Richmond Journal of Law and Technology

Volume 17 | Issue 2 Article 2

2011

The Admissibility of Electronic Evidence Under the Federal Rules of Evidence

Jonathan D. Frieden

Leigh M. Murray

Follow this and additional works at: http://scholarship.richmond.edu/jolt

 Part of the Evidence Commons, and the Internet Law Commons

Recommended Citation

Jonathan D. Frieden & Leigh M. Murray, *The Admissibility of Electronic Evidence Under the Federal Rules of Evidence*, 17 Rich. J.L. & Tech 5 (2011).
Available at: http://scholarship.richmond.edu/jolt/vol17/iss2/2

This Article is brought to you for free and open access by UR Scholarship Repository. It has been accepted for inclusion in Richmond Journal of Law and Technology by an authorized administrator of UR Scholarship Repository. For more information, please contact scholarshiprepository@richmond.edu.

THE ADMISSIBILITY OF ELECTRONIC EVIDENCE UNDER THE FEDERAL RULES OF EVIDENCE

By Jonathan D. Frieden* & Leigh M. Murray**

Cite as: Jonathan D. Frieden and Leigh M. Murray, *The Admissibility of Electronic Evidence Under the Federal Rules of Evidence*, XVII RICH. J.L. & TECH. 5 (2011), http://jolt.richmond.edu/v17i2/article5.pdf.

I. INTRODUCTION

[1] Following the December 2006 amendments to the Federal Rules of Civil Procedure, much has been written about the discovery of electronically-stored information ("ESI"). However, as one court noted,

> [v]ery little has been written . . . about what is required to insure that ESI obtained during discovery is admissible into evidence at trial . . . . This is unfortunate, because considering the significant costs associated with discovery of ESI, it makes little sense to go to all the bother and expense to get electronic information only to have it excluded from evidence or rejected from consideration during summary judgment because the proponent cannot lay a sufficient foundation to get it admitted.[1]

* Principal, Odin, Feldman & Pittleman, P.C., Fairfax, Virginia. B.A., 1994, University of Virginia; J.D., 1997, University of Richmond, T.C. Williams School of Law.

** Associate, Odin, Feldman & Pittleman, P.C., Fairfax, Virginia. B.A., 2005, The Pennsylvania State University; J.D., 2010, American University, Washington College of Law.

[1] Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 537-38 (D. Md. 2007).

Most information is now communicated, generated, or stored electronically.[2] As Chief United States Magistrate Judge Grimm of the United States District Court for the District of Maryland acknowledged in *Lorraine v. Markel American Insurance Company*, "[b]ecause it can be expected that electronic evidence will constitute much, if not most, of the evidence used in future motions practice or at trial, counsel should know how to get it right on the first try."[3] This Article is intended to be an overview of "how to get it right on the first try," at least in federal court.[4] The Article is roughly organized according to the Federal Rules of Evidence, with examples of how those rules have been applied to electronic evidence.

[2] It is important to remember that there is nothing "magical" about the admission of electronic evidence. The prevalence of electronic evidence has required no substantial changes to the Federal Rules of Evidence.[5] In analyzing the admissibility of such evidence, it is often best to treat it as originating from the most similar, non-electronic source as thoughtful application of traditional evidentiary principles will nearly always lead to the correct result.[6] Thus, while electronic evidence may present some unique challenges to admissibility and complicate matters of establishing authenticity and foundation, it does not require the proponent to discard his knowledge of traditional evidentiary principles or learn anything truly new.

---

[2] *See Electronic Discovery in Litigation*, INFOLOGY, 1, http://www.infology.net/downloads/The%20Strategic%20Value%20of%20Electronic%20Discovery.pdf (last visited Jan. 10, 2011).

[3] *Lorraine*, 241 F.R.D. at 585.

[4] *Id.*

[5] *See* Jonathan L. Moore, *Moore on Upgrading the Federal Rules of Evidence to Accommodate ESI*, LEGAL INFORMATICS BLOG (June 11, 2010, 9:04 PM), http://legalinformatics.wordpress.com/2010/06/11/moore-on-upgrading-the-federal-rules-of-evidence-to-accommodate-esi/.

[6] *See* Sarah Van Deusen Phillips, *The Documentalist, Legal Considerations for Electronic Evidence, Part 2: Relevance and Authenticity*, WORD PRESS (Apr. 26, 2010), http://crlgrn.wordpress.com/2010/04/.

II. TYPES OF ELECTRONIC EVIDENCE AND THE ANALYTICAL FRAMEWORK FOR ADMISSION

[3] Electronically stored information that is admitted as evidence at a trial or hearing is electronic evidence.[7] It may include: electronic communications, such as e-mails, text messages, and chat room communications; digital photographs; website content, including social media postings; computer-generated data; and computer-stored records.[8]

[4] The seminal decision addressing the admissibility of electronic evidence is Judge Grimm's 51-page opinion in *Lorraine v. Markel American Insurance Company*, which reads as a comprehensive guide to the admission of electronic evidence.[9] In *Lorraine*, Judge Grimm describes a decision model for addressing the admission of electronic evidence, which, unsurprisingly, is nearly identical to the one many proponents apply to the admission of more traditional forms of evidence.[10]

[5] The *Lorraine* model suggests that the proponent of electronic evidence focus first on relevance, asking whether the electronic evidence has any tendency to make some fact that is of consequence to the litigation more or less probable than it would be otherwise.[11] Second, the proponent should address authenticity, asking if he can present evidence demonstrating that the electronic evidence is what it purports to be.[12] Third, the proponent must address any hearsay concerns associated with

[7] *See* Christine Sgarlata Chung & David J. Byer, *The Electronic Paper Trail: Evidentiary Obstacles to Discovery and Admission of Electronic Evidence*, 4 B.U. J. SCI. & TECH. L. 5, 9 (1998), *available at* https://www.bu.edu/law/central/jd/organizations/journals/scitech/volume4/4jstl05.pdf.

[8] *See* Michael D. Gifford, *Admitting Electronic Evidence in Federal Court: I've Got All This Evidence Data – Now What Do I Do With It?,* AM. B. ASS'N, 2 (2008), http://www.abanet.org/labor/basics/elist/papers/lied.pdf.

[9] *See generally Lorraine*, 241 F.R.D. 534.

[10] *Compare Lorraine*, 241 F.R.D. at 537-38, *with* Gifford, *supra* note 8, at 4.

[11] *See Lorraine*, 241 F.R.D. at 540 (citing FED. R. EVID. 401).

[12] *See id*. at 541-42.

the electronic evidence, asking if it is a statement by the declarant, other than one made by the declarant while testifying at the trial or hearing, offered for the truth of the matter asserted, and, if the electronic information is hearsay, whether an exclusion or exception to the hearsay rule applies.[13] Fourth, the proponent must address the application of the original documents rule.[14] Fifth, and finally, the proponent should consider "whether the probative value of the [electronic] evidence is substantially outweighed by the danger of unfair prejudice[,]" confusion, or waste of time.[15] Careful consideration of these traditional evidentiary principles will permit a proponent to successfully admit electronic evidence.

III. RELEVANCE CONSIDERATIONS

A. Logical Relevance

[6] Under the Federal Rules of Evidence, relevant evidence is generally admissible, and irrelevant evidence is not.[16] "Relevant evidence" is defined as evidence that has "*any* tendency to make the existence of *any* fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence."[17] Rules 401 and 402 of the Federal Rules of Evidence address this fundamental question of "logical relevance."[18]

---

[13] *See id*. at 562-63.

[14] *See id*. at 576.

[15] *See id*. at 583. On this last consideration, we will depart from Judge Grimm's model and instead address logical relevance (the first consideration in the *Lorraine* model) together with pragmatic relevance (the fifth and final consideration in the *Lorraine* model).

[16] FED. R. EVID. 402 ("All relevant evidence is admissible, except as otherwise provided by the Constitution of the United States, by Act of Congress, by [the Federal Rules of Evidence], or by other rules prescribed by the Supreme Court pursuant to statutory authority.").

[17] FED. R. EVID. 401 (emphasis added). This question is "different from whether evidence is sufficient to prove a point." *Lorraine*, 241 F.R.D. at 541 (emphasis omitted).

[18] *See* FED. R. EVID. 401; FED. R. EVID. 402.

[7] As one might expect, demonstrating that evidence has *any* tendency to prove or disprove *any* fact of consequence to adjudication of the action is not particularly difficult.[19] The Federal Rules' logical relevance test is quite yielding, particularly in light of the fact that a court's determination of logical relevance is reviewed under an abuse of discretion standard.[20] This test is applied to electronic evidence in the same way that it is applied to more traditional forms of evidence.[21] To those accustomed to applying the Federal Rules' logical relevance test to more traditional forms of evidence, the test's application to electronic evidence is fairly intuitive; it seems that, even under the view that electronic evidence is fundamentally strange or "magical," logical relevance is logical relevance.

B. Pragmatic Relevance

[8] Even logically relevant evidence may be held inadmissible "if its probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the jury, or by considerations of undue delay, waste of time, or needless presentation of cumulative evidence."[22] Under Rule 403 of the Federal Rules of Evidence, this test of "pragmatic relevance" focuses only on *unfair*

[19] *See Lorraine*, 241 F.R.D. at 541 ("Establishing that ESI has some relevance generally is not hard for counsel.").

[20] *See* United States v. Becton, 601 F.3d 588, 594 (D.C. Cir. 2010) (stating that determinations of the district courts concerning relevancy are reviewed for an abuse of discretion); United States v. Alvarez, 358 F.3d 1194, 1205 (9th Cir. 2004) (acknowledging the wide discretion afforded to trial judges in determining whether evidence is relevant and noting that a reviewing court will only consider "whether the decision was based on relevant factors and whether there was 'a clear error of judgment.'") (quoting United States v. Soulard, 730 F.2d 1292, 1296 (9th Cir. 1984).

[21] *Compare* Dickens v. State, 927 A.2d 32, 38 (Md. Ct. Spec. App. 2007) (holding that threatening text messages from a husband to his wife in the months preceding her murder were relevant to show that the husband's decision to murder his wife was deliberate and premeditated), *with* State v. Corwin, 295 S.W.3d 572, 579 (Mo. Ct. App. 2009) (holding that a rape victim's Facebook postings, which showed her dancing and drinking with men other than the accused rapist, were not relevant).

[22] FED. R. EVID. 403.

prejudice, since all evidence is prejudicial.[23] "'Unfair prejudice' . . . means an *undue* tendency to suggest decision on an improper basis, commonly, though not necessarily an emotional one."[24]

[9] Like logical relevance, the Federal Rules' test for pragmatic relevance is applied to electronic evidence in the same way it is applied to more traditional forms of evidence.[25] A court is most likely to invoke Rule 403 to exclude otherwise relevant electronic evidence where such evidence: (1) "contain[s] offensive or highly derogatory language that may provoke an emotional response;"[26] (2) consists of computer animations or simulations where "there is a substantial risk that the jury may mistake them for the actual events [at issue] in the litigation;"[27] (3) consists "of summaries of voluminous electronic writings, recordings or

[23] Indeed, the purpose of evidence is to prejudice the opposing party. United States v. Clark, 577 F.3d 273, 288 (5th Cir. 2009) (noting that, for purposes of analyzing evidence under Rule 403, "it is not enough to simply show that the evidence is prejudicial as virtually all evidence is prejudicial or it is not material") (quoting United States v. Rocha 916 F.2d 219, 239 (5th Cir. 1990)) (internal quotation marks omitted); Dollar v. Long Mfg., N.C., Inc., 561 F.2d 613, 618 (5th Cir. 1977) ("Of course, 'unfair prejudice' as used in Rule 403 is not to be equated with testimony simply adverse to the opposing party. Virtually all evidence is prejudicial or it isn't material. The prejudice must be 'unfair.'").

[24] FED. R. EVID. 403 advisory committee's note.

[25] *See, e.g.*, Monotype Corp. v. Int'l Typeface Corp., 43 F.3d 443, 449-50 (9th Cir. 1994) (affirming a trial court's decision to exclude e-mails that would have been overly prejudicial to the opposing party and would have confused the jury).

[26] Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 584 (D. Md. 2007) (citation omitted) (discussing electronic evidence); *see also Monotype*, 43 F.3d at 450 (holding that a district court did not err in excluding e-mails under Rule 403 because they were derogatory in nature and lacked probative value).

[27] *Lorraine*, 241 F.R.D. at 584 (citation omitted) (discussing electronic evidence); *see also* State v. Farner, 66 S.W.3d 188, 210 (Tenn. 2002) (excluding an animation under Tennessee's counterpart to Rule 403 because the animation was based upon inaccurate and incomplete information and depicted the accident a total of fifteen times, which the court suggested was unduly cumulative).

photographs under Rule 1006;"[28] or (4) is potentially unreliable or inaccurate.[29]

IV. AUTHENTICATION

A. Requirement of Authentication of Electronic Evidence

[10] Before being admitted, evidence must be authenticated – that is, the proponent of the evidence must make a showing sufficient to support a finding that the evidence is what it purports to be.[30] A "[c]ourt 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."[31]

[11] As Judge Grimm noted in *Lorraine*:

> [C]ounsel often fail to meet even this minimal showing when attempting to introduce ESI, which underscores the need to pay careful attention to this requirement. Indeed, the inability to get evidence admitted because of a failure to authenticate it almost always is a self-inflicted injury which can be avoided by thoughtful advance preparation.[32]

Due to the common perception that electronic records may be readily altered to appear to be something they are not,[33] "[a]uthenticity is often the

---

[28] *Lorraine*, 241 F.R.D. at 584 (citation omitted) (discussing electronic evidence).

[29] *See id.* (citation omitted) (discussing electronic evidence); *Farner*, 66 S.W.3d at 210 (excluding an animation of a car accident where the depiction was inconsistent with testimony regarding the speed of the vehicle and thus likely to be inaccurate).

[30] *See* FED. R. EVID. 901.

[31] *Lorraine*, 241 F.R.D. at 542 (quoting United States v. Safavian, 435 F. Supp. 2d 36, 38 (D.D.C. 2006)) (internal quotation marks omitted).

[32] *Id.* at 542.

[33] *See* Jerold S. Solovy & Robert L. Byman, *Don't Let Your E-Evidence Get Trashed*, LAW TECHNOLOGY NEWS (June 11, 2007), http://www.law.com/jsp/lawtechnologynews/

central battleground for determining admissibility of electronic evidence."[34]

[12] The proponent of electronic evidence often has to swim against the tide of a judiciary that is highly skeptical of such evidence.[35] Perhaps nowhere is such skepticism better articulated than in a decade-old decision from the United States District Court for the Southern District of Texas addressing the admissibility of information discovered on the Internet:

> While some look to the Internet as an innovative vehicle for communication, the Court continues to warily and wearily view it largely as one large catalyst for rumor, innuendo, and misinformation. So as to not mince words, the Court reiterates that this so-called Web provides no way of verifying the authenticity of the alleged contentions that Plaintiff wishes to rely upon in his Response to Defendant's Motion. There is no way Plaintiff can overcome the presumption that the information he discovered on the Internet is inherently untrustworthy. 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

PubArticleLTN.jsp?id=1181293533711 ("[A]ltering an e-mail takes nothing more than an impure heart and a keystroke."); Gifford, *supra* note 8, at 3 ("In the era when paper statements were dropped into a manila file until needed again, alteration or tampering was relatively easy to detect. . . . [W]ith paperless data greater attention must be given to the foundation necessary to establish the security of stored data.").

[34] Keiko L. Sugisaka, *Admissibility of E-Evidence in Minnesota: New Problems or Evidence as Usual?* 35 WM. MITCHELL L. REV. 1453, 1459 (2009).

[35] *See* Steven Goode, *The Admissibility of Electronic Evidence*, 29 REV. LITIG. 1, 2 (2009).

> for almost nothing, even under the most liberal interpretation of the hearsay exception rules . . . .[36]

[13] The Southern District of Texas's early distrust of electronic evidence has been shared, and discussed with equal force, by Federal Courts across the country.[37] Though this distrust is often applied to evidence obtained from the Internet, it is equally apparent where courts address the admissibility of e-mail and other electronic evidence.[38]

[14] However, some courts seem less willing to dismiss electronic evidence based on the mere fact that such evidence is susceptible to alteration.[39] Indeed, some courts will admit, for example, e-mails, after a threshold showing of authenticity and then leave the determination of whether thee-mails were altered for the jury.[40]

B. Authenticating Evidence by Extrinsic Evidence

[15] Rule 901(b) of the Federal Rules of Evidence sets forth a non-exclusive list identifying ten ways extrinsic evidence may authenticate

---

[36] St. Clair v. Johnny's Oyster & Shrimp, Inc., 76 F. Supp. 2d 773, 774-75 (S.D. Tex. 1999) (holding that "voodoo information taken from the Internet" was insufficient to withstand a motion to dismiss).

[37] *See, e.g.*, United States v. Jackson, 208 F.3d 633, 637 (7th Cir. 2000) (expressing skepticism over the admissibility of Internet web postings as a business record, particularly in light of the fact that the proponent presented no evidence that the ISP monitored the contents of the website); *see also* Wady v. Provident Life & Accident Ins. Co., 216 F. Supp. 2d 1060, 1064 (C.D. Cal. 2002) (quoting the *St. Clair* court and acknowledging that information retrieved from the Internet is inherently unreliable and easily distorted).

[38] *See* Leah Voigt Romano, *Developments in the Law: Electronic Discovery; VI: Electronic Evidence and the Federal Rules*, 38 LOY. L.A. L. REV. 1745, 1801 (2005).

[39] *See, e.g.*, United States v. Safavian, 435 F. Supp. 2d 36, 41 (D.D.C. 2006) ("The *possibility* of alteration does not and cannot be the basis for excluding e-mails as unidentified or unauthenticated as a matter of course, any more than it can be the rationale for excluding paper documents (and copies of those documents).").

[40] *See id.*

evidence for admission.[41] Though this list was prepared with more traditional forms of evidence in mind, most of the listed methods of authentication are easily applied to electronic evidence.[42]

1. Testimony of a Witness with Knowledge

[16] Under Rule 901(b)(1), a proponent may authenticate evidence through testimony that the evidence "is what it is claimed to be."[43] For non-electronic documents, the witness providing such testimony may be the person who drafted the document or who is responsible for maintaining the record.[44] For electronic evidence, the witness providing such testimony may be the person who created the electronic document or maintains the evidence in its electronic form.[45]

[17] Generally, a witness authenticating electronic evidence must "provide factual specificity about the process by which the electronically stored information is created, acquired, maintained, and preserved without alteration or change, or the process by which it is produced if the result of a system or process that does so."[46] Failure to provide such testimony may result in the subject electronic evidence being held to be inadmissible.[47]

---

[41] *See* FED. R. EVID. 901(b).

[42] Obviously, the methods described in FED. R. EVID. 901(b)(2) (Nonexpert Opinion on Handwriting), FED. R. EVID. 901(b)(5) (Voice Identification), and FED. R. EVID. 901(b)(6) (Telephone Conversations) do not typically apply to electronic evidence. The remaining methods do.

[43] FED. R. EVID. 901(b)(1).

[44] *See* United States v. Locke, 425 F.2d 313, 315 (5th Cir. 1970) (holding that records were properly authenticated through the testimony of the custodian of records).

[45] *See* United States v. Barlow, 568 F.3d 215, 220 (5th Cir. 2009) (holding that a chat log was properly authenticated by the testimony of a witness who participated in, and thus created, the chat).

[46] Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 545 (D. Md. 2007).

[47] *See, e.g.*, Am. Express Travel Related Servs. v. Vinhnee (*In re* Vee Vinhnee), 336 B.R. 437, 447 (B.A.P. 9th Cir. 2005) (holding that computer records were not properly

2. Comparison by Trier or Expert Witness

[18] Under Rule 901(b)(3) of the Federal Rules of Evidence, either an expert witness or the trier of fact may authenticate evidence by comparing it to properly authenticated specimens.[48] While this method was originally intended to authenticate handwriting or signatures,[49] it has recently been used to authenticate electronic communications as well.[50]

3. Distinctive Characteristics and the Like

[19] Under Rule 901(b)(4) of the Federal Rules of Evidence, a party may authenticate evidence using circumstantial evidence in conjunction with the "[a]ppearance, contents, substance, internal patterns, or other distinctive characteristics" of the evidence.[51] This is one of the most common methods of authenticating evidence.[52]

[20] Where a witness testifies that an e-mail or text message originated from the known e-mail address or screen name of another person, courts will often find that the e-mail or text message is an authentic communication from the purported sender.[53] This is particularly true

---

authenticated where the authenticating witness' testimony was vague, unpersuasive, and conclusory, and demonstrated a lack of knowledge regarding the relevant hardware and software).

[48] FED. R. EVID. 901(b)(3).

[49] *Lorraine*, 241 F.R.D. at 546 (citing FED. R. EVID. 901(b)(3) advisory committee's note).

[50] *See, e.g.*, United States v. Safavian, 435 F. Supp. 2d 36, 40 (D.D.C. 2006) (permitting the authentication of e-mails by comparison to other e-mails already authenticated under Federal Rule 901(b)(4)).

[51] FED. R. EVID. 901(b)(4).

[52] *Lorraine*, 241 F.R.D. at 546.

[53] *See, e.g.*, People v. Pierre, 838 N.Y.S.2d 546, 548-49 (N.Y. App. Div. 2007) (holding, under New York's adaptation of Rule 901(b)(3), that an instant message was properly authenticated as a communication from the defendant after "[t]he accomplice witness . . . testified to defendant's [instant messenger] screen name. . . . [and] that she sent an instant

where the content of the e-mail or text message reveals additional indicia of authenticity.[54]

[21] Authenticating other electronic evidence under Rule 901(b)(4) may involve the use of "hash values" or "metadata."[55] A hash value is "[a] unique numerical identifier that can be assigned to a file, a group of files, or a portion of a file, based on a standard mathematical algorithm applied to the characteristics of the data set."[56] An electronic document's hash value may constitute a distinguishing trait permitting authentication under Federal Rule 901(b)(4).[57]

[22] Metadata is "information describing the history, tracking, or management of an electronic document."[58] This "data about data" pertaining to the evidence in question may constitute a distinctive characteristic permitting authentication under Rule 901(b)(4).[59] However, this method of authentication is not entirely foolproof; network

message to that screen name, and received a reply, the content of which made no sense unless it was sent by defendant [and] there was no evidence that anyone had a motive, or opportunity, to impersonate defendant by using his screen name."); *see also* Simon v. State, 279 Ga. App. 844, 847 (Ga. Ct. App. 2006) (holding, under Georgia's version of Rule 901(b)(3), that e-mail correspondence between the defendant and his minor victim was properly authenticated "where . . . the witness testified that the [e-mails] accurately reflect[ed] the exchange between the parties, the witness communicated with the defendant at his known e-mail address," and the e-mail from the defendant referenced the defendant's nickname).

[54] *See Simon*, 279 Ga. App. at 847.

[55] *See Lorraine*, 241 F.R.D. at 546-47 (citations omitted) (internal quotation marks omitted).

[56] *Id.* (quoting FED. JUDICIAL CTR., MANAGING DISCOVERY OF ELECTRONIC INFORMATION: A POCKET GUIDE FOR JUDGES 24 (2007)).

[57] *Id.* at 547.

[58] *Id.* (quoting Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640, 646 (D. Kan. 2005)) (internal quotation marks omitted).

[59] *Id.* at 547-48 (quoting *Williams*, 230 F.R.D. at 646) (internal quotation marks omitted).

administrators and other users on the same network may access or alter electronic files stored on network computers.[60]

4. Public Records or Reports

[23] Under Rule 901(b)(7) of the Federal Rules of Evidence, a document may be authenticated by "[e]vidence that a writing authorized by law to be recorded or filed and in fact recorded or filed in a public office, or a purported public record, report, statement, or data compilation, in any form, is from the public office where items of this nature are kept."[61] "[T]he 'proponent of the evidence need only show that the office from which the records were taken is the legal custodian of the records;'" which may be accomplished through "'[t]he testimony of an officer who is authorized to attest to custodianship,'" or through "'[a] certificate of authenticity from the public office'" authorized to maintain the records.[62] Concerns about the accuracy of such evidence go to the weight of that evidence, not its admissibility.[63]

5. Ancient Documents

[24] Ancient documents may be authenticated under Rule 901(b)(8) of the Federal Rules of Evidence if the document "(A) is in such condition as to create no suspicion concerning its authenticity, (B) was in a place where it, if authentic, would likely be, and (C) has been in existence 20 years or

[60] *Id.* at 548 (citing JACK B. WEINSTEIN & MARGARET A. BERGER, WEINSTEIN'S FEDERAL EVIDENCE § 900.01 (Joseph M. McLaughlin ed., Matthew Bender 2d ed. 1997)).

[61] FED. R. EVID. 901(b)(7).

[62] *See Lorraine*, 241 F.R.D. at 548 (quoting JACK B. WEINSTEIN & MARGARET A. BERGER, WEINSTEIN'S FEDERAL EVIDENCE § 901.10 (Joseph M. McLaughlin ed., Matthew Bender 2d ed. 1997)).

[63] *See* United States v. Meienberg, 263 F.3d 1177, 1181 (10th Cir. 2001); United States v. Catabran, 836 F.2d 453, 458 (9th Cir. 1988) ("Any question as to the accuracy of the printouts, whether resulting from incorrect data entry or the operation of the computer program, as with inaccuracies in any other type of business records, would have affected only the weight of the printouts, not their admissibility.").

more at the time it is offered."[64] The Sixth Circuit has noted that despite the Rule's mandate "that the document be free of suspicion . . . suspicion goes not to the content of the document, but rather to whether the document is what it purports to be."[65] The theory behind this method is that, because of the age of the document, its author or creator is likely unavailable to testify regarding its authenticity; thus, courts must look to circumstantial evidence to guarantee the genuineness of the document.[66]

[25] This method of authentication is also significant in that it can qualify an exhibit under a corresponding hearsay exception, so that the exhibit may then be admitted for the truth of its contents.[67] Under Rule 803(16) of the Federal Rules of Evidence, "[s]tatements in a document in existence twenty years or more the authenticity of which is established" may be admitted as an exception to the hearsay rule.[68] Given the similar requirements of Rules 901(b)(8) and 803(16), courts frequently find that once a document is authenticated under 901(b)(8), it automatically qualifies under 803(16).[69] The rationale behind this exception is that, because the document was created long before the controversy arose, it is less likely that the document was fabricated or altered for purposes of the present litigation.[70]

---

[64] FED. R. EVID. 901(b)(8).

[65] United States v. Mandycz, 447 F.3d 951, 966 (6th Cir. 2006) (quoting United States v. Demjanjuk, 367 F.3d 623, 631 (6th Cir. 2004)) (internal quotation marks omitted).

[66] *See* MCCORMICK ON EVIDENCE § 225 (Kenneth S. Broud ed., 6th ed. 2006) (listing facts that support the genuineness of a document, such as "unsuspicious appearance, emergence from natural custody, prompt recording, and, in the case of a deed or will, possession taken under the instrument.").

[67] Fagiola v. Nat'l Gypsum Co. AC & S., 906 F.2d 53, 58 (2d Cir. 1990).

[68] FED. R. EVID. 803(16).

[69] *See Fagiola*, 906 F.2d at 58.

[70] *See* Columbia First Bank, FSB v. United States, 58 Fed. Cl. 333, 336 (Fed. Cl. 2003). The court noted the advisory committee's observation that "age affords assurance that the writing antedates the present controversy." *Id.* (quoting FED. R. EVID. 803(16) advisory committee's note).

[26] While 901(b)(8) has not been widely used to authenticate electronic evidence, the advisory committee notes make clear that the Rule applies to electronically-stored data.[71] The committee explains that "[t]his expansion is necessary in view of the widespread use of methods of storing data in forms other than conventional written records."[72]

[27] This inclusion of electronically stored data may become more significant in the coming years, as the twenty-year mark begins to reach back to a period when electronic data was becoming more pervasive. However, it is uncertain how courts will treat 'ancient electronic' evidence given the requirement under 901(b)(8) that the evidence be in a condition that creates "no suspicion concerning its authenticity."[73]

6. Process or System

[28] Under Rule 901(b)(9) of the Federal Rules of Evidence, a document may be authenticated by "[e]vidence describing a process or system used to produce a result and showing that the process or system produces an accurate result."[74] This method is often used to authenticate evidence generated by, or stored on, a computer.[75]

[29] One court has articulated an 11-step process for authenticating computer-generated or stored records.[76] The court found that to authenticate such records, a proponent must establish that:

> (1) The business uses a computer.
> (2) The computer is reliable.

[71] FED. R. EVID. 901(b)(8) advisory committee's note.

[72] *Id.*

[73] *See generally* FED. R. EVID. 901(b)(8).

[74] FED. R. EVID. 901(b)(9).

[75] *See* FED. R. EVID. 901(b)(9) advisory committee's note.

[76] *See In re* Vee Vinhnee, 336 B.R. 437, 446 (B.A.P. 9th Cir. 2005).

> (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.
> (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.[77]

C. Self-Authenticating Documents

[30] The Federal Rules of Evidence also identify a dozen categories of evidence that may be authenticated without extrinsic evidence.[78] Each of these categories provides an efficient method for authenticating evidence, but courts have identified three that are particularly relevant in the electronic evidence context.[79]

1. Official Publications

[31] "Books, pamphlets, or other publications purporting to be issued by public authority" are self-authenticating under Rule 902(5) of the Federal Rules of Evidence.[80] Thus, an e-mail, newsletter, or website

[77] *Id.*

[78] *See* FED. R. EVID. 902.

[79] *See* Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 551 (D. Md. 2007).

[80] FED. R. EVID. 902(5).

published by a public authority can be self-authenticating but the proponent of such evidence might also need to demonstrate that such a document satisfies the public record hearsay exception set forth in Rule 803(8).[81]

2. Trade Inscriptions and the Like

[32] Evidence may be authenticated by "[i]nscriptions, signs, tags, or labels purporting to have been affixed in the course of business and indicating ownership, control, or origin."[82] Many business communications, such as e-mails, "'contain information showing the origin of the transmission and identifying the employer-company'" meaning "'[t]he identification marker alone may be sufficient to authenticate an e-mail under Rule 902(7).'"[83]

3. Certified Domestic Records of Regularly Conducted Activity

[33] Rule 902(11) of the Federal Rules of Evidence provides a method of self-authentication for records of regularly conducted activity.[84] This method mirrors the requirements of the business records exception to the hearsay rule; therefore, courts often analyze it in conjunction with that exception.[85] The Rule provides that extrinsic evidence of authenticity is not required for admissibility if the evidence is an "original or a duplicate

[81] *See Lorraine*, 241 F.R.D. at 551.

[82] FED. R. EVID. 902(7).

[83] *Lorraine*, 241 F.R.D. at 551-52 (citing JACK B. WEINSTEIN & MARGARET A. BERGER, WEINSTEIN'S FEDERAL EVIDENCE § 900.07(3)(c) (Joseph M. McLaughlin ed., Matthew Bender 2d ed. 1997)).

[84] *See* FED. R. EVID. 902(11).

[85] *See* DirecTV, Inc. v. Murray, 307 F. Supp. 2d 764, 772 (D.S.C. 2004) (analyzing the admissibility of e-mails under Rules 902(11) and 803(6) and noting that the analyses under both rules "are necessarily intertwined"); *see also* Rambus, Inc. v. Infineon Tech. AG, 348 F. Supp. 2d 698, 701 (E.D. Va. 2004) ("[T]he most appropriate way to view Rule 902(11) is as the functional equivalent of testimony offered to authenticate a business record tendered under Rule 803(6).").

of a domestic record of regularly conducted activity that would be admissible under Rule 803(6)."[86] However, to be self-authenticating the record must be:

> accompanied by a written declaration of its custodian or other qualified person . . . certifying that the record (A) was made at or near the time of the occurrence of the matters set forth by . . . a person with knowledge of those matters; (B) was kept in the course of the regularly conducted activity; and (C) was made . . . as a regular practice.[87]

[34] To properly authenticate, the proponent must show that the custodian of the records is "not only . . . familiar with the maintenance of the records, but also with how they are created."[88] Furthermore, the record must be made pursuant to established procedures and must be kept as a regular practice by the business entity, much like the business records exception.[89]

[35] This method of self-authentication is particularly important to electronic evidence in light of the fact that most business records today are stored in electronic format.[90] Thus, not only will a proper declaration self-authenticate electronic evidence, but the content of the evidence may be

[86] FED. R. EVID. 902(11).

[87] *Id.*

[88] *Rambus*, 348 F. Supp. 2d at 703 (noting that the bar for qualifying a witness as the custodian of records is low).

[89] *See id.* at 704-05 ("It is not enough that a particular employee regularly makes and keeps the records as his or her own regular practice because it must be the regular practice of the business . . . to make and keep the record at issue.").

[90] *See, e.g.*, *DirecTV*, 307 F. Supp. 2d at 772 (finding that an electronic dealer's e-mails were properly self-authenticated under Rule 902(11) in light of the custodian of records' testimony that the e-mail records were kept in the normal course of business, were made at or near the time the events occurred, and that it was the custom of the business to regularly record orders by e-mail and keep those e-mails as records of such orders).

admitted for its truth because it qualifies under the business records exception to the hearsay rule.[91]

D. Authentication of Certain Types of Electronic Evidence

1. E-mails and Text Messages

[36] In modern litigation, it is rare when a case does not involve some communication by e-mail or text message.[92] Such a communication is easily authenticated if the proponent of the communication can secure the admission of the author or sender of the communication that he drafted or sent the communication.[93] Additionally, a recipient, [94] or non-recipient with knowledge that the communication was sent, [95] may authenticate an e-mail or text message. Also, a witness with knowledge of how the responsible Internet service providers or wireless telephone carriers sent

[91] *See id.*

[92] *See* Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 554 (D. Md. 2007) ("There is no form of ESI more ubiquitous than e-mail.").

[93] *See* Talada v. City of Martinez, 656 F. Supp. 2d 1147, 1158 (N.D. Cal. 2009) (finding that an e-mail had been properly authenticated by testimony from the sender, and that separate e-mails were also properly authenticated by a declaration from the recipient of the e-mails that they were accurate and true copies of the e-mails).

[94] In *People v. Brown*, a California court held that text messages from a witness' cellular telephone were properly authenticated in a criminal matter where the witness testified that the messages came from the defendant and were "signed" with the defendant's name. People v. Brown, No. A122791, 2009 WL 1878704, at *3 (Cal. Ct. App. June 30, 2009). The prosecution introduced the messages into evidence by introducing the cellular telephone as an exhibit and having the witness identify the telephone and read the messages from the telephone aloud. *Id.* at *3.

[95] In *Dickens v. State*, a Maryland court held that the testimony of a victim's mother regarding text messages sent to the victim from the victim's husband before she was murdered was sufficient to authenticate those messages under Maryland Rule 5-901(b), Maryland's equivalent to Federal Rule of Evidence 901(b). Dickens v. State, 927 A.2d 32, 36-37 (Md. Ct. Spec. App. 2007). The court also considered circumstantial evidence to corroborate the mother's testimony including the fact that the telephone was found near a home the defendant had visited shortly after the shooting and told residents that "he had done something to his girlfriend." *Id.* at 36 (internal quotation marks omitted).

and received an e-mail or text message, and how such messages are stored and retrieved, may authenticate such messages.[96] The threshold determination for authentication will often vary with the piece of evidence and the court the evidence is before; however, the Southern District of New York characterized this threshold requirement as "relatively low," and held that any remaining issues concerning authenticity should go to the weight of the evidence rather than its admissibility.[97]

[37] Comparing an e-mail or a text message with other e-mails or text messages already authenticated may serve to authenticate the e-mail or text message at issue.[98] This method is particularly useful in cases where the sender/recipient's e-mail address does not bear any indicia of identification.[99] For example, the e-mail address "joe.smith@doj.gov," indicates that the address most likely belongs to Joe Smith, who presumably works for the Department of Justice.[100] "MerrittDC@aol.com" does not contain the same obvious identifiers, but comparing an e-mail from "MerrittDC@aol.com" with a previous e-mail from the same address, which has already been independently and properly authenticated, will authenticate the latter e-mail, even though it does not contain the same information which authenticated the earlier e-mail.[101]

2. Chat Room Communications

[38] A proponent may authenticate chat room communications by demonstrating that: (1) the person alleged to be the sender had access to

[96] *See* State v. Taylor, 632 S.E.2d 218, 230 (N.C. Ct. App. 2006).

[97] *See* Bazak Int'l Corp. v. Tarrant Apparel Grp., 378 F. Supp. 2d 377, 391-92 (S.D.N.Y. 2005).

[98] *See* United States v. Safavian, 435 F. Supp. 2d 36, 40 (D.D.C. 2006).

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

[100] *See id.*

[101] *See id.* at 40-41 (comparing an e-mail from "MerrittDC@aol.com" with a previously authenticated e-mail and finding the subsequent e-mail properly authenticated).

the computer from which the chats were conducted; (2) the chats in question were conducted at the same time as chats the defendant admitted to conducting; (3) the chats were conducted using a screen name created by the defendant; and (4) the content of the chats was similar to chats the defendant admitted to conducting.[102] Additionally, a proponent seeking to admit transcripts of chat room dialogue must ensure that the transcripts accurately reflect the conversation.[103] Cutting and pasting portions of the chat in a way that alters the context of the communication or that fails to preserve the temporal integrity of the chat (for example, a chat room post time-stamped at 1:00 p.m., followed by a chat room post time-stamped at 12:45 p.m.), may raise suspicion and prevent such transcripts from being properly authenticated.[104]

[39] An even greater challenge in admitting chat room transcripts is proving the identity of the participants.[105] With no face-to-face interaction and screen names that often give no indication of the user's real name, identifying the parties to the conversation is often a difficult hurdle to overcome.[106] To authenticate chat room transcripts, parties often use circumstantial evidence, such as a witness testifying that she had previously communicated with a certain screen name, that the responses from the screen name would have not made sense were they not from a particular person, and that no one else had a motive to impersonate that particular person.[107]

---

[102] *See* United States v. Zahursky, 580 F.3d 515, 524 (7th Cir. 2009).

[103] *See* United States v. Jackson, 488 F. Supp. 2d 866, 871 (D. Neb. 2007).

[104] *See id.* at 870-71 (finding that a Microsoft Word document containing cut-and-paste portions of an online chat was not properly authenticated because there were several instances of missing information, and some of the timing sequences were not in order).

[105] *See* Reno v. Am. Civil Liberties Union, 521 U.S. 844, 855 (1997) (discussing the difficulty of determining the identity of chat room participants).

[106] *See id.* at 890.

[107] *See* People v. Pierre, 838 N.Y.S.2d 546, 548-49 (N.Y App. Div. 2007) (finding that a chat room conversation was properly authenticated through circumstantial evidence even though the witness did not save the conversation and no printable version was available to the court); *In re* F.P., 878 A.2d 91, 95-96 (Pa. Super. Ct. 2005) (considering circumstantial evidence in admitting Instant Message chats).

3. Websites

[40] Website authentication raises three distinct issues: "(1) What was actually on the website? (2) Does the exhibit or testimony accurately reflect it? (3) If so, is it attributable to the owner of the site?"[108] To address these questions, a proponent must often provide a witness with personal knowledge of the website who can testify "'that the printout accurately reflects the content of the page and the image of the page on the computer at which the printout was made.'"[109]

[41] A proponent also may authenticate a website under Rule 901(b)(4) when the printout contains distinctive characteristics that, combined with circumstantial evidence, show that the printout is what it purports to be.[110] While a highly fact-specific inquiry, the level of scrutiny applied to website printouts will often vary according to the particular website.[111] For example, current printouts from reputable business sites, such as bankofamerica.com or verizon.com, are less likely to be subject to the same scrutiny as the online-encyclopedia Wikipedia, a blog, or another website where content is easily manipulated.[112] Additional concerns may

[108] Goode, *supra* note 35 at 11.

[109] *See* Toytrackerz LLC v. Koehler, No. 08-2297-GLR, 2009 WL 2591329, at *6 (D. Kan. Aug. 21, 2009) (quoting Nightlight Sys., Inc. v. Nitelites Franchise Sys., Inc., 2007 WL 4563875, at *6 (N.D. Ga. May 11, 2007)) (finding that the proponent of various website printouts failed to authenticate them because there was no indication as to who retrieved the printout, when and how the pages were printed, or on what basis the printouts accurately reflected the website on a particular date); Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1154 (C.D. Cal. 2002) (holding that a plaintiff properly authenticated printouts from a website where he submitted declarations sufficient to show that the pictures were what they purported to be).

[110] *See* Goode, s*upra* note 35, at 29.

[111] *See id.*

[112] *See id.*

be raised regarding an author's identity, especially in the context of defamatory postings on blogs or other websites.[113]

[42] Even more dubious is content obtained from older versions of a website. If such content has not been archived by the operator of the website, the proponent may be forced to seek the admission of the website content as archived by the Internet Archive Company at http://www.archive.org.[114] Authentication of such evidence may be accomplished through testimony or affidavit that the Internet Archive Company retrieved copies of the website as it appeared on the dates in question from its electronic archives.[115] Though "the Internet Archive does not fit neatly into any of the non-exhaustive examples listed in Rule 901" and "is a relatively new source for archiving websites," at least one district court has held that, absent evidence that the Internet Archive is biased or unreliable, or evidence contesting the veracity of the proposed exhibit, such testimony or affidavit is sufficient to satisfy the threshold requirement for admissibility – that is, a prima facie showing of genuineness.[116] By contrast, printouts from official government websites have been held to be self-authenticating under Rule 902(5) of the Federal Rules of Evidence, which provides that books, pamphlets, or other publications purporting to be issued by public authority are self-authenticating.[117]

[113] *See* Wendler & Ezra, P.C. v. Am. Int'l Grp., Inc., 521 F.3d 790, 791-92 (7th Cir. 2008) (holding that a plaintiff failed to link a defamatory post on a third party website to the defendant).

[114] *See* Telewizja Polska USA, Inc. v. Echostar Satellite Corp., No. 02 C 3293, 2004 WL 2367740, at *6 (N.D. Ill. Oct. 15, 2004).

[115] *See id.*

[116] *Id.*

[117] Paralyzed Veterans of Am. v. McPherson, No. C 06-4670 SBA, 2008 WL 4183981, at *7 (N.D. Cal. Sept. 9, 2008) (holding that printouts from the California Secretary of State website were self-authenticating under Rule 902(5)).

4. Computer-Generated Records

[43] The authenticity of computer-generated records is generally shown through the testimony of a witness with knowledge of how the records are recorded, stored and maintained.[118] However, given the wide disparity among courts concerning the admission of computer-generated records, the difficulty in preparing such evidence is determining the level of scrutiny the court will apply to the evidence when assessing its authenticity.[119]

[44] Courts on one end of the spectrum will allow authentication of computer-generated evidence by a person "who has knowledge of the particular record system."[120] This camp does not require computer programmers or experts to testify as to the accuracy and intricacies of the particular computer program.[121] Rather, the proponent is only held to the standard of showing that the records were sufficiently precise and that the company relied upon such records in its business practices.[122]

[45] On the other end of the spectrum, courts require a much more rigorous process in order to make a sufficient showing that a computer-

[118] *See* U-Haul Int'l Inc. v. Lumbermens Mut. Cas. Co., 576 F.3d 1040, 1045 (9th Cir. 2009) (finding that computer-generated records were properly authenticated through testimony "regarding the process of inputting data into the computer and the process of querying the computer to compile the information"); *see also* Hardison v. Balboa Ins. Co., 4 F. App'x 663, 669 (10th Cir. 2001) (permitting the authentication of computer-generated records through affidavits and verified answers to interrogatories).

[119] *See* Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 559 (D. Md. 2007) (advising lawyers "to plan to authenticate the record by the most rigorous standard that may be applied").

[120] *See U-Haul*, 576 F.3d at 1045 (quoting United States v. Miller, 771 F.2d 1219, 1237 (9th Cir. 1985)) (internal quotation marks omitted).

[121] *See id.*

[122] *See id.*

generated record is what it purports to be.[123] These courts require specific testimony regarding not only the procedures for storing and maintaining the data, but also concerning the functionality of the particular hardware and software used to store, compute, and maintain the data.[124] Because the person inputting data is rarely familiar with the inner-workings of computer hardware or software, the proponent of such evidence will often need to retain an expert to explain these processes to the satisfaction of the court.[125]

V. HEARSAY

A. Hearsay

[46] "'Hearsay' is a statement, other than one made by the declarant while testifying at the trial or hearing, offered to prove the truth of the matter asserted."[126] In this context, "[a] 'statement' is (1) an oral or written assertion or (2) nonverbal conduct . . . intended . . . as an assertion,"[127] and "[a] 'declarant' is a *person* who makes a statement."[128]

1. Statement

[47] Evidence that does not meet the definition of a "statement" under the Federal Rules of Evidence is not hearsay.[129] "[F]or verbal or

[123] *See In re* Vee Vinhnee, 336 B.R. 437, 446 (B.A.P. 9th Cir. 2005) (listing "built-in safeguards to ensure accuracy and identify errors" as part of an eleven-step authentication process).

[124] *See id.* at 447 (noting that the witness' testimony concerning American Express' computer records was "vague, conclusory, and, in light of the assertion that '[t]here's no way that the computer changes numbers,' unpersuasive") (citation omitted).

[125] *See* Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 559 (D. Md. 2007).

[126] FED. R. EVID. 801(c).

[127] FED. R. EVID. 801(a).

[128] FED. R. EVID. 801(b) (emphasis added).

[129] *See* FED. R. EVID. 801(c).

nonverbal conduct to fall within the definition of the hearsay rule as defined under the Federal Rules of Evidence, it must be either an expressly assertive written or spoken utterance, or nonverbal conduct expressly intended to be an assertion – the federal rules appear to have excluded from the definition of hearsay 'implied assertions' . . . ."[130] An example of this concept is the following: A man stepping outside and opening his umbrella.[131] The man did not intend to assert that it is raining outside when he opened his umbrella, thus, his conduct was nonassertive.[132] Accordingly, a witness's testimony that the man stepped outside and opened his umbrella, offered to show that it was raining, is not hearsay.[133]

2. Declarant

[48] To be hearsay, the statement must be made by a person, the "declarant," not an animal or machine.[134] For example, when a dog trained to detect illegal substances finds drugs in the trunk of a car, hearsay is not an issue – the declarant is not a person.[135] But when a nun witnesses an accident and states what she saw, the dangers of faulty memory, perception, and ambiguity remain, even though the nun is less likely to lie about the events.[136] When viewed across the range of dogs to

[130] *Lorraine,* 241 F.R.D. at 563; *see* United States v. Safavian, 435 F. Supp. 2d 36, 44 (D.D.C. 2006) (explaining that an e-mail containing imperative statements is non-assertive verbal conduct and not hearsay).

[131] *See* Paul S. Milich, *Re-Examining Hearsay Under the Federal Rules: Some Method for the Madness*, 39 U. KAN. L. REV. 893, 903 (1991).

[132] *See id.*

[133] *See id.* ("Opening an umbrella normally is not intended to be an assertion about anything, and, thus, such nonverbal conduct does not fall within the federal definition of hearsay.").

[134] *See* FED. R. EVID. 801(c), *see also* John C. O'Brien, *The Hearsay Within Confrontation*, 29 ST. LOUIS U. PUB. L. REV. 501, 520 (2010).

[135] *See* O'Brien, *supra* note 134.

[136] PAUL R. RICE, ELECTRONIC EVIDENCE: LAW AND PRACTICE 199-200 n.12 (2005).

nuns, nothing to the left of dogs creates a hearsay problem.[137] Thus, machines, which are to the left of dogs, fall outside the scope of hearsay "because the hearsay problems of perception, memory, sincerity and ambiguity have either been addressed or eliminated."[138]

[49] In the context of electronic evidence, the concept of a declarant is often tested in the consideration of computer-generated evidence.[139] As the court stated in *Lorraine*:

> When an electronically generated record is entirely the product of the functioning of a computerized system or process, such as the "report" generated when a fax is sent showing the number to which the fax was sent and the time it was received, there is no "person" involved in the creation of the record, and no "assertion" being made. For that reason, the record is not a statement and cannot be hearsay.[140]

3. Offered to Prove the Truth of the Matter Asserted

[50] If a statement is not offered to prove the truth of the matter asserted, the statement is not hearsay.[141] Thus, verbal acts and legally operative facts, such as the fact that a contract was formed, are not hearsay

[137] *See id.*

[138] *Id*.

[139] *See generally* Adam Wolfson, "*Electronic Fingerprints": Doing Away with the Conception of Computer-Generated Records as Hearsay*, 104 MICH. L. REV. 151, 159 (2005).

[140] Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 564 (D. Md. 2007); *see* United States v. Khorozian, 333 F.3d 498, 506 (3d Cir. 2003) (explaining that a fax header was not a statement and thus not hearsay because it was created by a machine).

[141] *See* FED. R. EVID. 801(c) advisory committee's note ("If the significance of an offered statement lies solely in the fact that it was made, no issue is raised as to the truth of anything asserted, and the statement is not hearsay.").

because they are not offered for the truth of the matter asserted.[142] Obviously, one must consider the purpose of offering evidence in the hearsay analysis, because evidence may be admissible for one purpose but inadmissible for another.[143]

4. Inadmissibility

[51] Generally, hearsay is inadmissible.[144] "The hearsay rule excludes such evidence because it possesses testimonial dangers of perception, memory, sincerity, and ambiguity that cannot be tested through oath and cross-examination."[145]

B. Hearsay Exclusions

[52] By express exclusion under the Federal Rules of Evidence, certain prior statements by a witness and certain admissions by a party-opponent are not hearsay.[146] Courts often apply this latter exclusion, for admissions of a party-opponent, to electronic evidence.[147] "Given the near universal

[142] *See Lorraine*, 241 F.R.D. at 567 n.50 ("A verbal act is an utterance of an operative fact that gives rise to legal consequences. Verbal acts, also known as statements of legal consequence, are not hearsay, because the statement is admitted merely to show that it was actually made, not to prove the truth of what was asserted in it."); *see, e.g.*, Transportes Aereos Pegaso, S.A. v. Bell Helicopter Textron Inc., 623 F. Supp. 2d 518, 530 (D. Del. 2009) (holding that hearsay evidence of a declarant soliciting a bride was a verbal act and thus fell outside of the hearsay rule); Banks v. State, 608 A.2d 1249, 1254 (Md. Ct. Spec. App. 1992) (noting that examples of verbal acts include language in will bequests, offer and acceptance, and libel or slander).

[143] *See, e.g.*, United States v. Siddiqui, 235 F.3d 1318, 1323 (11th Cir. 2000) (holding that an e-mail between the defendant and a co-worker was not hearsay because it was not offered to prove the truth of the statements contained in the e-mail but instead to demonstrate that a relationship between the two existed).

[144] *See* FED. R. EVID. 802.

[145] RICE, *supra* note 136, at 262.

[146] *See* FED. R. EVID. 801(d).

[147] *See Lorraine*, 241 F.R.D. at 568; Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 454 F. Supp. 2d 966, 973 (C.D. Cal. 2006) (holding that e-mails sent by corporate employees were admissible as admissions by a party's agent under Rule 801(d)(2)).

use of electronic means of communication, it is not surprising that statements contained in electronically made or stored evidence often have been found to qualify as admissions by a party opponent if offered against that party."[148]

C. Hearsay Exceptions

[53] While the hearsay rule may operate to exclude a vast array of evidence, the numerous and expansive exceptions to the rule operate to include more than the rule excludes.[149] Among these exceptions are Rules 803 and 804 of the Federal Rules of Evidence, which list twenty-eight exceptions to the hearsay rule.[150] In addition, Rule 807 provides a residual exception for statements bearing "circumstantial guarantees of trustworthiness."[151] If a statement falls under one of these exceptions, the content of the proffered evidence is admissible for its truth.[152] The following hearsay exceptions are most commonly used when dealing with electronic evidence.

1. Present Sense Impression

[54] "A statement describing or explaining an event or condition made while the declarant was perceiving the event or condition, or immediately thereafter" is not excluded by the hearsay rule, regardless of whether the declarant is available to testify at the trial or hearing.[153] Contemporaneousness is the key to this exception; such statements are considered trustworthy because the declarant simultaneously perceives the

[148] *Lorraine*, 241 F.R.D. at 568 (citations omitted); *see also MGM Studios*, 454 F. Supp. 2d at 973.

[149] *See generally* FED. R. EVID. 803; FED. R. EVID. 804.

[150] *See generally* FED. R. EVID. 803; FED. R. EVID. 804.

[151] FED. R. EVID. 807.

[152] FED R. EVID. 801(c).

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

event and makes a statement concerning the event, thereby minimizing the dangers of poor memory or insincerity.[154]

[55] Statements made in an e-mail or a human-generated but computer-stored record may qualify as a present sense impression in the same way as a more traditional letter or hardcopy record.[155] Moreover, though they have no close analogue in the non-electronic world, social networking posts assemble the present sense impressions of millions upon millions of users.[156]

2. Excited Utterance

[56] "A statement relating to a startling event or condition made while the declarant was under the stress of excitement caused by the event or condition" also survives the hearsay rule, regardless of whether the declarant is available to testify at the trial or hearing.[157] The *Lorraine* court noted that "[t]he theory behind [this] exception is that perception of a startling or exciting event produces in the declarant an emotional state that reduces the likelihood that the description of the event while under this emotional state will be inaccurate or purposely misstated."[158] Therefore, e-mails, human-created but computer-stored records, and social

[154] *See* FED. R. EVID. 803 advisory committee's note.

[155] *See* United States v. Ferber, 966 F. Supp. 90, 99 (D. Mass. 1997) (holding that an e-mail from the defendant's co-worker describing a conversation with the defendant was admissible as a present sense impression because it was prepared shortly after the conversation). *But see* State v. Microsoft Corp., No. CIV A. 98-1233(CKK), 2002 WL 649951, at *2 (D.D.C. Apr. 12, 2002) (finding that an e-mail discussing events from days prior was not admissible under the present sense impression exception because the e-mail was not composed while the declarant was perceiving an event or immediately thereafter).

[156] *See* Bass v. Miss Porter's Sch., No. 3:08cv1807 (JBA), 2009 WL 3724968, at *1 (D. Conn. Oct. 27, 2009) ("Facebook usage depicts a snapshot of the user's relationships and state of mind at the time of the content's posting.").

[157] FED. R. EVID. 803(2).

[158] Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 569 (D. Md. 2007) (citing FED. R. EVID. 803(2)).

media postings can all constitute excited utterances so long as they are created under the "stress of excitement" caused by a startling event or condition.[159]

3. Then Existing State of Mind or Condition

[57] The Federal Rules of Evidence also exclude statements by declarants concerning their state of mind or condition from the hearsay exception.[160] Rule 803(3) provides for the admissibility of:

> [a] statement of the declarant's then existing state of mind, emotion, sensation, or physical condition (such as intent, plan, motive, design, mental feeling, pain, and bodily health), but not including a statement of memory or belief to prove the fact remembered or believed unless it relates to the execution, revocation, identification, or terms of declarant's will.[161]

[58] Like the present sense impression exclusion listed in Rule 803(1), contemporaneousness is key to this exception.[162] As the *Lorraine* court noted, this exception:

> has been used to prove a wide variety of matters, including the reason why the declarant would not deal with a supplier or dealer, motive, competency, ill-will, . . . lack of intent to defraud, willingness to engage in criminal conduct, the

[159] *See Ferber*, 966 F. Supp. at 99 (internal quotation marks omitted) ("An excited utterance must be made under the 'stress of excitement,' and any amount of time that passes between the exciting event and the statement will remove the declarant from the stress of the situation.").

[160] FED R. EVID. 803(3).

[161] *Id.* These statements are excluded from the hearsay rule regardless of whether the declarant is available to testify at the trial or hearing. *Id.*

[162] Fed. R. Evid. 803(3) advisory committee's note (explaining that Rule 803 is essentially the same as Rule 801).

> victim's state of mind in an extortion case, and confusion or secondary meaning in a trademark infringement case.[163]

The exception is particularly useful in admitting e-mails, which, due to the seeming informality of the medium, often contain remarkably candid expressions of the writer's state of mind.[164] Social networking websites are also littered with expressions of their users' states of mind.[165]

4. Business Records

[59] "[M]emorand[a], report[s], record[s], or data compilation[s] . . . made at or near the time [of an event] by, a person with knowledge" are excepted from the hearsay rule "if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business [to keep such records]."[166] If a custodian or qualified witness demonstrates these requirements through his testimony, the evidence may be admitted.[167] This business records exception is often analyzed in conjunction with Rule 902(11) of the Federal Rules of Evidence, which

[163] *Lorraine*, 241 F.R.D. at 570 (citation omitted).

[164] *See id.* at 554 ("Perhaps because of the spontaneity and informality of e-mail, people tend to reveal more of themselves, for better or worse, than in other more deliberative forms of written communication. For that reason, e-mail evidence often figures prominently in cases where state of mind, motive and intent must be proved. Indeed, it is not unusual to see a case consisting almost entirely of e-mail evidence.").

[165] *See* Susan W. Brenner, *Internet Law in the Courts*, 13 J. INTERNET L. 16, 18 (2009).

[166] FED. R. EVID. 803(6).

[167] *Id.*; *see also* Sea-Land Serv., Inc. v. Lozen Int'l, LLC, 285 F.3d 808, 819 (9th Cir. 2002) (affirming the trial court's admission of bills of lading under the business records exception after the custodian stated that the company kept the records in the ordinary course of business); United States v. Catabran, 836 F.2d 453, 457 (9th Cir. 1988) (holding that the trial court properly admitted computer printouts under the business records exception after the custodian provided sufficient foundation); United States v. Vela, 673 F.2d 86, 89-90 (5th Cir. 1982) (holding that telephone records were properly admitted as a business record because the custodian described how the records were prepared and maintained).

provides for the authentication of certified domestic records of regularly-conducted business activities without extrinsic evidence.[168]

[60] Business records are viewed as trustworthy, and therefore excepted from the hearsay rule, because they are kept by trained record keepers and regularly checked for accuracy.[169] However, the business records exception is not limited to records made and kept by a "business." Rather the records of government agencies,[170] private clubs,[171] and individual households[172] may all qualify under the exception.

[61] It has been noted that "[t]he business record exception is one of the hearsay exceptions most discussed by courts when ruling on the admissibility of electronic evidence."[173] E-mails[174] and computer-stored

[168] *See supra* Part IV.C.3 (discussing self-authentication under Rule 902(11)).

[169] *See* State v. Microsoft Corp., No. CIV A. 98-1233(CKK), 2002 WL 649951, at *2 (D.D.C. Apr. 12, 2002) (citation omitted).

[170] *See, e.g.*, United States v. Szehinskyj, 104 F. Supp. 2d 480, 491-92 (E.D. Pa. 2000) (admitting documents of the German government concerning the regulation of concentration camps under the business records exception because the records outlined the camps operations).

[171] *See, e.g.*, Keogh v. Comm'r of Internal Revenue, 713 F.2d 496, 500 (9th Cir. 1983) (holding that the private diary of country club employee was admissible under the business records exception and rejecting the argument that the exception applies solely to commercial businesses).

[172] *See, e.g.*, United States v. Ferber, 966 F. Supp. 90, 98-99 (stating that if it were common household practice to compose e-mails following significant telephone conversations, such e-mails would be admissible under the business records exception).

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

[174] *See* Pierre v. RBC Liberty Life Ins., No. 05-1042-C, 2007 WL 2071829, at *2 (M.D. La. July 13, 2007) (finding that e-mails fell within Rule 803(6) because they "were prepared by . . . employees during the ordinary course of business"); DirecTV, Inc. v. Murray, 307 F. Supp. 2d 764, 772-73 (D.S.C. 2004) (finding that sales records contained in e-mails were admissible under the business records exception when sales orders were regularly received via e-mail and the e-mails were retained as records of each order); Rambus, Inc. v. Infineon Techs. AG, 348 F. Supp. 2d 698, 706 (E.D. Va. 2004) (noting that e-mails can qualify as business records). *But see Microsoft*, 2002 WL 649951, at *2 (declining to admit e-mails under the business records exception because there was a

and computer-generated records[175] may qualify under the business records exception to the hearsay rule, provided that they meet the requirements set forth in Rule 803(6).[176]

5. Public Records

[62] Also exempt from the hearsay rule are:

> [r]ecords, reports, statements, or data compilations, in any form, of public offices or agencies, setting forth (A) the activities of the office or agency, or (B) matters observed pursuant to duty imposed by law as to which matters there was a duty to report, excluding, however, in criminal cases matters observed by police officers and other law enforcement personnel, or (C) in civil actions and proceedings and against the Government in criminal cases, factual findings resulting from an investigation made pursuant to authority granted by law, unless the sources of information or other circumstances indicate lack of trustworthiness.[177]

[63] Public records are viewed as trustworthy because public officials are expected to perform their duties appropriately, but are unlikely to remember the details of those activities independent of the record

"complete lack of information regarding the practice of composition and maintenance of [the] e-mails"); *Ferber*, 966 F. Supp. at 99 (declining to admit e-mails under the business records exception because the author of the e-mails "was under no business duty to make and maintain" such e-mails).

[175] *See* United States v. Cestnik, 36 F.3d 904, 909-10 (10th Cir. 1994) (holding that computer-generated money transfer records were admissible under the business records exception to the hearsay rule because the records were kept according to a standard procedure and in the normal course of business).

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

[177] FED. R. EVID. 803(8).

created.[178] Because public records are deemed to have a higher degree of accuracy than business records, the proponent of a public record typically is not required to provide foundational testimony to demonstrate a public record's admissibility, whereas, to qualify under the business records exception, the proponent must adduce testimony from the custodian of the records or an otherwise qualified witness.[179]

[64] Furthermore, "[p]ublic records and government documents are generally considered 'not to be subject to reasonable dispute.' This includes public records and government documents available from reliable sources on the Internet."[180] It does not appear "that any appellate court has passed definitively upon the admissibility as evidence of public records printed from a government website. . . . Trial courts have, however, found such copies admissible."[181] Courts have applied the public records exception to the hearsay rule to admit information displayed on the websites of the United States Census Bureau[182] and the United States Postal Service.[183] In addition, at least one court applied this exception to admit the public record of a foreign government.[184] The

[178] *See* FED. R. EVID. 803(8) advisory committee's note (citing Wong Wing Foo v. McGrath, 196 F.2d 120 (9th Cir. 1952)).

[179] Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 574 (D. Md. 2007); *see* United States v. Doyle, 130 F.3d 523, 546 (2d Cir. 1997) (noting that foundation witnesses are not required under Rule 803(8)).

[180] United States *ex rel.* Dingle v. Bioport Corp., 270 F. Supp. 2d 968, 972 (W.D. Mich. 2003) (citation omitted).

[181] Bernstein v. City of New York, No. 28863/04, 2007 WL 283072, at *3 (N.Y. Sup. Ct. Feb. 1, 2007) (citation omitted).

[182] *See* U.S. Equal Emp't Opportunity Comm'n v. E.I. Du Pont De Nemours & Co., No. Civ.A. 03-1605, 2004 WL 2347559, at *1 (E.D. La. Oct. 18, 2004) (holding that a table of information compiled by the United States Census Bureau and printed from the Census Bureau's website was admissible as a public record under Rule 803(8)).

[183] *See* Chapman v. S.F. Newspaper Agency, No. C 01-02305 CRB, 2002 WL 31119944, at *2 (N.D. Cal. Sept. 20, 2002) (holding that a printout of a page from the United States Postal Service website was admissible as a public record under Rule 803(8)(A)).

[184] *See* United States v. New-Form Mfg. Co., 277 F. Supp. 2d 1313, 1326 (Ct. Int'l Trade 2003) (holding that a record created from information available on the official website of

exception has also been applied to e-mails that otherwise met the requirements of Rule 803(8).[185]

6. Market Reports and Commercial Publications

[65] The hearsay rule does not preclude the admission of "[m]arket quotations, tabulations, lists, directories, or other published compilations, generally used and relied upon by the public or by persons in particular occupations."[186] Such information is viewed as trustworthy, and worthy of hearsay exception, because of the public's reliance on the material, which incentivizes the compiler of the information to provide accurate information.[187]

[66] Nearly all of the market reports and commercial publications contemplated by this exception to the hearsay rule are now available on the Internet.[188] Thus, whereas twenty years ago a court might have been asked to apply this exception to the National Automobile Dealers Association (NADA) "Blue Book," which provides value information for new and used motor vehicles, the proponent of such evidence is now more likely to ask the court to admit value information from the NADA or

the Office of the Superintendent of Bankruptcy Canada was admissible under Rule 803(17)).

[185] *See* Lester v. Natsios, 290 F. Supp. 2d 11, 26 (D.D.C. 2003) (finding that e-mails regarding a job vacancy at a government agency were admissible as public records under Rule 803(8)).

[186] FED. R. EVID. 803(17).

[187] FED. R. EVID. 803(17) advisory committee's note.

[188] *Cf.* United States *ex rel.* Dingle v. Bioport Corp., 270 F. Supp. 2d 968, 972 (W.D. Mich. 2003).

Kelley's websites.[189] Both have been admitted to demonstrate the value of a motor vehicle.[190]

VI. PROVING THE CONTENT OF ELECTRONIC WRITINGS, RECORDINGS, AND PHOTOGRAPHS

A. Original Document Rule and Other Methods of Proving Contents

[67] The Federal Rules of Evidence state that "[t]o prove the content of a writing, recording, or photograph, the original writing, recording, or photograph is required, except as otherwise provided in these rules or by Act of Congress."[191] For data maintained on "a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original.'"[192] "A duplicate is admissible to the same extent as an original unless (1) a genuine question is raised as to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original."[193]

[68] If the original is lost or destroyed (unless destroyed by the proponent of the evidence in bad faith), not obtainable by judicial practice, or in the possession of the proponent's opponent, the original is not required and the proponent may seek to admit other "secondary" evidence of the content of the writing, recording, or photograph.[194] Further, the

[189] *See generally* State v. Erickstad, 620 N.W.2d 136, 145 (N.D. 2000); *see also* Irby-Greene v. M.O.R., Inc., 79 F. Supp. 2d 630, 636 n.22 (E.D. Va. 2000) (indicating the court's reliance on the Kelley Blue Book Internet website for valuation of two vehicles).

[190] *See* Hess v. Riedel-Hess, 794 N.E.2d 96, 103 (Ohio Ct. App. 2003) (holding that the NADA appraisal guide printed from NADAguides.com was admissible pursuant to Ohio Rule of Evidence 803(17)); *Erickstad*, 620 N.W.2d at 145-46 (holding that the valuation information for a pickup truck found on the Kelley Blue Book website was admissible).

[191] FED. R. EVID. 1002.

[192] FED. R. EVID. 1001(3).

[193] FED. R. EVID. 1003.

[194] *See* FED. R. EVID. 1004.

proponent need not account for the missing original if the testimony or written admission of his opponent proves the content of the record.[195] Finally, if writings, recordings, or photographs are voluminous, their contents may be presented via summary, chart or calculation.[196] In that case, the original writings, recordings, or photographs, or duplicates thereof, must be made available for examination or copying, or both, by other parties to the litigation.

B. Application to Electronic Evidence

[69] Electronic evidence consists entirely of writings, recordings, and photographs.[197] Accordingly, the original document rule applies whenever a party attempts to prove the contents of the electronic evidence.[198] E-mails, text messages, chat room dialogue, and other electronic records all qualify as writings because they consist of letters, words, or numbers set down by mechanical or electronic recording, or other forms of data compilation.[199] Due to "the myriad ways that electronic records may be deleted, lost as a result of system malfunctions, purged as a result of routine electronic records management software (such as the automatic deletion of e-mail after a set period of time) or otherwise unavailable,"[200]

---

[195] *See* FED. R. EVID. 1007.

[196] FED. R. EVID. 1006.

[197] *See* FED. R. EVID. 1001(1).

[198] *See* Lorraine v. Markel Am. Ins. Co, 241 F.R.D. 534, 578 (D. Md. 2007).

[199] *See* State v. Espiritu, 176 P.3d 885, 892 (Haw. 2008) (admitting printouts of text messages received by the victim and holding that the original text messages were not required under an exception to the original writing rule, which excuses the production of an original or duplicate if the original was lost or destroyed absent bad faith on the part of the proponent); Adams v. State, 117 P.3d 1210, 1218 (Wy. 2005) (admitting computer printouts of a chat room dialogue between the defendant and a police officer where "[t]he State's witness testified that the chat log exhibits were exact copies of the communication between the parties contained on the computer and thus, they were either appropriate computer 'originals' or duplicates which were properly authenticated.").

[200] *Lorraine*, 241 F.R.D. at 580.

proponents must often resort to secondary evidence to prove their contents.[201]

VII. CONCLUSION

[70] Though certain issues, such as authentication, may be more complicated in the context of electronic evidence, traditional evidentiary principles can be consistently adapted to address questions regarding the admissibility of electronic evidence. Guided by the *Lorraine* model and the cases cited in this article, the proponent of electronic evidence should have little difficulty successfully moving the admission of his or her evidence. When all else fails, comparison of the electronic evidence with its most similar non-electronic analogue will enable a proponent to draw upon the court's familiarity with traditional evidentiary principles to provide comfort in the trustworthiness of the electronic evidence. As one court has said, "[t]he potentially limitless application of computer technology to evidentiary questions will continually require legal adaptation." [202] That adaptation must necessarily begin with the proponents of electronic evidence.

[201] *See Espiritu*, 176 P.3d at 893 (admitting secondary evidence of the content of text messages where the witness no longer had the text messages at issue because she no longer had the cellular telephone or cellular telephone service from the provider through which she had received the messages); *see also* United States v. Hunter, 266 F. App'x 619, 621-22 (9th Cir. 2008) (admitting excerpts of a series of text messages as summaries under Rule 1006 and holding that, "if the defendant objects to the summary of the evidence, he cannot have the evidence excluded, but instead, can compel the government to introduce the rest of the incomplete evidence.").

[202] Penny v. Commonwealth, 370 S.E.2d 314, 317 (Va. Ct. App. 1988).