sorts of communications; it is not enough to say that as a general business matter, most companies receive and send emails as part of their business model. Fifth, a custodian or qualified witness must attest that these conditions have been fulfilled - which certainly requires an email-by-email inquiry. Lastly, the objecting defendant is permitted under the rule to argue that the particular email should be excluded due to concerns of lack of trustworthiness, based on the information source underlying the email content or the circumstances under which the email was sent and received. Clearly, there is no across-the-board rule that all emails are admissible as business records.

See also Rogers v. Or. Trail Elec. Consumers Coop., Inc., No. 3:10-CV-1337-*AC, 2012 WL 1635127, at 9 (D. Or. May 8, 2012)*; Innovention Toys, LLC v. MGA Entm't, Inc., No. 07-6510, 2012 WL 5893476 at 7 (E.D. La. Nov. 4, 2012).

[137] See, e.g., *Lorraine, 241 F.R.D. at 543* ("[While] anybody with the right password can gain access to another's e-mail account and send a message ostensibly from that person … the same uncertainties exist with traditional written documents. A signature can be forged; a letter can be typed on another's typewriter; distinct letterhead stationary can be copied or stolen." (quoting *In re F.P., 878 A.2d 91, 95 (Pa. 2005))*); see also *In re Vee Vinhnee, 336 B.R. 437 (B.A.P. 9th Cir. 2005)*.

[138] *State v. Swinton, 847 A.2d 921, 942 (Conn. 2004)*.

into evidence computer enhanced photographs of bite marks and images that purported to represent the defendant's dental structure as lacking a proper foundation. [139] The approach of the court in Swinton was to assess the admissibility itself (rather than the weight) of computer enhanced evidence.

**[*250]** It is significant that the Swinton court itself grappled with the concept of computer-generated evidence, and noted that there "is no universal definition of that term." [140] The Swinton court also recognized the unique evidentiary issues presented by computer-generated evidence. [141] It was also noted that that the appearance of computer-generated evidence at trials in Connecticut was limited and typically involved business records. [142] In a manner strikingly reminiscent of Judge Van Graafeiland's dissenting comments in Perma Research, [143] the members of the Swinton court appear to bemoan the paucity of understanding by both attorneys and the members of the judiciary about the nature and issues presented by digital data, and suggested that this lack of understanding has contributed in turn to the scarcity of relevant authority. [144]

The Swinton reliability test for admissibility of computer-generated evidence has been accorded increasing authority, and has been relied upon and extended by other courts when considering the admissibility of computer-generated (rather than enhanced) exhibits. In a recent New Jersey decision, the court stated:

In our view, the use of a computer-generated exhibit requires a more detailed foundation than that for just photographs or photo enlargements. The latter "must be proved to be faithful representations of the subject at the time in question. Fundamentally, photographs are deemed to be pictorial communications of a qualified witness." However, considering the reliability problems arising from computer-generated exhibits and the processes by which they are created, there must be "testimony by a person with some degree of computer expertise, who has sufficient knowledge to be examined and cross-examined about the functioning of the computer." [145]

**[*251]** In holding that web page print-outs bearing a URL (Uniform Resource Locator) address and date stamp were improperly authenticated by declaration, one court pointed out that "printouts from a website do not bear the indicia of reliability demanded for other self-authenticating documents under *Fed. R. Evid. 902*. To be authenticated,

---

[139] *Id. at 938*. The court in Swinton addressed the admissibility of computer generated information in terms of reliability:

A witness must be able to testify, adequately and truthfully, as to exactly what the jury is looking at, and the defendant has a right to cross-examine the witness concerning the evidence. Without a witness who satisfactorily can explain or analyze the data and the program, the effectiveness of cross-examination can be seriously undermined, particularly in light of the extent to which the evidence in the present case had been "created.'

*Id. at 951-52* (footnotes omitted).

[140] *Id. at 937*.

[141] The Court "did not agree with the state's proposition that the enhanced photographs in the present case are like any other photographs admitted into evidence, and we determine that, to the extent that a computer was both the process and the tool used to enable the enhanced photographs to be admitted as evidence, we consider these exhibits, for the purposes of this analysis, to be computer generated." *Id. at 938* (footnote omitted).

[142] Id.

[143] See supra note 17.

[144] *Swinton, 847 A.2d at 939-40 n.25* ("Commentators have attempted to explain this lack of case law involving basic foundational challenges to this sort of evidence. "Although computer systems raise serious reliability issues, the reported cases do not adequately reflect this reality.'… Why do the reported cases fail to adequately expose the serious reliability issues raised by computerized information? Many people, including defense attorneys, prosecutors, judges, and juries, do not understand computers." (internal citation omitted)).

[145] *Rodd v. Raritan Radiological Assoc., 860 A.2d 1003, 1011-12 (N.J. Super. Ct. App. Div. 2004)* (internal citations omitted).

some statement or affidavit from someone with knowledge is required; for example, Homestore's web master or someone else with personal knowledge would be sufficient." [146]

More recently, a bankruptcy panel for the Ninth Circuit upheld a bankruptcy court's refusal to admit the unopposed offer of a computer-generated printout consisting of an American Express cardholder's transactions. [147] Adopting what appears to be the blending of the business records hearsay exception under Rule 803(6) with the "accurate result" standard provided by Rules 901(b)(1) and (9), and the "equivalent circumstantial guarantees of trustworthiness" set forth in Rule 807, the court affirmed the lower court's finding that "the electronic nature of the records necessitated, in addition to the basic foundation for a business record, an additional authentication foundation regarding the computer and software utilized in order to assure the continuing accuracy of the records." [148] That additional authentication addressed the electronic records continuing integrity over time, such that its integrity (or statefulness) at the time of assertion was unchanged from the time of creation. [149] To date, however, decisional authority still pays undue homage to Rule 901's low bar to authenticity, to Rule 803(6)'s presumptive trustworthiness of business records, or to a characterization of digital data as non-hearsay. Accordingly, the FRE offer a reliability and testability by-pass in connection with authentication and hearsay evaluation of computer generated information. Moreover, where digital data is considered non-hearsay, if such evidence could reasonably be reliable, the evaluation for reliability goes to the trier of fact as a matter of evidential weight rather than admissibility. [150] The **[*252]** mutability and largely untestable characteristic of digital data gives rise to a substantially enhanced risk that untestable manipulated evidence could render an unjust result.

Old Rule, New Rule, or New Standard?

Irrespective of whether admissibility of digital data will be made subject to Rule 807's circumstantial guarantee, whether a new evidence rule addressing computer-generated information is promulgated, or whether decisional authority moves toward a new common law standard, testable reliability should remain the focus and hallmark for digital data admissibility. Treating all computer-generated information as hearsay subject to its affirmative trustworthiness guarantees pursuant to Rule 807 would substantially reduce low-quality evidentiary admissibility, and provide a more robust "reliability" standard that would better serve the goals of litigation and the attendant administration of justice. If Rule 807 is not utilized to reach this objective, the introduction of a new evidence rule incorporating a heightened affirmative reliability showing by a proponent seeking to admit digital data as evidence would effectuate the same result. [151] It is suggested that either approach would foster the development and

---

[146] *In re Homestore.com, Inc. Sec. Litig., 347 F. Supp. 2d 769, 782-83 (C.D. Cal. 2004)*.

[147] *In re Vee Vinhnee, 336 B.R. 437, 450-51 (B.A.P. 9th Cir. 2005)*.

[148] *Id. at 442* (emphasis added).

[149] *Id. at 444* ("Authenticating a paperless electronic record, in principle, poses the same issue as for a paper record, the only difference being the format in which the record is maintained: one must demonstrate that the record that has been retrieved from the file, be it paper or electronic, is the same as the record that was originally placed into the file.").

[150] See Churches of Christ in Christian Union v. Evangelical Benefit Trust, No. C2-07-*CV-1186, 2009 WL 2146095, at 5 (S.D. Ohio July 15, 2009)* (quoting *Lexington Ins. Co. v. W. Pa. Hosp., 423 F.3d 318, 328-29 (3d Cir. 2005)*):

We have repeatedly noted that "the burden of proof for authentication is slight.' … In Link, we elaborated on the standard for authentication of documents: The showing of authenticity is not on a par with more technical evidentiary rules, such as hearsay exceptions, governing admissibility. Rather, there need be only a prima facie showing, to the court, of authenticity, not a full argument on admissibility. Once a prima facie case is made, the evidence goes to the jury and it is the jury who will ultimately determine the authenticity of the evidence, not the court. The only requirement is that there has been substantial evidence from which they could infer that the document was authentic.

[151] A hearsay rule applicable to the testing of both witnesses and computer-generated information could potentially prove both complex and unwieldy. Ultimately, the characterization of digital data as hearsay is an interim solution providing some means for

evolution (especially as technology evolves) of a flexible, yet uniform requirement of an affirmative showing of testable reliability. An express rule change or adoption, the adoption of a unified approach to, and required showing of reliability would represent a significant step forward in the development of a flexible but uniform set of criteria to establish admissibility for digital data consistent with the two primary objectives of litigation: ascertaining the truth, and the efficient administration of justice.

In the future, computer-generated information that is (1) by human input, (2) by hybrid human and computer input, or (3) by the computer only, becomes merely digital data, subject to some admissibility concurrency requirement of reliability and testability. Pseudo-distinctions between **[*253]** computer-generated and computer-stored information would disappear, and the requirement of testable reliability could be universally imposed and uniformly considered. In addition, the confusion between "computer stored" and "computer enhanced" data may also disappear, thereby removing the current illogical, contradictory, and ultimately unworkable distinction that surrounds digital data.

Conclusion

Digital data comprises a species of evidence that came into existence only during the last seventy or so years. [152] It comes into being from a programmer's or coder's use of a computer interpreting his assertions by way of a language and in a manner that permits the computer output to "speak" as an agent on behalf of that application's programmer. Unlike non-electronic (i.e., "physical") evidence, such as paper and ink, digital data is designed to be mutable. [153] Digital data, as currently generated in most computing environments, is also not testable for accuracy and reliability. This inherent mutability, when combined with digital data's native untestability, renders an accurate assessment of reliability nothing more than mere guesswork, and invites the introduction and easy admission of manipulated or fabricated digital evidence. Rule 901's authentication schema fails to address the testable reliability of digital evidence integrity. Since the bar to authentication is admittedly low, there is also a correspondingly low requirement for any showing of testably reliable accuracy. This low bar to authentication fails to address reliable accuracy, because it requires nothing more than corroboration showing that a computing device will repetitively turn on, process information, and provide output in a consistent manner. [154] Unfortunately electronically stored information may be easily authenticated even if programmed to provide erroneous information, so long as a testimony of compliance with what is essentially a rote-based checklist is offered. [155] From this, an ostensibly

---

incorporating a reliability and testability requirement into the admissibility schema. What may work best is a new, separate evidence rule made expressly applicable to computer-generated evidence, and requiring a threshold showing of testable accuracy, reliability and trustworthiness as a pre-requisite to admissibility.

[152] ENIAC (Electronic Numerical Integrator And Computer) "was the first electronic general-purpose computer. It was Turing-complete, digital, and capable of being reprogrammed to solve a full range of computing problems." ENIAC, Wikipedia, *http://en.wikipedia.org/wiki/ENIAC* (last visited Aug. 7, 2013).

[153] *Nearon et al., supra note 16*.

[154] See *Link v. Mercedes-Benz of N. Am., Inc., 788 F.2d 918, 927 (3d Cir. 1986)* ("The burden of proof for authentication is slight. "All that is required is a foundation from which the fact-finder could legitimately infer that the evidence is what the proponent claims it to be.'").

[155] See *In re McFadden, 471 B.R. 136, 157 (Bankr. D.S.C. 2012)*:

Professor Imwinkelreid, one of the foremost experts on evidentiary foundations, endorses the use of the following eleven-part test to authenticate electronic business records:

1. The business uses a computer.

2. The computer is reliable.

3. The business has developed a procedure for inserting data into the computer.

4. The procedure has built-in safeguards to ensure accuracy and identify errors.

5. The business keeps the computer in a good state of repair.

"proper" foundation for admissibility **[*254]** may be laid, because, based on this minimal showing, a trier of fact could reasonably find that digital data is "what the proponent claims it is." [156] Rule 901's authentication regime fails to address even minimal standards of digital data testability and reliability, and so the search for reliability inevitably leads the bench and bar to the hearsay rules and exceptions embodied in Rules 806 and 807.

The near-presumptive trustworthiness schema of Rule 803(6)'s business records exception provides at best a mere gloss to a showing of reliability, resulting in a low bar to admissibility which offers only a hat-tip to the Federal Rules' reliability objective. The proposed characterization of all computer generated information as hearsay is also supported by both an examination of computer language, as well as long-standing authority that treats computer source and object code as "speech" for purposes of the First Amendment. [157] There is no supportable or substantial reason to change the meaning of computer-generated information from "speech" for protecting First Amendment rights, to "non-speech" in determining whether it is hearsay, especially in those cases where hearsay would necessarily invoke rights under the Confrontation Clause in criminal matters under Crawford and its progeny.

The need for revised evidentiary rules to add a flexible requirement of testable reliability as a pre-condition for admissibility of digital data is clear. Where computer information is offered for its truth, some showing of testable reliability should be required in order to minimize the likelihood of **[*255]** easy admissibility of potentially undetectable, manipulated, or fabricated digital evidence. Adopting a testable reliability standard would require the inclusion of a means to ascertain not only that digital evidence is "what it purports to be," but that such evidence is what it purports to be as of the time that relevance has been asserted, and that such evidence has remained unchanged since that time. The affirmative showing of trustworthiness guarantees required by Rule 807 provides the preferable approach. A recent concurrence by Chief Judge Posner of the U.S. Court of Appeals for the Seventh Circuit may indicate that judicial momentum for such recognition is gaining traction. [158] Characterizing all digital data as residual hearsay under Rule 807 would impose at least some circumstantial but affirmative "guarantee" of trustworthiness, which would increase the reliability and testability of evidence sought to be introduced for use at pre-trial or trial proceedings.

---

6. The witness had the computer readout certain data.

7. The witness used the proper procedures to obtain the readout.

8. The computer was in working order at the time the witness obtained the readout.

9. The witness recognizes the exhibit as the readout.

10. The witness explains how he or she recognizes the readout.

11. If the readout contains strange symbols or terms, the witness explains the meaning of the symbols or terms for the trier of fact.

[156] *Fed. R. Evid. 901(a)*.

[157] See *United States v. Elcom Ltd., 203 F. Supp. 2d 1111, 1126 (N.D. Cal. 2002)*:

The government contends that computer code is not speech and hence is not subject to First Amendment protections. The court disagrees. Computer software is expression that is protected by the copyright laws and is therefore "speech' at some level, speech that is protected at some level by the First Amendment… . While there is some disagreement over whether object code, as opposed to source code, is deserving of First Amendment protection, the better reasoned approach is that it is protected. Object code is merely one additional translation of speech into a new, and different, language.

[158] See *United States v. Boyce, 742 F.3d 792, 801 (7th Cir. 2014)* (Posner, C.J., concurring) ("What I would like to see is Rule 807 ("Residual Exception") swallow much of Rules 801 through 806 and thus many of the exclusions from evidence, exceptions to the exclusions, and notes of the Advisory Committee. The "hearsay rule" is too complex, as well as being archaic. Trials would go better with a simpler rule, the core of which would be the proposition (essentially a simplification of Rule 807) that hearsay evidence should be admissible when it is reliable, when the jury can understand its strengths and limitations, and when it will materially enhance the likelihood of a correct outcome.").

End of Document