

**BACK TO THE FUTURE: *LORRAINE V. MARKEL AMERICAN
INSURANCE CO.* AND NEW FINDINGS ON THE
ADMISSIBILITY OF ELECTRONICALLY STORED
INFORMATION**

Hon. Paul W. Grimm, Michael V. Ziccardi, Esq.,**
Alexander W. Major, Esq.****

I. Do the Rules of Evidence Apply to Electronic Evidence?.....	361
II. Preliminary Matters and Conditional Relevance.....	363
III. Authentication of ESI.....	366
A. Rule 901.....	367
B. Rule 902.....	384

*The Honorable Paul W. Grimm is the Chief United States Magistrate Judge for the United States District Court for the District of Maryland. He was appointed to the court in February 1997. Judge Grimm received an A.B. degree, *summa cum laude*, from the University of California, Davis, and graduated *magna cum laude* from the University of New Mexico School of Law. Judge Grimm retired as a Lieutenant Colonel in the U.S. Army Reserve. He has written numerous books and articles on evidence, civil procedure, and trial practice, and currently serves as an adjunct faculty member at the University of Baltimore and University of Maryland Schools of Law. Judge Grimm has published a number of decisions detailing the admissibility of electronically stored information, including *Lorraine v. Markel American Insurance Co.*, 241 F.R.D. 534 (D. Md. 2007), which serves as the starting point of this Article. The opinions expressed herein are those of the authors themselves, and do not purport to be those of the federal judiciary, or the District of Maryland.

**Michael V. Ziccardi, Esq., is currently the 2008-09 law clerk to the Hon. Paul W. Grimm. Mr. Ziccardi received a B.A. degree, *summa cum laude*, from the George Washington University, and graduated *cum laude* from the University of Baltimore School of Law. During law school, Mr. Ziccardi served as the Managing Editor of the *Law Review*, and Captain of the AAJ Mock Trial Team. Mr. Ziccardi would like to thank Nina Wu, J.D. Candidate 2009, University of Maryland School of Law, and Michelle Lambert, J.D. Candidate 2010, University of Baltimore School of Law, for their help in preparing this Article for publication.

***Alexander W. Major, Esq., is a member of Venable LLP's Commercial Litigation group in Baltimore, Maryland, and part of the firm's E-Discovery Task Force. Before assuming his current position, he was the law clerk to the Hon. Paul W. Grimm and a litigation associate at Arnold and Porter LLP in Washington, D.C. Mr. Major is a graduate, *cum laude*, of the Catholic University of America, Columbus School of Law. Prior to a career in law, he served ten years as a U.S. Air Force intelligence officer and is presently a Major in the Air Force Reserve.

IV. The Hearsay Rule and its Exceptions as Applied to ESI/Digital Evidence	396
A. Rule 803 Hearsay Exceptions	402
B. Rule 804 Hearsay Exceptions	410
V. The Original Writing Rule as Applied to ESI/Digital Evidence	412
VI. Prejudicial Impact	418
VII. Conclusion	418

Imagine the following hypothetical, patterned on an actual case pending in federal court,¹ and you can begin to appreciate why there is a growing awareness of the need to have clear analytical thinking regarding the admissibility of electronically stored information, variously referred to as “ESI,” “digital,” “electronic,” “computer generated,” or “computer stored” evidence in state and federal courts.

ConsumerPro is a corporation that provides installment credit to consumers with poor or un-established credit records to enable them to purchase on credit expensive electronic and computer products like flat screen televisions, computers, and entertainment systems. Under their business plan, a purchaser agrees to buy a product in installments, such as automatic withdrawals from a bank account, and only after the purchaser has made a series of payments is the product shipped to the purchaser, who then continues to make payments until the purchase price is fully paid.

ConsumerPro has a website that advertises its products, has contact information for inquiries about billing, and provides customer service. ConsumerPro makes most of its sales by running advertisements on national television by targeting its ads during popular TV programs. The ads pitch the products, then list a telephone number to call for more information and to make a purchase, and encourage the viewer to call immediately to get the benefit of a time limited special deal. When the purchaser calls the number, she speaks with a telemarketing employee of Tele-Sales, Inc., a separate company that ConsumerPro contracts with to handle the sales calls. Because ConsumerPro provides installment credit, it must comply with a host of federal and state consumer protection laws that require certain mandatory disclosures that must be given, or the purchase is voidable, and ConsumerPro could also face civil and criminal penalties. In order to comply with all the regulatory

1. The names of the parties used in the hypothetical are fictitious, as are some of the facts.

requirements, ConsumerPro's general counsel has carefully drafted the script that must be read with complete accuracy by the telemarketers working at Tele-Sales call centers. To insure regulatory compliance, the contract between ConsumerPro and Tele-Sales requires use of the script provided by ConsumerPro, without deviation, and creates a penalty to Tele-Sales for each call that fails to adhere to the script. Because the Tele-Sales telemarketers receive very sensitive financial information from the purchasers who call in, they operate under strict security conditions. No writing materials are permitted in the call center. The telemarketers have a phone headset they wear, and log into a secure ConsumerPro website, where the current version of the script is accessed and read to the purchaser, and when the telemarketer receives the purchaser's financial information, it is entered by computer keyboard directly into the ConsumerPro website, which electronically records all the details of the purchase. In addition, all the sales calls are recorded so that ConsumerPro can monitor them to ensure compliance with the disclosure script. Thus, there are no "paper" copies of the script, or the individual installment sales contracts; all this information is electronically displayed and maintained by ConsumerPro. If a dispute arises regarding a particular sale, ConsumerPro can print off the screen for the contract, and then listen to the recording of the sales call to determine if there was regulatory compliance and a valid sale.

After six months of handling sales calls for ConsumerPro, Tele-Sales's contract is abruptly cancelled by ConsumerPro, allegedly because of systemic failures to comply with the obligation to adhere to the marketing script. ConsumerPro contends that so many calls were noncompliant that most of the contracts are voidable, and refuses to pay Tele-Sales. Tele-Sales contends that their telemarketers faithfully read the script, and that ConsumerPro changed the script frequently, significantly altering its content, and that ConsumerPro is attempting to avoid paying for calls that followed the script that appeared on the ConsumerPro marketing site, by referencing a subsequently changed version of the script. ConsumerPro denies this, and contends that they matched the applicable script to the call, and determined that calls were noncompliant. Because Tele-Sales does not have access to any "hard copies" of the various scripts they followed, they must rely on what their telemarketers recall as the content of the scripts. Tele-Sales sues ConsumerPro in federal court for breach of contract, and ConsumerPro files a counterclaim for breach of contract.

In addition to its difficulties with Tele-Sales, ConsumerPro has other problems. Thousands of customer complaints have been filed with the Federal Trade Commission and various state Attorneys General alleging unfair sales practices, misleading, inaccurate and false representations posted on the ConsumerPro website, bait-and-switch tactics, failure to adhere to the credit sales terms, failure to refund money for cancelled sales, and customer service complaints regarding inferior or deficient products. The FTC conducts an investigation, initiates enforcement proceedings, concludes violations of federal law occurred, and negotiates a consent decree with ConsumerPro. The FTC posts on its website the investigation report and consent decree, and posts a warning on its website for consumers, warning them about ConsumerPro. Various state Attorneys General conduct their own investigations, commence enforcement proceedings, post the results of their investigations, and also post consumer warnings on their websites. Eventually, a class action consumer fraud lawsuit is filed against ConsumerPro.

Myriad evidentiary issues are raised by this hypothetical. First, with the exception of the contract between Tele-Sales and ConsumerPro, all of the “documentary evidence” that will determine the outcome of the contract suit is computer generated and stored ESI. Second, the class action against ConsumerPro will depend largely on consumer testimony about what they saw on ConsumerPro’s website, which has been changed many times, as well as the results of the FTC and Attorneys General investigations that found unfair trade practices and consumer fraud. The evidentiary issues associated with introducing electronic evidence are complicated, and until recently, have not been addressed in any comprehensive way.

In a recent opinion, however, *Lorraine v. Markel American Insurance Co.*,² the United States District Court for the District of Maryland undertook the first comprehensive analysis of the evidentiary rules and case law that govern the admissibility of electronic evidence at trial, and for use at summary judgment.³ It remains the most comprehensive single opinion regarding the admissibility of ESI, and

2. 241 F.R.D. 534 (D. Md. 2007).

3. See FED. R. CIV. P. 56(e)(1) (providing that “[a] supporting or opposing affidavit must be made on personal knowledge, set out facts that would be admissible in evidence, and show that the affiant is competent to testify on the matters stated”).

has frequently been cited by other courts and in secondary sources.⁴ This Article will analyze the *Lorraine* opinion and its impact, as well as provide some insight regarding additional authority relating to this new frontier of evidence law.

I. DO THE RULES OF EVIDENCE APPLY TO ELECTRONIC EVIDENCE?

It is not a frivolous question to ask, “Do the existing rules of evidence adequately deal with admissibility of electronic evidence?” In a thoughtful, recently published book, attorney George Paul, who has extensive experience dealing with evidentiary issues associated with ESI/digital evidence,⁵ made the following observations:

The current evidentiary scheme comprises three main historical policies: (1) the notion of authentic writings, exemplified by the search for an “original” object tying certain people, acting at a certain time, to certain permanently recorded information; (2) the rule against hearsay, giving litigants the right to test factual statements through cross-examination, unless there was an accepted policy reason not to do so;

4. See, e.g., *Paralyzed Veterans of America v. McPherson*, No. C 06-4670 SBA, 2008 WL 4183981, at *7 (N.D. Cal. Sept. 9, 2008) (citing *Lorraine*, 241 F.R.D. at 551); *Phillips v. Morbark, Inc.*, 519 F. Supp. 2d 591, 596 (D.S.C. 2007) (citing *Lorraine*, 241 F.R.D. at 534-553); *Scotts Co. LLC v. Liberty Mut. Ins. Co.*, 2:06-CV-899, 2007 WL 1723509, at *3 n.2 (S.D. Ohio June 12, 2007) (citing *Lorraine*, 241 F.R.D. at 547); *Estate of Gonzales v. Hickman*, No. ED CV 05-660 MMM (RCx), 2007 WL 3237727, at *2 n.3 (C.D. Cal. May 30, 2007) (citing *Lorraine*, 241 F.R.D. at 534); *Adams v. Disbennett*, No. 9-08-14, 2008 WL 4615623, at *3-4 (Ohio Ct. App. Oct. 20, 2008) (citing *Lorraine*, 241 F.R.D. at 543); THE SEDONA CONFERENCE WORKING GROUP ON ELECTRONIC DOCUMENT RETENTION AND PRODUCTION, THE SEDONA CONFERENCE COMMENTARY ON ESI EVIDENCE & ADMISSIBILITY 1 (2008) [hereinafter SEDONA CONFERENCE COMMENTARY] (recognizing *Lorraine* as the “recent, leading case on the subject” of using ESI as evidence “at trial or in motion practice”); Gordon J. Calhoun & Susan F. Friedman, *The Stage is Set*, N.Y. L.J., Feb. 21, 2008, at 24 (“[*Lorraine*] provides an exegesis about what counsel must do when proffering ESI during dispositive motions or trials As ESI may likely constitute the majority of information offered as evidence in the future, counsel should utilize [*Lorraine*] as a road map to save time and money by getting the evidentiary foundation issues right on the first audition.”); Adam I. Cohen, *The Revised Federal Rules of Civil Procedure: Where We Are One Year Later*, CORPORATE COUNSELOR, Feb. 2008, at 4 (“In an opinion that is required reading for lawyers aspiring to use ESI to win a case, Judge Grimm delivered a sweeping review of prior case law and analysis of the Federal Rules of Evidence with respect to admissibility issues associated [with] all manner of electronic evidence.”); Sheldon M. Finkelstein & Evelyn R. Storch, *Admissibility of Electronically Stored Information: It’s Still the Same Old Story*, LITIGATION, Spring 2008, at 13, 17 (“A helpful starting place for any analysis of admissibility of ESI is Chief United States Magistrate Judge Paul W. Grimm’s decision in [*Lorraine*]. The lengthy ‘soup to nuts’ opinion is an authority-rich discourse of every facet of the admission of evidence generally and of ESI in particular.”); Dale Conder, Jr., *The Admissibility of Electronically Stored Information*, FOR THE DEFENSE, Sept. 2008, at 23, 29 (citing *Lorraine*, 241 F.R.D. at 554, 574).

5. See GEORGE L. PAUL, FOUNDATIONS OF DIGITAL EVIDENCE xxi (2007).

and (3) the notion that evidence, particularly evidence implicating specialized knowledge, be generally scientific in that it be subject to a “test” of its hypotheses or methodologies. These policies are all stressed by digital evidence There is now a new world of [digital] evidence. New foundations are necessary.⁶

While this may be true, and a “new world order” of admitting and weighing electronic evidence an inevitable outcome, this will not occur overnight, and in the interim there must be a method of dealing with the ever changing forms of digital or electronic evidence in court proceedings. This means that the existing law of evidence must be applied to the admissibility of electronic evidence, and courts that have been asked to do so have expressed no significant concerns about the adequacy of those rules to accomplish this task. As one court noted, “Essentially, appellant would have us create a whole new body of law just to deal with e-mails or instant messages. . . . We believe that e-mail messages and similar forms of electronic communications can be properly authenticated within the existing framework of [the rules of evidence].”⁷ Recognizing this, the *Lorraine* opinion identifies the following five evidentiary “hurdles” that must be evaluated in order to assess the admissibility of electronically stored or digital evidence:

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. Whenever ESI is offered as evidence, either at trial or in summary judgment, the following evidence rules must be considered: (1) is the ESI **relevant** as determined by Rule 401 (does it have any tendency to make some fact that is of consequence to the litigation more or less probable than it otherwise would be); (2) if relevant under 401, is it **authentic** as required by Rule 901(a) (can the proponent show that the ESI is what it purports to be); (3) if the ESI is offered for its substantive truth, is it **hearsay** as defined by Rule 801, and if so, is it

6. *Id.* at 13-14.

7. *In re F.P.*, 878 A.2d 91, 95 (Pa. Super. Ct. 2005). *See also* DAVID F. HERR, MANUAL FOR COMPLEX LITIGATION § 11.446 (4th Ed. 2007) (stating that “the Federal Rules of Evidence apply to computerized data as they do to other types of evidence”); *Lorraine*, 241 F.R.D. at 538 n.5 (“FED. R. EVID. 102 contemplates that the rules of evidence are flexible enough to accommodate future ‘growth and development’ to address technical changes not in existence as of the codification of the rules themselves. Further, courts have had little difficulty using the existing rules of evidence to determine the admissibility of ESI, despite the technical challenges that sometimes must be overcome to do so.”).

covered by an applicable exception (Rules 803, 804 and 807); (4) is the form of the ESI that is being offered as evidence an **original** or **duplicate** under the original writing rule, or if not, is there admissible secondary evidence to prove the content of the ESI (Rules 1001-1008); and (5) is the probative value of the ESI substantially outweighed by the danger of **unfair prejudice** or one of the other factors identified by Rule 403, such that it should be excluded despite its relevance.⁸

However, before discussing each of these evidentiary hurdles, the *Lorraine* opinion noted the importance of Federal Rules of Evidence 104(a) and 104(b), which deal with preliminary rulings on admissibility of evidence, existence of a privilege, and qualifications of witnesses, and the related concept of conditional relevance.⁹

II. PRELIMINARY MATTERS AND CONDITIONAL RELEVANCE.

As noted in *Lorraine*, “the relationship between Rule 104(a) and (b) can complicate the process by which ESI is admitted into evidence at trial, or may be considered at summary judgment.”¹⁰ Rule 104(a) states:

Preliminary questions concerning the qualification of a person to be a witness, the existence of a privilege, or the admissibility of evidence shall be determined by the court, subject to the provisions of subdivision (b). In making its determination it is not bound by the rules of evidence except those with respect to privileges.¹¹

This rule is important for several reasons. First, it establishes the role of the trial judge as the one who must determine whether evidence is admissible, which includes the familiar foundational rulings such as whether evidence is relevant, and if so, if it is excessively prejudicial; whether an expert witness is qualified to testify, and if so whether her opinions have a sufficient factual basis and are based on reliable methodology; whether out of court statements, whether written or oral, are hearsay, and if so, whether they fall within the scope of a hearsay exception; whether an evidentiary privilege applies; and when the contents of a writing, recording or photograph are being proved, whether the proof constitutes an original, duplicate, or acceptable secondary

8. *Lorraine*, 241 F.R.D. at 538.

9. *Id.*

10. *Id.* at 539.

11. FED. R. EVID. 104(a).

evidence of its contents under the original writing rule.¹² These preliminary evidentiary rulings can be purely “legal,” such as whether proffered evidence is relevant (does it have “any tendency” to make a fact that is “of consequence” to the litigation more probable or less probable than it would be without the proffered evidence), but may also involve mixed questions of law and fact, such as whether a document qualifies as a business record (was it a record of a “business,” made at or near the time of the events referenced in the record, by someone with personal knowledge of those facts, was the activity that the record refers to a “regular” one, is it the regular practice of the business to “make and maintain” the record for use in its business, and whether the document is otherwise trustworthy, all of which require the judge to engage in fact finding).

Rule 104(a) is qualified by Rule 104(b), which states: “When the relevancy of evidence depends upon the fulfillment of a condition of fact, the court shall admit it upon, or subject to, the introduction of evidence sufficient to support a finding of the fulfillment of the condition.”¹³ This is the so-called “conditional relevance” rule, and it reserves for the jury the determination of disputed facts that must be established in order for certain proffered evidence to be relevant. Thus, for example, if the plaintiff contends that her supervisor created a hostile workplace by sending her inappropriate e-mails, and the supervisor denies that he authored the e-mails, claiming instead that someone else “spoofed” them on his computer, the harassing e-mails will not be “relevant” (tend to prove intentional gender based discrimination) unless the jury first determines that the supervisor is the author.

The *Lorraine* opinion notes the importance of Rule 104(b) with regard to one very important component of determining the admissibility of ESI, whether it is authentic, noting “because authentication is essentially a question of conditional relevancy, the jury ultimately resolves whether evidence admitted for its consideration is that which the proponent claims.”¹⁴ *Lorraine* also points out a little appreciated

12. See, e.g., CHRISTOPHER B. MUELLER & LAIRD C. KIRKPATRICK, EVIDENCE 31-37 (3rd Ed. 2003).

13. FED. R. EVID. 104(b).

14. *Lorraine*, 241 F.R.D. at 539-40 (quoting *United States v. Branch*, 970 F.2d 1368, 1370 (4th Cir. 1992)); see also FED. R. EVID. 901(a) advisory committee’s notes to the 1972 proposed rules (“Authentication and identification represent a special aspect of relevancy This requirement of showing authenticity or identity falls in the category of relevancy dependent upon fulfillment of a condition of fact and is governed by the procedure set forth in Rule 104(b).”) (citations omitted).

aspect of the relationship between Rule 104(a) and 104(b). When a judge makes a preliminary determination under Rule 104(a) that evidence is admissible, or a privilege applies, or that a witness is qualified, he is not required to apply the rules of evidence except the rules of privilege when considering the facts proffered in support of and against the ruling.¹⁵ In contrast, however, when the jury is finding facts under the conditional relevance rule to determine whether proffered evidence is relevant, such as when they determine whether evidence of a posting on a website is authentic, the facts that they consider must be admissible in evidence.¹⁶ *Lorraine* summarizes this distinction as follows:

In short, there is a significant difference between the way that Rule 104(a) and 104(b) operate. Because, under Rule 104(b), the jury, not the court, makes the factual findings that determine admissibility, the facts introduced must be admissible under the rules of evidence. It is important to understand this relationship when seeking to admit ESI. For example, if an e-mail is offered into evidence, the determination of whether it is authentic would be for the jury to decide under Rule 104(b), and the facts that they consider in making this determination must be admissible into evidence. In contrast, if the ruling on whether the e-mail is an admission by a party opponent or a business record turns on contested facts, the admissibility of those facts will be determined by the judge under 104(a), and the Federal Rules of Evidence, except for privilege, are inapplicable.¹⁷

Few counsel fully appreciate the importance of this distinction, which is especially important when dealing with admissibility of ESI, because the most challenging aspect of admitting digital evidence is to establish its authenticity.¹⁸ *Lorraine* devotes its most extensive discussion to this issue. The essential point to take away from this

15. See FED. R. EVID. RULE 104(a) (“*In making its determination [the court] is not bound by the rules of evidence except those with respect to privileges.*”) (emphasis added). See also FED. R. EVID. 1101(d)(1) (“The rules (other than with respect to privileges) do not apply in the following situations: . . . The determination of questions of fact preliminary to admissibility of evidence when the issue is to be determined by the court under rule 104.”).

16. *Lorraine*, 241 F.R.D. at 540.

17. *Id.*

18. PAUL, *supra* note 5, at 17 (“Thus two monumental changes are brought on by digital technology, affecting the two most important concepts in the law of evidence. The first is related to the new type of writing that has evolved, viewed in its discrete manifestations. The ‘object’ the law examines has changed radically. It is no longer physical matter. It is information itself. Indeed, writing’s departure from the world of physical artifacts revolutionizes the concept of *authenticity*. The written record must now be analyzed differently than before.”).

discussion in *Lorraine* is that the proponent of digital evidence must carefully consider how she will authenticate it if its admissibility is challenged, and note that the evidence proffered to establish its authentication must itself be admissible into evidence.

III. AUTHENTICATION OF ESI

In actuality, the authentication of evidence is a relatively straightforward concept: “A piece of paper or electronically stored information, without any indication of its creator, source, or custodian may not be authenticated under Federal Rule of Evidence 901.”¹⁹ Nevertheless, in the two years since *Lorraine* was issued, courts and counsel still seem to struggle with the basic principles of authentication as it applies to electronic evidence. Some courts are still permitting only rudimentary admissibility standards and counsel are still, at times, failing to meet that low bar. As electronic evidence becomes more ubiquitous at trial, it is critical for courts to start demanding that counsel give more in terms of authentication—and counsel who fail to meet courts’ expectations will do so at their own peril.

It may come as no surprise to the readers of this Article that *Lorraine* was drafted, in part, as a “how to” for the authentication of electronic evidence. It was written to assist counsel in better preparing themselves for the use of electronic evidence during trial by clarifying how Rules 901 and 902 might apply. As *Lorraine* demonstrates, electronic evidence comes in many forms and it is no secret that someone highly adept with computers has the ability to make viewers see whatever he or she wants them to see. But it is also a very real possibility that someone *inept* with computers may also alter electronic evidence so as to make it unusable or inadmissible.²⁰ Therefore, as technology continues creating relevant evidence while, simultaneously, outpacing the working knowledge and ability of most lawyers and judges to deal with it, ensuring proper authentication of electronic evidence becomes a greater responsibility for attorneys and judges alike.

19. *United States v. O’Keefe*, 537 F. Supp. 2d 14, 20 (D.D.C. 2008).

20. *See, e.g.*, STEPHEN A. SALTZBURG ET AL., FEDERAL RULES OF EVIDENCE MANUAL pt.4, at 20 (9th ed. vol. 5 2006) (“The wrinkle for authenticity purposes is that, because Internet data is electronic, it can be manipulated and offered into evidence in a distorted form.”).

A. Rule 901

Rule 901 requires that evidence be authenticated before being admitted.²¹ That requirement sets a relatively low bar, permitting evidence to be authenticated if the “matter in question is what its proponent claims.”²² But, as *Lorraine* points out, the rule is silent as to how, exactly, courts and lawyers should demonstrate that evidence is “what its proponent claims.”²³

As a launching point, *Lorraine* relied on a number of Rule 901(b) illustrations²⁴ to describe the best manner by which to authenticate particular forms of electronic evidence. The particular illustration to be applied depends generally on the type of electronic evidence to be admitted, the manner in which it was created, and its intended use at trial. The most likely illustrations to apply to the majority of electronic evidence under Rule 901 include:

- E-mail Evidence:
 - Rule 901(b)(1), “Testimony of a Witness with Knowledge”
 - Rule 901(b)(3), “Comparison by Trier or Expert Witness”
 - Rule 901(b)(4), “Distinctive Characteristics and the Like”
- Internet Websites
 - Rule 901(b)(1), “Testimony of a Witness with Knowledge”
 - Rule 901(b)(3), “Comparison by Trier or Expert Witness”
 - Rule 901(b)(4), “Distinctive Characteristics and the Like”
 - Rule 901(b)(7), “Public Records or Reports”
 - Rule 901(b)(9), “Process or System”
- Chat Room and Text Messages

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

22. *Id.*

23. *Lorraine*, 241 F.R.D. at 542 (quoting FED. R. EVID. 901(a)).

24. Structurally, Rule 901 has two parts. Rule 901(a) contains the substantive requirement that evidence be authenticated or identified before it may be admitted. Rule 901(b) provides the non-exclusive illustrations of how this may be done. The proponent of the evidence can, therefore, “pick and choose” among these illustrations, but is also free to develop others. FED. R. EVID. 901.

- Rule 901(b)(1), “Testimony of a Witness with Knowledge”
- Rule 901(b)(4), “Distinctive Characteristics and the Like”
- Computerized Records or Data
 - Rule 901(b)(1), “Testimony of a Witness with Knowledge”
 - Rule 901(b)(3), “Comparison by Trier or Expert Witness”
 - Rule 901(b)(4), “Distinctive Characteristics and the Like”
 - Rule 901(b)(9), “Process or System”
- Computer Animations
 - Rule 901(b)(1), “Testimony of a Witness with Knowledge”
 - Rule 901(b)(3), “Comparison by Trier or Expert Witness”
- Computer Simulations
 - Rule 901(b)(1), “Testimony of a Witness with Knowledge”
 - Rule 901(b)(3), “Comparison by Trier or Expert Witness”
- Digital Photographs
 - Rule 901(b)(9), “Process or System”²⁵

With this “checklist” in mind, it is helpful to see what courts have done with various types of ESI when determining whether it is authentic.

1. Internet Websites

Introduction of the content of websites, and website search results, is becoming an increasingly common evidentiary occurrence. Searches and Internet surfing are easy and common practices, but using those results at trial requires counsel to step away from the computer, and think about how, exactly, the proffered website should be authenticated.

In *Whelan v. Hartford Life & Accident Insurance Co.*,²⁶ decided after *Lorraine*, the plaintiff sought to introduce Nexis printouts as

25. See *Lorraine*, 241 F.R.D. at 541-49 (discussing Rule 901 and its subparts); *id.* at 554-63 (applying Rule 901 to the types of evidence listed above).

26. No. CV06-4948PSG (PLAX), 2007 WL 1891175, at *11 (C.D. Cal. June 28, 2007).

evidence to show that the doctor who performed the plaintiff's examination was biased and closely affiliated with an insurance company.²⁷ The plaintiff argued that the printouts would demonstrate that the doctor was associated with a network of providers that "cater[ed] exclusively to the insurance industry."²⁸ To authenticate the printouts, plaintiff's counsel submitted a declaration "stating that the printouts are true and correct copies of the result of an internet search of services provided to insurance companies by [the network of providers]."²⁹ The defendant objected to the evidence, in part, on the grounds that the evidence had not been authenticated.³⁰

The court examined the evidence and held that, although the printouts had a URL address and date stamp, the attorney's declaration was insufficient to authenticate them.³¹ What was required, the court held, was a "declaration by the person who personally conducted the search, or by the company stating that the computer printouts are a true and correct copy of the information from its website."³² The standard insisted upon by the court in *Whelan* reflects the manner in which courts may avoid the concerns identified in *Lorraine* that a website may include information not officially sanctioned by its alleged owner. Accordingly, when faced with the authentication of websites, as reflected in *Whelan*, courts may require "proof by the proponent that the organization hosting the website actually posted the statements or authorized their postings."³³

A similar case, also decided after *Lorraine*, related to the authentication of websites and e-mails serves not only to underscore the importance of authentication, but as a warning that authentication should be done properly. In *Bowers v. Rector & Visitors of the University of Virginia*,³⁴ the authentication of e-mails and websites became an issue in the plaintiff's claims associated with her termination from the University.³⁵ As part of her cross-motion for summary judgment, the

27. *Id.* at *11.

28. *Id.*

29. *Id.*

30. *Id.*

31. *Id.*

32. *Id.*

33. *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 555 (D. Md. 2007) (citing *United States v. Jackson*, 208 F.3d 633, 638 (7th Cir. 2000); *St. Luke's Cataract & Laser Inst. P.A. v. Sanderson*, No. 8:06-CV-223-T-MSS, 2006 WL 1320242 (M.D. Fla. May 12, 2006); *Wady v. Provident Life & Accident Ins. Co. of Am.*, 216 F. Supp. 2d 1060, 1064 (C.D. Cal. 2002)).

34. No. 3:06cv00041, 2007 WL 2963818, at *1 (W.D. Va. Oct. 9, 2007).

35. *Id.* at *1.

plaintiff, by counsel, submitted a thirty-eight page memorandum and seventy-four exhibits totaling over 600 pages.³⁶ Included with those 600 pages were an incendiary affidavit, fifty-one unauthenticated e-mails, and unauthenticated printouts from a Virginia Employment Commission website and a University of Virginia webpage.³⁷ The defendants responded by contending that most of plaintiff's evidence was inadmissible and moved to strike the plaintiff's unauthenticated submissions while also seeking sanctions under Rule 56(g).³⁸

As part of her reply, plaintiff's counsel attempted to remedy her failure to authenticate the e-mails and websites by way of a personal affidavit wherein "she stated that the contested exhibits were in fact 'authentic' because the e-mails had been obtained from the defendants during the course of discovery and the web pages were taken from 'published' internet websites."³⁹ Her attempt to authenticate was viewed by the court as "an abject failure on her part either to understand or to appreciate a number of evidence rules, including *inter alia* Evidence Rules 402, 404, 802, 805, and 901."⁴⁰ Accordingly, the court granted the defendants' motion for Rule 56(g) sanctions, in part because:

[T]he submission by plaintiff's counsel of . . . more than fifty unauthenticated copies of e-mails convincingly demonstrates both a recklessness and an absence of preparation on the part of plaintiff's counsel. Equally so, her resort to use of her own affidavit in a misguided quick-and-easy attempt to fix significant evidentiary deficiencies, demonstrates a recklessness in preparation and a failure to exercise legal judgment abject.⁴¹

2. Chat Rooms and Text Messages

Anyone with teenage children or who has been to the mall recognizes that chat rooms and instant and text messaging are playing a larger part in the way we communicate as a society. Like it or hate it, it is a form of communication that is becoming increasingly pervasive, and therefore will be offered as evidence in civil and criminal cases. Chat room and text or instant messaging "dialogues," for example, pose

36. *Id.*

37. *Id.*

38. *Id.* at *2.

39. *Id.*

40. *Id.* at *6.

41. *Id.* at *7.

unique challenges to authentication due in large part to the fact that they typically are created by parties using anonymity-protecting “screen names” on websites where the host cannot be assumed to know the content. Courts have recognized numerous ways to authenticate the use of chat room transcripts, including authentication circumstantially under Rule 901(b)(4) and testimony by a witness with personal knowledge.⁴²

In *Adams v. Disbennett*,⁴³ the court held that a witness with personal knowledge was sufficient to authenticate instant message texts. In a case arising between disgruntled online lovers, the municipal court permitted the plaintiff to introduce transcripts of instant messaging that took place between the couple.⁴⁴ On appeal, defendant claimed that the court erred by admitting transcripts that plaintiff claimed were not properly authenticated under Ohio’s equivalent of Rule 901.⁴⁵ At trial, the court permitted the plaintiff to authenticate the documents through his own testimony based on personal knowledge.⁴⁶ As part of that testimony, the plaintiff identified his and defendant’s screen names, stated that he had not changed any of the private messages, and testified that the exhibits were a printout of what he saw on the screen on the various days the two chatted.⁴⁷

The defendant rebutted this evidence by stating that “she could not recall typing the messages [the plaintiff] attributed to her.”⁴⁸ Relying in part on *Lorraine*, defendant challenged the authentication of the documents and urged the Court of Appeals of Ohio to find error in the lower court’s ruling through the use of a more exacting standard for the authentication of the transcripts.⁴⁹ The court denied the defendant’s plea, finding no error since “there need be only a prima facie showing, to the court, of authenticity” and that the jury would be the final assessor of the full authenticity of the transcripts.⁵⁰ Accordingly, the court of appeals found that the “trial court was in the best position to observe the witnesses and assess credibility” and that it did not abuse its discretion when it authenticated the plaintiff’s exhibits.⁵¹

42. *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 556 (D. Md. 2007)

43. No. 9-08-14, 2008 WL 4615623 (Ohio Ct. App. Oct. 20, 2008).

44. *Id.* at *2.

45. *Id.*

46. *Id.* at *3.

47. *Id.*

48. *Id.*

49. *Id.* at *3-4 (citing *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 543 (D. Md. 2007)).

50. *Id.* at *3 (quoting *United States v. Reilly*, 33 F.3d 1396, 1404 (3d Cir. 1994)).

51. *Id.* at *4.

3. Computerized Records or Data

As *Lorraine* warned, “although computer records are the easiest to authenticate, there is growing recognition that more care is required to authenticate these electronic records than traditional ‘hard copy’ records.”⁵² Cases decided after *Lorraine* illustrate this trend.

A case in point is *United States v. Baker*,⁵³ where prosecutors failed to authenticate key evidence related to the prosecution of a man charged with distributing child pornography. That key piece of evidence was a report put together by the National Center for Missing and Exploited Children (“NCMEC”) that summarized the tip it had received from Yahoo, Inc. regarding Baker’s uploading of child pornography to a website, along with the filenames of the forty-six images he uploaded.⁵⁴ Relying solely on Rules 803(6) and 803(8), the government argued that the report was admissible hearsay as a business or public record.⁵⁵ But “[t]he Government’s position misse[d] the mark” in that it completely failed to authenticate the evidence.⁵⁶

During the course of the trial, the government failed to offer evidence to authenticate the NCMEC report.⁵⁷ The only witness called to identify the report and the forty-six images it named was the investigating police officer from the Texas Attorney General’s Cyber Crimes Unit.⁵⁸ This officer, however, did not testify that he had any personal knowledge of how the NCMEC report was prepared; nor did the officer have any knowledge of how the NCMEC responds to tips it receives from internet service providers.⁵⁹ Additionally, the Government did not contend that the report was self-authenticating under Rule 902 or under any authentication methods listed in Rule 901(b).⁶⁰ In fact, the court pointed out, “[t]he record [was] devoid of any evidence authenticating [the exhibit].”⁶¹ Accordingly, as the

52. *Lorraine*, 241 F.R.D. at 557.

53. 538 F.3d 324 (5th Cir. 2008).

54. *Id.* at 331.

55. *Id.*

56. *Id.* This ruling emphasizes the critically important point that began the analysis in *Lorraine*, namely that there are a series of evidentiary rules that must be considered when planning to introduce ESI, and failure to do so risks exclusion of the evidence. *Lorraine*, 241 F.R.D. at 538-39.

57. *Baker*, 538 F.3d at 331.

58. *Id.* at 326.

59. *Id.* at 332.

60. *Id.*

61. *Id.*

unauthenticated exhibit was the only evidence introduced to demonstrate that the suspect uploaded child pornography, the court reversed and vacated those charges.⁶²

As demonstrated above, failing the simple first step of authentication proved fatal to the prosecution's case. The *Baker* court recognized that the showing required to authenticate digital evidence need not be great, and simply calling the NCMEC's record custodian under Rule 901(b)(7) would have been sufficient for authentication.⁶³ It would appear that the Fifth Circuit was not, in this case, concerned about the accuracy of the report, only that it was in fact what the Government purported it to be.⁶⁴

In another case dealing with computer files associated with child pornography, *United States v. Salcido*,⁶⁵ a court once again examined whether the Government's evidence was properly authenticated. On the appeal of his conviction, Salcido claimed that the Government failed to authenticate the pornographic video and image files that were the basis of the charges against him.⁶⁶ At trial, the Government introduced the video and image evidence "by presenting detailed evidence as to the chain of custody, specifically how the images were retrieved from the defendant's computers."⁶⁷ The Ninth Circuit found that this was sufficient to authenticate the video and image evidence under Rule 901.⁶⁸

The *Baker* and *Salcido* cases are noteworthy because they underscore that, while the authentication of digital evidence may not be necessarily rigorous, it must occur. Both cases illustrate the observation made in *Lorraine* that "to date, more courts have tended towards the lenient rather than the demanding approach" of authentication.⁶⁹

For example, a similar, and surprisingly low bar for authentication was used by the U.S. District Court of Arizona in *Linderoth Associates v. Amberwood Development, Inc.*⁷⁰ In support of its motion for summary judgment in a copyright case, a defendant proffered computer

62. *Id.* at 332-33.

63. *Id.* at 331 n.12.

64. *See* *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 557-59 (D. Md. 2007) (comparing standards for the admissibility of business records).

65. 506 F.3d 729 (9th Cir. 2007), *cert. denied*, 128 S. Ct. 1918 (2008).

66. *Id.* at 732-33.

67. *Id.* at 733.

68. *Id.*

69. *Lorraine*, 241 F.R.D. at 558.

70. No. CV 06-00426-PHX-NVWAR, 2007 WL 2696851, at *2 (D. Ariz. Sept. 12, 2007).

printouts purporting to identify the dates it started and finished an architectural plan that was at issue in the case.⁷¹ The plaintiff claimed that the printout was not properly authenticated and the court permitted the defendant to supply additional evidence to do so.⁷² In response, the defendant filed an affidavit with the court from the company's vice-president wherein he "swore that he 'assist[s] with the management of the electronic storage of [defendant's] files, including AutoCad files for floor plans and drawings,' that he understood that '[defendant's] database recorded the start and modification dates' for the [at-issue] file, and that he had personally reviewed the file and verified that its creation date was [as stated in the printout]."⁷³ Over the plaintiff's objections, the court held that the defendant's proffer was sufficient to authenticate the printouts.⁷⁴ The court concluded that it would not be necessary for the individual authenticating the record to possess "technical knowledge of how the computer functions, nor is it necessary that the authenticator be the one who created the file. It [would be] sufficient if the person authenticating the record ha[d] personal knowledge of the record system and [was] the custodian of the record in question."⁷⁵

The authentication rule applied in *Linderoth* seemed to be an amalgamation of Rules 901(b)(1) and 901(b)(7), requiring the custodian of the record to have personal knowledge of the record system, but not the record itself. Although Rules 901(b)(1) and 901(b)(7) may be sufficient for the authentication of some computer records, counsel should be cautious when relying on their minimal standards. In relation to the type of computer record offered in *Linderoth*, the standard used by the court was minimal. Were the printouts that were proffered a report automatically generated by AutoCad? If so, was the process that created them reliable and accurate? How did the court know that the dates reported on AutoCad and echoed in the report were, in fact, the proper dates? The answers to these questions are unclear. As a result, the opinion offers little guidance to attorneys who may be trying to authenticate similar files or reports in the future. Accordingly, a more proper authentication for such evidence may be Rule 901(b)(9).⁷⁶ Rule

71. *Id.* at *2.

72. *Id.*

73. *Id.*

74. *Id.*

75. *Id.*

76. FED. R. EVID. 901(b)(9) ("Evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result.").

901(b)(9) “[was] designed for situations in which the accuracy of a result is dependent upon a process or system which produces it.”⁷⁷ Under the Rule 901(b)(9) standard “it is common for the proponent to provide evidence of the input procedures and their accuracy, and evidence that the computer was regularly tested for programming error,” and “[a]t a minimum, the proponent should present evidence sufficient to warrant a finding that the information is trustworthy and provide the opponent with an opportunity to inquire into the accuracy of the computer and of the input procedures.”⁷⁸

4. Computer Records as Digital Images of Paper Records

Another variety of digital evidence that has been the subject of scrutiny is digital images of paper records. A November 2008 White Paper prepared by Cohasset Associates, Inc., emphasizes that many companies who currently possess paper records are in the process of converting or transforming them into computer records through scanning.⁷⁹ The White Paper provides an exacting review on the subject of digital images and, in part, on how such images should be authenticated for use at trial. Citing to *Lorraine* and *In re Vee Vinhnee*,⁸⁰ the paper suggests that, when seeking to authenticate digital copies of paper records, the proponent should add three steps to Professor Imwinkelried’s eleven-steps for foundation suggested for computer records.⁸¹ These steps include:

77. FED R. EVID. 901(b)(9) advisory committee’s notes to the 1972 proposed rules.

78. JACK B. WEINSTEIN & MARGARET A. BERGER, WEINSTEIN’S FEDERAL EVIDENCE § 901.12[3], at 901-101 (2d ed. Supp. 2002) (citations omitted). *See, e.g.*, *Novak v. Tucows, Inc.*, No. 06-CV-1909, 2007 WL 922306, at *4 (E.D.N.Y. Mar. 26, 2007) (holding evidence created for trial was sufficiently authenticated under Rule 901(b)(9) in that it sufficiently described “a process or system used to produce a result and showing that the process or system produces an accurate result”) (quoting FED. R. EVID. 901(b)(9)) (internal quotation marks omitted).

79. *See* COHASSET ASSOCIATES, INC., THE LEGALITY OF DIGITAL IMAGE COPIES OF PAPER RECORDS (October 2008), available at <http://www.cohasset.com> (click on “White Papers” tab, then click on “The Legality of Digital Image Copies of Paper Records”) [hereinafter THE WHITE PAPER]. Cohasset Associates, Inc., is a nationwide consulting firm specializing in document-based information management, and has edited and published numerous studies on the use of alternative media for data storage.

80. *Id.* at 15 (citing *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 537 (D. Md. 2007); *In re Vee Vinhnee*, 336 B.R. 437, 448 (B.A.P. 9th Cir. 2005)).

81. *Id.* at 15-16. As noted by the *In re Vee Vinhnee* court, Professor Imwinkelried recognized “electronic records as a form of scientific evidence,” and suggested an eleven-step protocol for authentication of such evidence. 336 B.R. at 446.

- *The business has established policies and procedures* – guiding the execution of specific activities and serving to enhance the quality with which those activities are performed. (This is significantly broader in scope than the #3 Imwinkelried requirement, which is focused on “inserting data into the computer.”)
- *The business demonstrates it has created and retained “management evidence” detailing (for future quality verification) who did what, where and when in the execution of the specific activities in the regular course of business* – showing that degree to which the policies and procedures were followed.
- *The business manifests that its “management evidence” was regularly audited for quality* – and, as part of an ongoing continuous improvement process, deficiencies were addressed and improvements were made to achieve high quality⁸²

In proposing the additional steps, the White Paper suggests that challenges to a records management process could be foreclosed by establishing that the process by which documents were managed and/or converted was sound. This is especially critical in terms of digitally converted records where the original, paper records are destroyed and no longer accessible after the information they contained is moved.⁸³ If, at trial, the process used by the proponent of digitized records is found faulty, “the consequence of a ruling that some or all of that small percentage [of litigation relevant documents] is inadmissible could prove very costly.”⁸⁴

5. Authentication by Experts

Under Rule 901(b)(3), the authentication of some forms of electronic evidence may, at times, require the use of an expert to explain either the technology used to create the evidence or the evidence

82. THE WHITE PAPER, *supra* note 79, at 15-16.

83. *Id.* at 17.

84. *Id.* at 19 (comment by Judge Ronald J. Hedges as to the use of the additional requirements).

resulting from the use of technology.⁸⁵ It should be noted, however, that authentication by an expert need not be overly burdensome. Courts recognize that experts who rely on computers for their exhibits, opinions, or testimony, need not be intimately familiar with why or how the computers or software used by the expert works, so long as additional foundations are laid.

In *Connecticut v. Foreman*,⁸⁶ a criminal defendant attempted to have his conviction overturned, in part, because the lower court wrongly admitted computer generated, but non-enhanced, fingerprint evidence.⁸⁷ As part of his argument, the defendant claimed that the state failed to properly authenticate the computer-generated evidence since the fingerprint expert did not know “how the software . . . manipulated or converted the images [of fingerprints], what the rate of error was in producing the images, or if there was any peer review of that scientific methodology.”⁸⁸ The court, relying upon Rule 901 and federal case law, rejected the defendant’s argument and found that the State had laid sufficient foundation for the admissibility of the evidence by showing the computer technology relied on by the witness was in use throughout the state, the expert was highly trained, the identification results were independently verified, and by way of the unique nature of fingerprints themselves.⁸⁹ The court concluded that the expert had sufficient knowledge of the processes to lay an adequate foundation, despite not knowing the algorithms utilized in the computer programs or of any published error rates for the program.⁹⁰

However, a word of caution on the use of experts; if relying on an expert to authenticate evidence, the expert and his or her opinions or proposed testimony should be disclosed pursuant to Federal Rule of Civil Procedure 26(a)(2).⁹¹ Failure to do so may make the expert’s testimony, and thereby the expert’s authentication, impermissible at trial. This was the lesson learned by counsel in *Insight Technology v. Surefire, LLC*,⁹² another post-*Lorraine* case, when defendant failed to identify the witness it was planning to use to authenticate computer animations in a patent case. Defendants attempted to argue that the failure was harmless

85. FED. R. EVID. 901(b)(3).

86. 954 A.2d 135 (Conn. 2008).

87. *Id.* at 157.

88. *Id.*

89. *Id.* at 160-62.

90. *Id.* at 161-62.

91. *See* FED. R. CIV. P. 26(a)(2).

92. Civ. No. 04-CV-74-JD, 2007 WL 3244092, at*2 (D.N.H. Nov. 1, 2007).

because the proffered animations “depict devices which are well known to [plaintiff] and have been the subject of [the] litigation since the outset;” the animations only show the devices “more clearly.”⁹³ Plaintiff objected to the expert’s opinion claiming it was prejudiced by the lack of notice and did not have the chance to depose the expert.⁹⁴ The court agreed, and reasoned that plaintiff was indeed prejudiced because, in part, the animations showed the devices “more clearly.”⁹⁵ As a result, the expert’s testimony was stricken.⁹⁶ As for the animations, the court, citing to *Lorraine*, held that “[t]o be admissible, the animations must be authenticated by independent evidence or be self authenticating.”⁹⁷ But, in the absence of the expert’s testimony, “the animations are unauthenticated drawings of unauthenticated devices” and were held inadmissible and therefore not able to support the defendant’s motion for summary judgment.⁹⁸

6. Computer Animations and Simulations

As referenced by the *Insight Technology* court, computer animations are most often used by practitioners as demonstrative evidence “to illustrate and explain a witness’s testimony,”⁹⁹ and to be admissible, must be “authenticated by testimony of a witness with personal knowledge of the content of the animation, upon a showing that it fairly and adequately portrays the facts and that it will help to illustrate the testimony given in the case.”¹⁰⁰ Such a standard has been held to be applicable in both state¹⁰¹ and federal courts;¹⁰² however, when dealing

93. *Id.* at * 2.

94. *Id.*

95. *Id.*

96. *Id.*

97. *Id.* at *3 (citing FED. R. EVID. 901; *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 559 (D. Md. 2007)).

98. *Id.*

99. *Lorraine*, 241 F.R.D. at 559 (quoting *State v. Sayles*, 662 N.W. 2d 1, 9 (Iowa 2003)); accord *Insight Tech.*, 2007 WL 3244092, at *3 (citing *Lorraine*, 241 F.R.D. at 559).

100. *Insight Tech.*, 2007 WL 3244092, at *3 (quoting *Lorraine*, 241 F.R.D. at 559); see also *Lorraine*, 241 F.R.D. at 560 (stating that “the most frequent methods of authenticating computer animations [and simulations] are 901(b)(1) (witness with personal knowledge), and 901(b)(3) (testimony of an expert witness)”).

101. See, e.g., *Tull v. Fed. Express Corp.*, 197 P.3d 495, 500 (Okla. Civ. App. 2008) (noting a computer animation used as a demonstrative aid must be a fair and accurate representation of the evidence to which it relates, it must be relevant, and its probative value must not be substantially outweighed by the danger of unfair prejudice, confusion of the issues, misleading the jury, undue delay, needless presentation of cumulative evidence, or unfair and harmful surprise); see also

with the *authenticity* and *admissibility* of computer simulations, practitioners should recognize the use of different standards in state and federal courts. Although this point was briefly alluded to in *Lorraine*, the next section of this Article will provide elaboration not contained in *Lorraine* to help bring the case forward, and provide a more thorough commentary on the law covering the admissibility of computer simulations.¹⁰³

Unlike computer animations, which are offered into evidence for demonstrative purposes, computer simulations are a form of scientific evidence offered for substantive purposes.¹⁰⁴ “[S]ubstantive evidence has independent probative value and can be used by an expert as the basis of the expert’s opinion,” and, as a result, is subject to more stringent reliability “tests.”¹⁰⁵ Depending on the court in which the proponent of the computer simulation was operating, such tests would include either the standards elicited in *Frye v. United States*,¹⁰⁶ Federal Rule of Evidence 702, and *Daubert v. Merrell Dow Pharmaceuticals*,

Lorraine, 241 F.R.D. at 560 (citing *People v. Cauley*, 32 P.3d 602 (Colo. App. 2001); *Clark v. Cantrell*, 529 S.E.2d 528, 536 (S.C. 2000)).

102. See, e.g., *Colgan Air, Inc. v. Raytheon Aircraft Co.*, 535 F. Supp. 2d 580, 583-84 (E.D. Va. 2008) (noting “demonstrative aids,” including “computer animations,” are authenticated based on testimony from a witness that they are substantially accurate representations of what that witness is trying to describe) (citation omitted)); *Insight Tech.*, 2007 WL 3244092, at *3; *Lorraine*, 241 F.R.D. at 559 (“The use of computer animations is allowed when it satisfies the usual foundational requirements for demonstrative evidence. At a minimum, the animation’s proponent must show the computer simulation fairly and accurately depicts what it represents, whether through the computer expert who prepared it or some other witness who is qualified to so testify, and the opposing party must be afforded an opportunity for cross-examination.”) (quoting *Friend v. Time Mfg. Co.*, No. 03-343-TUC-CKJ, 2006 WL 2135807, at *7 (D. Ariz. July 28, 2006) (internal quotation marks omitted)).

103. One student commentator has posited that *Lorraine* does not effectively differentiate between state and federal law when discussing the admissibility of computer simulations. See Lindsay Kemp, Comment, *Lorraine v. Markel: An Authoritative Opinion Sets the Bar for Admissibility of Electronic Evidence (Except for Computer Animations and Simulations)*, 9 N.C. J. L. & TECH. 16, 27 (2007) (“However, *Lorraine* hardly mentioned that the rules of admitting scientific evidence [in federal court] are governed by Federal Rules of Evidence 702 and 703, and this omission could be confusing to a lawyer looking to *Lorraine* as an authoritative and all-inclusive guide.”) (footnote omitted); but see *Lorraine*, 241 F.R.D. at 560-61 (stating that “[u]se of an expert witness to authenticate a computer simulation likely will also involve Federal Rules of Evidence 702 and 703”).

104. *Lorraine*, 241 F.R.D. at 560 (citing WEINSTEIN & BERGER, *supra* note 78, § 900.03[1], at 900-21; IMWINKELRIED, EVIDENTIARY FOUNDATIONS, § 4.09[4][a], [c] (2002 Lexis)); see also Hon. Paul W. Grimm & Claudia Diamond, *Low-Tech Solutions to High-Tech Wizardry: Computer Generated Evidence*, 37 MD. B.J. 5, 9-10 (2004).

105. WEINSTEIN & BERGER, *supra* note 78, § 900.07[d][ii], at 900-123.

106. 293 F. 1013 (App. D.C. 1923).

Inc.,¹⁰⁷ or some variation thereof.¹⁰⁸ Whereas a court relying on the *Frye* analysis must see if a novel theory and method used by the expert witness have been generally accepted within the relevant scientific community,¹⁰⁹ a court using a Rule 702 and/or *Daubert* analysis must determine whether the testimony, regardless of novelty, is based on sufficient facts or data, is the product of reliable principles and methods, and the witness applied the principles and methods reliably to the facts of the case.¹¹⁰

For example, in *State v. Sipin*,¹¹¹ a defendant and his co-passenger were allegedly traveling in the defendant's vehicle at a high rate of speed when the vehicle suddenly collided with a mailbox and a large tree.¹¹² As a result of the crash, the defendant suffered from permanent brain damage, and the co-passenger died from injuries sustained in the crash.¹¹³ The State charged the defendant with vehicular homicide, but there was a genuine dispute as to whether the defendant or the co-passenger had been driving the vehicle at the time of the crash; when local neighbors approached the accident scene, they noticed that both men had been ejected from the car, and neither was present in the driver's seat.¹¹⁴ The co-passenger was found on the ground between the passenger-side door and the tree, with only one foot in the car, and the defendant was found about ten to fifteen feet behind the vehicle.¹¹⁵

In order to prove the defendant was the driver of the vehicle at the time of the crash, the State sought to admit into evidence a computer simulation generated by the "PC-CRASH" program, as well as the

107. 509 U.S. 579 (1993) (adopting the standard for admission of expert testimony set forth in Rule 702).

108. See Alice B. Lustre, Annotation, *Post-Daubert Standards for Admissibility of Scientific and Other Expert Evidence in State Courts*, 90 A.L.R.5th 453 (2001) (providing an exhaustive compilation of the various evidentiary standards used by particular courts).

109. *Frye*, 293 F. at 1014.

110. FED. R. EVID. 702; see also FED. R. EVID. 702 advisory committee's notes to the 2000 amendments ("*Daubert* set forth a non-exclusive checklist for trial courts to use in assessing the reliability of scientific expert testimony. The specific factors explicated by the *Daubert* Court are (1) whether the expert's technique or theory can be or has been tested . . . ; (2) whether the technique or theory has been subject to peer review and publication; (3) the known or potential rate of error of the technique or theory when applied; (4) the existence and maintenance of standards and controls; and (5) whether the technique or theory has been generally accepted in the scientific community.").

111. 123 P.3d 862 (Wash. Ct. App. 2005).

112. *Id.* at 864.

113. *Id.* at 865.

114. *Id.* at 864.

115. *Id.*

accompanying testimony by the State's PC-CRASH expert witness.¹¹⁶ In response, the defendant asserted that the computer generated evidence was inadmissible under *Frye*, and the trial court conducted a *Frye* hearing to determine the admissibility of the PC-CRASH simulation and the expert witness's testimony.¹¹⁷

During the *Frye* hearing, the expert witness testified that the PC-CRASH simulation program involved "'inputting' variables from the scene and the vehicle, such as steering, braking, and speed, [which] would create a predictive image of the vehicle movement, based on the laws of physics."¹¹⁸ The expert could not provide any validation studies that had been done on the use of the PC-CRASH program to simulate the movement of a human body within the *interior* of a vehicle during a car accident; however, the expert asserted that such simulations would be identical to PC-CRASH system principles used to predict interaction between a human body and the *exterior* of a vehicle.¹¹⁹

At the conclusion of the *Frye* hearing, the trial court admitted the PC-CRASH system into evidence, and permitted the expert witness to testify at trial.¹²⁰ The defendant was convicted, and subsequently appealed.¹²¹ On appeal, he contended that the PC-CRASH system had not been validated for the use exercised by the expert witness in reconstructing the accident.¹²²

In its analysis, the Court of Appeals of Washington initially recounted the standard under *Frye* to address the admissibility of computer simulations as substantive evidence:

Jurisdictions that have addressed the issue uniformly hold that the admissibility of computer-generated models or simulations (as opposed to animations) as substantive proof or as the basis for expert testimony regarding matters of substantive proof is conditioned upon a sufficient showing that (1) the computer is functioning properly; (2) the input and underlying equations are sufficiently complete and accurate (and disclosed to the opposing party so that they can be challenged); and (3) the program is generally accepted by the appropriate community of scientists for use in the particular situation at hand. *We agree with these courts, and hold that . . . computer-generated simulations used as*

116. *Id.* at 865.

117. *Id.*

118. *Id.*

119. *Id.*

120. *Id.* at 866.

121. *Id.*

122. *Id.*

*substantive evidence or as the basis for expert testimony regarding matters of substantive proof must have been generated from computer programs that are generally accepted by the appropriate community of scientists to be valid for the purposes at issue in the case.*¹²³

The appellate court found that the PC-CRASH computer simulation did not meet the requirements of *Frye* due to the two post-trial declarations provided by the defendant, three scholarly papers, and manuals for the PC-CRASH program that all suggested that there was a “lack of consensus in the relevant scientific community” regarding the use of the PC-CRASH program by the State.¹²⁴ It should be noted that although the *Sipin* court purportedly applied the *Frye* test and its central focus of general acceptance within the relevant scientific community, the three-factor test the court embraced was more akin to the post-*Daubert* version of Rule 702. Specifically, the examination of sufficiently complete input (i.e., sufficient underlying facts), and that the underlying equations used by the computer program as part of its analysis are sufficiently complete and accurate (i.e., reliable methods and principles). Accordingly, the analysis applied by the court, which is more detailed

123. *Id.* at 868-69 (emphasis added) (citations omitted); *see also* Ruffin *ex rel.* Sanders v. Boler, 890 N.E.2d 1174, 1181, 1187 (Ill. App. Ct. 2008) (addressing admissibility of computer simulation to “describe the contact forces that are experienced between [an] infant’s shoulder and the maternal pelvis during labor”); State v. Phillips, 98 P.3d 838, 842-43 (Wash. Ct. App. 2004) (addressing admissibility of PC-CRASH computer simulation to predict movement of a vehicle in a single-impact crash). The three-factor test mentioned by the *Sipin* court is drawn from *Commercial Union Insurance Co. v. Boston Edison Co.*, 591 N.E.2d 165, 168 (Mass. 1992), which, as suggested by *Lorraine*, is often used by courts following *Frye* to gauge the admissibility of computer simulations as substantive evidence. *See* Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 560 (D. Md. 2007) (citing *Commercial Union*, 591 N.E.2d at 168; *Bray v. Bi-State Dev. Corp.*, 949 S.W.2d 93 (Mo. Ct. App. 1997); *Kudlacek v. Fiat*, 509 N.W.2d 603 (Neb. 1994)); *see also* State v. Clark, 655 N.E.2d 795, 812 (Ohio App. Ct. 1995) (“[W]hile the third prong of the test invokes the *Frye* test, which has been rejected in Ohio, we believe the fact that other jurisdictions, including our own, allow for the admission of computer-generated simulations or reconstructions speaks for the reliability of such simulations within the relevant technical community.” (citations omitted)). Interestingly, as with the *Commercial Union* court, the *Sipin* court did not question whether the computer running the simulation program was running properly, or the input and underlying equations were accurate. *See Sipin*, 123 P.3d at 868-69; *Commercial Union*, 591 N.E.2d at 168; *but see Bray*, 949 S.W.2d at 97-98 (“Courts have not required the first requirement of the *Commercial Union* guideline, that the computer be functioning properly, to be affirmatively shown in the absence of any challenge thereto. . . . With respect to the second *Commercial Union* guideline, cases generally require that the accuracy of the input be established. However, the relevant technical or scientific community’s use of or reliance on such software has been held sufficient to establish the accuracy of the software.”) (citations omitted)).

124. *Sipin*, 123 P.3d at 870.

than the language in *Frye* itself, would result in the same outcome as if Rule 702/*Daubert* had been used.

By contrast, in *Turner v. Liberty Mutual Fire Insurance Company*,¹²⁵ the plaintiff sued his insurer, defendant Liberty Mutual, for allegedly breaching an insurance contract after the defendant failed to pay insurance proceeds to the plaintiff after a fire destroyed his home.¹²⁶ The defendant countered that the plaintiff was solely responsible for the destruction of his home.¹²⁷ To justify its contention, the defendant sought to have an expert witness testify at trial regarding two reports.¹²⁸ The first report concluded “the fire evolution could not have developed as rapidly as it did without the introduction of accelerants into the floor surfaces of the home.”¹²⁹ The second report, which was based on various computer simulations, noted that the fire would still have to “be classified as incendiary.”¹³⁰ To prevent the expert from testifying, the plaintiff filed a motion *in limine*, and the U.S. District Court, Northern District of Ohio, relying on Rule 702 and *Daubert*, analyzed the admissibility of the computer simulations used as the underlying basis for the expert’s report.¹³¹ Through its analysis, the court unquestionably found the computer simulations to be inherently *reliable*, and therefore admissible under Rule 702 and *Daubert*: the software was found to have been sufficiently tested, was adequately subject to peer review and publication, had known error rates for the court to consider, and the computer simulation methodology was generally accepted by the relevant scientific community.¹³²

Reading the *Sipin* and *Turner* cases in tandem, the lesson to be learned is, be it under *Frye* or the Rule 702/*Daubert* approach, courts recognize that when computer simulations, as opposed to animations, are offered into evidence, proponents must satisfy the authentication requirements of Rule 901, and also must demonstrate that the evidence is reliable. Under Rule 702/*Daubert*, this requires including evidence of a sufficient factual basis, as well as proof that the analytical methodology

125. No. 4:07-cv-00163, 2007 WL 2713062 (N.D. Ohio Sept. 14, 2007).

126. *Id.* at *1.

127. *Id.*

128. *Id.*

129. *Id.*

130. *Id.*

131. *Id.* at *2-3.

132. *Id.* at *3-4. See also *Silong v. United States*, No. CV F 06-0474 LJO DLB, 2007 WL 2535126, at *1-3 (E.D. Cal. Aug. 31, 2007) (applying *Daubert* factors to computer model displaying potential injury to child during birth).

used by the computer program is reliable and based on reliable principles. Similarly, under a *Frye* analysis, courts are not likely to adopt mere conclusory statements from the witness who performed the simulation that experts in the same field have generally accepted, but, instead, will demand evidence that demonstrates sufficient factual “input,” and that the program itself is “valid,” meaning that the analysis that it performs is the product of reliable methodology. It should be kept in mind that the approach taken by the courts regarding admissibility of computer simulations conjoins the standards governing authentication under Rules 901 and 902 with the expert witness rules under Rules 702-704, and thus an expert witness likely will be required to authenticate the computer simulation.

B. Rule 902

For purposes of authentication, Rule 902 is markedly different from its counterpart, Rule 901, under the Federal Rules of Evidence. Rule 902 provides that extrinsic evidence of authentication as a pre-condition to admissibility is not required for certain types of proffered materials; therefore, the requirement of Rule 901 that the exhibit must be shown to be what it purports to be will be automatically met if the exhibit falls into any of the classifications listed under Rule 902.¹³³ The benefit of this rule is easily apparent—by having an exhibit be “self-authenticating,” it dispenses with the need of having an authenticating witness come to trial and testify to her knowledge of and familiarity with an exhibit. With countless documents and records now available online, the application of Rule 902 to the digital realm stands to be a boon for any given proponent of a particular exhibit, although, surprisingly, lawyers and courts have been slow to take advantage of it.

Lorraine recognized that Rule 902, in its entirety, could provide for the self-authentication of ESI, and explicitly noted Rules 902(5), 902(7), and 902(11) as permitting self-authentication of electronic records.¹³⁴ Of the three rules, Rule 902(5), which permits self-authentication of official records, has been most readily used by other courts to justify the self-authentication of official records posted on the websites of public authorities.

133. FED. R. EVID. 902.

134. See *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 551 (D. Md. 2007) (citing FED. R. EVID. 902(5), (7) & (11)).

1. Self-Authentication of Official Publications under Rule 902(5)

Rule 902(5) provides for the self-authentication of “[o]fficial publications,” which could include “[b]ooks, pamphlets, or other publications purporting to be issued by public authority.”¹³⁵ With this point in mind, and relying on the ruling in *Equal Employment Opportunity Commission v. E.I. DuPont de Nemours and Co.*,¹³⁶ the *Lorraine* court noted that printed web pages from websites of public authorities would qualify as self-authenticating “official publications” under Rule 902(5).¹³⁷ Taking into account the frequency with which official publications from government agencies could impact pending litigation, as well as the increasing tendency for such agencies to have their own websites, Rule 902(5) could now be seen as providing a convenient avenue for authenticating such publications.¹³⁸

Most recently, in *Williams v. Long*,¹³⁹ the United States District Court for the District of Maryland determined whether printed web pages from various Maryland State government websites could qualify as self-authenticating official publications under Rule 902(5). In the case, the plaintiffs alleged that their employer, the defendant, violated the Fair Labor Standards Act (“FLSA”)¹⁴⁰ by failing to compensate the plaintiffs at the minimum wage and provide overtime pay.¹⁴¹ The plaintiffs subsequently moved to conditionally certify a collective action, and sought approval and facilitation of a notice to class members potentially interested in joining the suit.¹⁴² In order to justify the certification, the plaintiffs would have to prove there were other individuals “similarly situated” to the plaintiffs; therefore, plaintiffs’ counsel attached five exhibits to the plaintiffs’ motion for certification, which detailed the defendant’s alleged actions against those similarly situated to the instant plaintiffs.¹⁴³

135. FED R. EVID. 902(5).

136. No. Civ.A. 03-1605, 2004 WL 2347559, *1-2 (E.D. La. Oct. 18, 2004) (holding printed webpage from the website of the U.S. Census Bureau as self-authenticating under Rule 902(5)).

137. *Lorraine*, 241 F.R.D. at 551 (citing *E.I. DuPont*, 2004 WL 2347556).

138. *Id.*

139. 585 F. Supp. 2d 679 (D. Md. 2008).

140. 29 U.S.C. § 201 (2008).

141. *Williams*, 585 F. Supp. 2d at 681.

142. *Id.*

143. *Id.* at 682 (citing 29 U.S.C. §216(b) (West 2008)) (outlining the requirements for certification of a class action under the FLSA).

The court noted that two of the five exhibits consisted of printed web pages from websites.¹⁴⁴ The plaintiffs' first exhibit was printed web pages from the Maryland Judiciary Case search website,¹⁴⁵ which had not been authenticated by any attached affidavit or extrinsic evidence.¹⁴⁶ A reading of the web pages revealed that there were three pending lawsuits against the defendant in the Baltimore City District Court; however, the suits were only described as "Contract" claims, and failed to address the facts of each particular suit.¹⁴⁷ Additionally, the plaintiffs' third exhibit featured printed case search results from the Employment Standards Service of the Division of Labor and Industry, in the Maryland Department of Labor, Licensing and Regulation.¹⁴⁸ The search results showed there were four closed claims against the defendant, but not did mention the facts of each particular claim, and were also not authenticated by any affidavit or extrinsic evidence.¹⁴⁹ The court went on to consider each website that hosted the particular web pages and found that access to the information contained in the Employment Standards Service web pages was not available without an employee e-mail address and password.¹⁵⁰ At a subsequent hearing on the plaintiffs' motion, plaintiffs' counsel proffered that he had obtained the information contained in the third exhibit through a request for records under the Maryland Public Information Act.¹⁵¹

Before addressing the applicability of Rule 902(5) to the plaintiffs' submitted web pages, the *Williams* court defined the applicability of Rule 902(5) to any information posted on the Internet.¹⁵² This resulted in the court analyzing how a "public authority" was defined under the rule, as well as an "other publication."¹⁵³ First, the court noted that "Rule 902(5) [was] silent on what level of government must authorize the publication";¹⁵⁴ however, "Rule 902(5) [was] most often construed to cover the governmental bodies listed in [Rule 902(1)], which provides for self-authentication of domestic publication documents under

144. *Id.* at 682-83.

145. *Id.* at 682.

146. *Id.*

147. *Id.*

148. *Id.*

149. *Id.*

150. *Id.* at 683.

151. *Id.*

152. *See id.* at 685-87.

153. *Id.* at 686-87.

154. *Id.* at 686 (quoting WEINSTEIN & BERGER, *supra* note 78, § 902.07[1], at 902-29).

seal.”¹⁵⁵ As a result, the following entities would be regarded as public authorities: “(1) the United States, (2) any State, (3) any district, commonwealth, territory, or insular possession of the United States, (4) the Panama Canal Zone, (5) the Trust Territory of the Pacific Islands, [and] (6) a political subdivision, department, officer, or agency of any of the preceding bodies.”¹⁵⁶ The universe of public authorities, thus, is broad. Second, the court remarked that Rule 902(5) would cover the self-authentication of “‘statute books and case reports,’ as well as ‘legislative reports, published transcripts of hearings, maps and surveys, collected statistics, commissioned studies, manuals,’ and other data compilation publications from public authorities.”¹⁵⁷

With these two points in mind, *Williams* recognized that courts were accepting “the posting of information on a website sponsored by a public authority [as] the functional equivalent of publication” under Rule 902(5).¹⁵⁸ Accordingly, postings on “government websites” were

155. *Id.*; see also FED. R. EVID. 902(1).

156. *Williams*, 585 F. Supp. 2d at 686 (quoting WEINSTEIN & BERGER, *supra* note 78, § 902.07[1], at 902-30 & n.4).

157. *Id.* at 686-87 (quoting CHRISTOPHER B. MUELLER & LAIRD C. KIRKPATRICK, FEDERAL EVIDENCE § 9:34, at 589 (3d ed. 2007); see also MUELLER & KIRKPATRICK, *supra*, § 9:34, at 589 n.4 (citing *Gregg v. Forsyth*, 65 U.S. 179 (1860) (authentication of papers contained in volumes of American State Papers); *Watkins v. Holman’s Lessee*, 41 U.S. 25, 39 (1842) (authentication of “volume of state papers published . . . under an act of congress”); *United States v. Aluminum Co. of Am.*, 1 F.R.D. 71, 74 (S.D.N.Y. 1939) (authentication of a “public document, lawfully printed at the Government Printing Office in obedience to a valid order made by the Senate”); *United States v. Shafer*, 132 F. Supp. 659, 665 (D. Md. 1955), *aff’d*, 229 F.2d 124 (4th Cir. 1956) (authentication of documents published in the Federal Register); *Stewart v. United States*, 211 F. 41, 45 (9th Cir. 1914) (authentication of a map from the General Land Office)); *Williams*, 585 F. Supp. 2d at 687 (citing *Conjour v. Whitehall Twp.*, 850 F. Supp. 309, 312 n.1 (E.D. Pa. 1994) (self-authentication of local ordinances and regulations); *Biggers ex. rel. Key v. S. Ry. Co.*, 820 F. Supp. 1409, 1415 (N.D. Ga. 1993) (self-authentication of a certified copy of a state map issued by the Georgia Department of Transportation)).

158. *Williams*, 585 F. Supp. 2d at 687 (citing *Sannes v. Jeff Wyler Chevrolet, Inc.*, No. C-1-97-930, 1999 WL 33313134, at *3 n.3 (S.D. Ohio Mar. 31, 1999) (recognizing the Federal Trade Commission (“FTC”), an agency of a governmental body, as a public authority, and thereby determining information published on the FTC’s website to be self-authenticating); *Hispanic Broad. Corp. v. Educ. Media Found.*, No. CV027134CAS (AJWX), 2003 WL 22867633, at *5 n.5 (C.D. Cal. Oct. 30, 2003) (“[E]xhibits which consist of records from government websites, such as the FCC website, are self-authenticating.”); *Shell Oil Co. v. Franco*, No. CV 03-8846 NM (PJWx), 2004 WL 5615656, at *5 n.7 (C.D. Cal. May 18, 2004) (noting “records from government websites are self-authenticating,” and permitted a plaintiff to introduce internet reports from the U.S. State Department website); *Estate of Gonzales v. Hickman*, No. ED CV 05-660 MMM (RCx), 2007 WL 3237727, at *2 n.3 (C.D. Cal. May 30, 2007) (finding the Office of the Inspector General’s report to be self-authenticating based on availability on the Internet)).

deemed to be “inherently authentic.”¹⁵⁹ *Williams* also noted the following:

A proponent of ESI could use the [uniform resource locator], date, and/or official title on a printed webpage to show that the information was from a public authority’s website, and therefore, self-authenticating. . . . [T]he public authority’s selection of the posted information for publication on its website [would act] as the necessary “seal of approval” needed to establish that the information came from a public authority for purposes of Rule 902(5).¹⁶⁰

Through this method, the court found the printed web pages from the Maryland Judiciary Case Search and Employment Standards Service websites to be self-authenticating.¹⁶¹ Although access to the webpage from the Employment Standards Service website was limited by security measures, the court cautioned that it was important not to confuse “‘publication,’ as used by Rule 902(5), with ‘unrestricted publication to the general public.’”¹⁶² Rule 902(5) contains no requirement that information must be readily available to the public, and simply because additional measures, such as a subpoena or request or records, would have to be employed to gain access to a publication does not mean that

159. *Williams*, 585 F. Supp. 2d at 687. One court has, however, found that the *type* of information found on a website may affect whether the information itself can be found to be self-authenticating under Rule 902(5). See *In re Poirier*, 346 B.R. 585, 588-89 (Bankr. D. Mass. 2006) (declining to take judicial notice of information posted on the Department of Education’s (“DOE”) website because there were too many links to various “documents” which could not be reasonably identified as “official records,” “reports,” or a “publication issued by a public authority”); *but see Williams*, 585 F. Supp. 2d at 688 n. 4 (“The correctness of the conclusion reached by the *In re Poirier* court is questionable. Rule 902(5) provides for self-authentication of ‘other publications,’ and it is the act of posting information on the Internet by a qualifying public authority that *is* the act of publication. Because the DOE is a department of one of the governmental bodies listed in Rule 902(1), then the DOE would also be considered a public authority. Thus, when the DOE *posted* information on its site, it vouched for its authenticity, thereby making it self-authenticating under Rule 902(5). There is nothing in the rule that states the public authority publishing the information (whether in print form, or online) must originate the information posted. Rather, the publication must have actually been approved by the public authority, or, as some would say, ‘made official.’ Thus, the information’s adoption by reference by the public authority seems sufficient to meet the requirements of Rule 902(5).”).

160. *Williams*, 585 F. Supp. 2d at 689; *see also, e.g., Schaghticoke Tribal Nation v. Kempthorne*, No. 3:06-cv-00081 (PCD), 2008 WL 4000179, at *3 (D. Conn. Aug. 26, 2008) (finding Government press release to be self-authenticating because petitioner included the web address for the press release in its Local Rule 56(a)(1) statement, thereby allowing the court to verify that the press release was a copy of an official document issued by a public authority).

161. *Williams*, 585 F. Supp. 2d at 689.

162. *Id.* at 689-90.

the publication could not be self-authenticating.¹⁶³ Thus, if information was published on a website by a public authority, and that information was obtained pursuant to a federal or state freedom of information act, then that printed information would in fact be self-authenticating under Rule 902(5).¹⁶⁴

2. Self-Authentication of Inscriptions under Rule 902(7)

Rule 902(7) permits the self-authentication of “[i]nscriptions, signs, tags, or labels purporting to have been affixed in the course of business and indicating ownership, control, or origin.”¹⁶⁵ As noted by one commentator, “‘business e-mails often contain information showing the origin of the transmission and identifying the employer-company.’”¹⁶⁶ Therefore, “[t]he identification marker alone may be sufficient to authenticate an e-mail under Rule 902(7).”¹⁶⁷ However, simply because an individual’s sending address is present on an e-mail does not constitute definitive proof that the person actually sent the e-mail, and authentication of an e-mail could still possibly require testimony from a person with personal knowledge of the transmission or its receipt to ensure its trustworthiness.¹⁶⁸

At this time, no case since *Lorraine* has discussed the use of Rule 902(7) to gauge the authenticity of an e-mail. Nevertheless, at least one court has implicitly recognized the authenticity of an e-mail based on the identity of its author. In *Sklar v. Clough*,¹⁶⁹ students at the Georgia Institute of Technology filed suit against various Georgia Tech officials, alleging that Georgia Tech was banning the use of students’ activities fees for religious and political activities, and unconstitutionally establishing a specific religious view with the school’s “Safe Space Program.”¹⁷⁰ In their opposition to the students’ motion for summary

163. *Id.*

164. *Id.*; *c.f. id.* (citing *Wolf Lake Terminals, Inc. v. Mut. Marine Ins. Co.*, 433 F. Supp. 2d 933, 944 (N.D. Ind. 2005) (discussing the self-authentication of two U.S. Government documents obtained through the FOIA); *Schmutte v. Resort Condos. Int’l, LLC*, No. 1:05-cv-0311-LJM-WTL, 2006 WL 3462656, at *14 (S.D. Ind. Nov. 29, 2006) (discussing the self-authentication of Department of Labor file produced pursuant to a FOIA request)).

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

166. *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 551-52 (D. Md. 2007) (quoting WEINSTEIN & BERGER, *supra* note 78, § 900.07[3][c], at 900-105).

167. *Id.* at 552 (quoting WEINSTEIN & BERGER, *supra* note 78, § 900.07[3][c], at 900-105).

168. WEINSTEIN & BERGER, *supra* note 78, § 900.07[3][c][i], at 900-105.

169. No. 1:06-CV-0627-JOF, 2007 WL 2049698 (N.D. Ga. July 6, 2007).

170. *Id.* at *1.

judgment, the officials contended that various attached exhibits had “not been properly authenticated, [were] hearsay, and [were] not otherwise admissible at trial.”¹⁷¹ In particular, officials sought to exclude various e-mails from school officials that purportedly detailed the extent of the involvement of the Georgia Tech administration with the Safe Space Program.¹⁷² Without relying on Rule 902(7), the court did find the e-mails to be “authenticated,” mainly “because they were produced by [the school officials] in the litigation.”¹⁷³ Other courts have frequently held that if a document is produced by an opposing party during discovery, then it is sufficiently authenticated, and will qualify as an admission of a party opponent, thereby qualifying the document as non-hearsay under Rule 801(d)(2).¹⁷⁴ As a result, a proponent of an e-mail, which had been sent in the regular course of business, could rely on an identification marker to prove the e-mail came from a party opponent, thereby guaranteeing its authenticity and admissibility.

3. Self-Authentication of Domestic Records under Rule 902(11)

Rule 902(11) provides for the following:

(11) Certified domestic records of regularly conducted activity. The original or a duplicate of a domestic record of regularly conducted activity that would be admissible under Rule 803(6) if accompanied by a written declaration of its custodian or other qualified person, in a manner complying with any Act of Congress or rule prescribed by the Supreme Court pursuant to statutory authority, certifying that the record:

(A) was made at or near the time of the occurrence of the matters set forth by, or from information transmitted by, a person with knowledge of those matters;

(B) was kept in the course of the regularly conducted activity; and

(C) was made by the regularly conducted activity as a regular practice.

A party intending to offer a record into evidence under this paragraph must provide written notice of that intention to all adverse parties, and must make the record and declaration available for inspection

171. *Id.*

172. *Id.*

173. *Id.* at *5.

174. *See, e.g.,* Sea-Land Serv., Inc. v. Lozen Int'l, 285 F.3d 808, 821-22 (9th Cir. 2002); Snyder v. Whittaker Corp., 839 F.2d 1085, 1089 (5th Cir. 1988); Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 454 F. Supp. 2d 966, 972 (C.D. Cal. 2006); *In re Homestore.com, Inc.*, 347 F. Supp. 2d 769, 781 (C.D. Cal. 2004). For a more thorough discussion on hearsay in an ESI context, see *infra* Part IV.

sufficiently in advance of their offer into evidence to provide an adverse party with a fair opportunity to challenge them.¹⁷⁵

As recognized by the *Lorraine* court, compliance with Rule 902(11) requires a proponent of electronic evidence to establish all the elements of the business record exception to the hearsay rule; therefore, courts usually analyze an authenticity issue under Rule 902(11) concomitantly with the business record exception under Rule 803(6).¹⁷⁶ First, in *Rambus, Inc. v. Infineone Technologies AG*,¹⁷⁷ a plaintiff computer memory systems designer filed suit against a defendant manufacturer for patent infringement.¹⁷⁸ After the judgment in the trial was appealed, affirmed, and reversed in part, the case was remanded.¹⁷⁹ On remand, the defendant filed a motion *in limine* to preclude the plaintiff from entering into evidence fourteen third-party declarations, and 148 documents purportedly self-authenticated by the declarations through Rule 902(11).¹⁸⁰ In its analysis, the court noted the following:

[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) because the declaration permitted by Rule 902(11) serves the same purpose as authenticating testimony. Therefore, the declaration must satisfy the substantive criteria set forth in Rule 902(11) in order to lay a proper foundation for admission of the record.¹⁸¹

The court held that the declarations did not permit self-authentication of the business entity's records because the declarations failed to satisfy the requirements of Rule 902(11): the statements made no reference to the third-party's knowledge of the manufacturers' recordkeeping practices and whether the records were made by regularly conducted activity as regular practice.¹⁸²

Second, in *In re Vee Vinhnee*,¹⁸³ the appellate bankruptcy panel relied on a merged Rule 902(11) and 803(6) analysis to uphold the trial bankruptcy judge's decision to exclude evidence of electronic business

175. FED. R. EVID. 902(11).

176. *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 571-72 (D. Md. 2007).

177. 348 F. Supp. 2d 698 (E.D. Va. 2004).

178. *Id.* at 698.

179. *Id.* at 700.

180. *Id.*

181. *Id.* at 701.

182. *Id.* at 708.

183. 336 B.R. 437 (B.A.P. 9th Cir. 2005).

records.¹⁸⁴ The court's outcome hinged on the overall reliability of a declarant's statement authenticating the records; the court noted dissatisfaction with the declarant's knowledge of the hardware and software used to produce the information, and remarked that the declaration in no way established the declarant was "'qualified' to provide the requisite testimony[, and] . . . the declaration did not contain information sufficient to warrant a conclusion that the ' . . . computers [were] sufficiently accurate in the retention and retrieval of the information contained in the documents.'"¹⁸⁵ Further, the court remarked that a "'qualified' witness or person under Rules 803(6) and 902(11) need not be an expert," but there would have to "be enough information presented to demonstrate that the person is sufficiently knowledgeable about the subject of the testimony."¹⁸⁶ The court did not find that the declarant possessed the requisite knowledge, for he "merely asserted" that he was "personally familiar with the hardware and software computer record-keeping systems," and failed to "indicate his job title or anything about his training and experience that would import an aura of verisimilitude to his assertions."¹⁸⁷

Following *Lorraine*, one court found that a declarant's testimony failed to meet the requirements of Rule 902(11). In *United States v. Schultz*,¹⁸⁸ the defendant was charged with allegedly using a government credit card to purchase personal items. The defendant's lawyer contended that the defendant had committed the crimes because of mental health issues, which resulted from mistreatment she supposedly endured while training for and participating in the California National Guard.¹⁸⁹ As evidence, defense counsel wanted to submit, *inter alia*, statements the defendant allegedly posted on Craig's List discussing the alleged abuse.¹⁹⁰

The court initially declined to admit the defendant's statement into evidence, finding that that statement failed to meet the relevancy requirement under Rule 402.¹⁹¹ Afterwards, the United States Government sought to have other sections of the Craig's List postings

184. *Id.* at 444-50.

185. *Id.* at 448.

186. *Id.*

187. *Id.*

188. No. Cr. S-07-76 KJM, 2008 WL 152132 (E.D. Cal. Jan. 16, 2008).

189. *Id.* at *1.

190. *Id.*

191. *Id.* (citing FED. R. EVID. 402).

admitted into evidence,¹⁹² and at a subsequent hearing, the court had to determine whether these sections were self-authenticating under Rule 902(11)(A).¹⁹³ Citing *Rambus* and *United States v. Childs*,¹⁹⁴ the court found that the sections were not self-authenticating; the Government could not prove, “given the nature of the Craig’s List postings,” that the records had been “made at or near the time of the occurrence of the matters set forth by, or from information transmitted by, a person with knowledge of those matters.”¹⁹⁵

4. Self-Authentication of ESI under Rules 902(4) and 902(6)

Although not specifically addressed in *Lorraine*,¹⁹⁶ courts have begun to analyze the self-authentication of ESI under Rules 902(4) and 902(6).

a. Rule 902(4)

Rule 902(4) provides for self-authentication of the following:

A copy of an official record or report or entry therein, or of a document authorized by law to be recorded or filed and actually recorded or filed in a public office, including data compilations in any form, certified as correct by the custodian or other person authorized to make the certification, by certificate complying with paragraph (1), (2), or (3) of this rule or complying with any Act of Congress or rule prescribed by the Supreme Court pursuant to statutory authority.¹⁹⁷

The primary purpose of Rule 902(4) is to make it unnecessary to remove original records from their official custody for litigation, for modern copying methods and the integrity of those certifying the copies offer some assurance against the possibilities of mistake or fraud.¹⁹⁸ Also, Rule 902(4)’s reference to “data compilations in any form” has been interpreted to include electronically stored or recorded data and

192. *United States v. Schultz*, No. Cr. S-07-76 KJM, 2008 WL 162164, at *2 (E.D. Cal. Jan. 17, 2008).

193. *Id.*

194. 5 F.3d 1328, 1333 (9th Cir. 1993) (stating that “exhibits can be admitted as business records of an entity, even when that entity was not the maker of those records, so long as the other requirements of Rule 803(6) are met and the circumstances indicate the records are trustworthy”).

195. *Schultz*, 2008 WL 162164, at *2 (quoting FED. R. EVID. 902(11)(A)).

196. *See* 241 F.R.D. 534 (D. Md. 2007).

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

198. MUELLER & KIRKPATRICK, *supra* note 157, §9:33, at 571.

computer output,¹⁹⁹ and at least one case preceding *Lorraine* has discussed whether an electronic record could be self-authenticating under Rule 902(4). In *Brewer v. United States*,²⁰⁰ the plaintiff failed to file tax returns for a number of years, prompting the Government to obtain liens on the plaintiff's property, issue levies, and seize and sell the plaintiff's property.²⁰¹ Instead of challenging the merits of the tax assessments, the plaintiff brought suit to quiet title of his past wages, an annuity fund, and property in Florida and New York.²⁰² In response, the Government filed a motion to dismiss.²⁰³

The court granted the Government's motion, and in doing so, relied on information contained in an Internal Revenue Service Form 4340, Certificate of Assessments and Payments, which was originally submitted by the Government as an attachment to the motion.²⁰⁴ The plaintiff had moved to strike the document, arguing that it was improperly authenticated and inadmissible hearsay.²⁰⁵ The court declined to agree with the plaintiff, and noted that "Form 4340 [was] a compilation of data stored in a computer, reflecting entries into an official record."²⁰⁶ Additionally, the accompanying signature of a custodian "attest[ed] to the accuracy of the completed form," thereby making it "properly admissible under Rule 902(4)."²⁰⁷ Such a finding highlights an important point when relying on Rule 902(4) when self-authenticating ESI—as required by Rule 902(4), a proponent of ESI must still obtain a certificate of a custodian in order to ensure the information is true, accurate, and was properly recorded. If not, then the ESI will not fall under the purview of Rule 902(4), and as a result, will not be self-authenticating.²⁰⁸

199. *Id.* at 572; see also FED. R. EVID. 803(6) advisory committee's note to the 1972 proposed rules ("The expression 'data compilation' is used as broadly descriptive of any means of storing information other than the conventional words and figures in written or documentary form. It includes, but is by no means limited to, electronic computer storage.").

200. 764 F. Supp. 309 (S.D.N.Y. 1991).

201. *Id.* at 311.

202. *Id.*

203. *Id.* at 313.

204. *Id.* at 318.

205. *Id.*

206. *Id.*

207. *Id.*

208. See, e.g., *In re Lebbos*, No. 06-22225-D-7, 2008 WL 2474579, at *2 (Bankr. E.D. Cal. June 18, 2008).

b. Rule 902(6)

Rule 902(6) provides that printed materials, such as newspapers or periodicals, are self-authenticating.²⁰⁹ Contrary to the assertion made in *Lorraine*, one scholarly authority notes that because the rule references “printed” materials, it would be difficult to use Rule 902(6) to “authenticate electronic or hardcopy of material made available only over the Internet, such as Slate magazine, to wire service reports like Reuters.”²¹⁰ One could also argue that the proliferation of electronic records defeats the original purpose of the rule itself; self-authentication under Rule 902(6) was permissible because it seemed exceedingly difficult to forge a newspaper or periodical because of distinct appearance, typeset, logo, and other discernible characteristics,²¹¹ but with the accessibility of electronic versions of such newspapers and periodicals, it would be much easier craft forgeries through the technical advancements of photo-editing software and/or data manipulation.²¹² This troublesome, but perhaps resolvable aspect of relying on Rule 902(6) to self-authenticate ESI was recently mentioned in *Parikh v. Premera Blue Cross*:²¹³

The problem the Court now faces is the fact that all of the newspaper or other periodical articles submitted by Defendant appear to have been printed from an internet media search service. The original clippings, or even photocopies of the originals, are not provided. Instead, the Court has merely received what appears to be the purported text of the articles typed into and printed from a computer. *There are no distinctive headlines, nor are there any unique typesetting techniques employed that would make these purported copies of original text difficult to forge. Additionally, in many cases, the Court cannot tell from which internet service the documents were obtained. The Court questioned the Defense attorney about these documents at oral argument and he admitted to the Court that he had no personal knowledge regarding where these documents were found on the internet because he had an assistant obtain these documents for him.*

209. FED. R. EVID. 902(6).

210. SALTZBURG ET AL., *supra* note 20, § 902.02[4], at 902-10.

211. MUELLER & KIRKPATRICK, *supra* note 157, §9:35, at 592; *See, e.g., Goguen ex rel. Estate of Goguen v. Textron, Inc.*, 234 F.R.D. 13, 17 n.2 (D. Mass. 2006).

212. *See, e.g., Colin Miller, Even Better Than the Real Thing: How Courts Have Been Anything but Liberal in Finding Genuine Questions Raised as to the Authenticity of Originals under Rule 1003*, 68 MD. L. REV. 160, 207-209 (2008).

213. No. C01-0476P, 2006 WL 2841998, at *4 (W.D. Wash. Sept. 29, 2006).

*For these reasons, the Court must reject the articles submitted by Defendants as non-self-authenticating.*²¹⁴

In an ESI context, such a ruling is a proverbial two-sided coin; attorneys should be aware that they cannot simply use a word processing program to retype a periodical into a computer and expect a court to recognize the output as self-authenticating under Rule 902(6), but they should also recognize that the court has provided a rough framework as to how online accessible periodicals can be self-authenticating under the federal rules. First, a proponent would most likely have to show that the printout of the periodical came from the periodical's website—this could be done by making sure the URL appears at the top of the printed page. Second, the proponent would most likely have to show to the court that the webpage of the online periodical uses a specific or particular font, which is comparable to the practices of most paper periodicals. There would be, of course, additional considerations not considered by the *Parikh* court. When analyzing issues involving the definition of “periodicals” under Rule 902(6), courts often focus on the printing schedule of the article, magazine, or newsletter to establish if the written piece is truly a “periodical” in the classical sense.²¹⁵ Therefore, online versions of articles on the Newsweek website, which are posted on a predetermined basis, may soon be held to be self-authenticating under the rule, and a retyped article from a news blog will not. Given the changes that the newspaper industry presently is undergoing, “online” publications by former “print-based” publishers can be expected to grow exponentially. Lawyers and courts, therefore, will be called upon with greater regularity to rely on Rule 902(6) as a basis for authenticating these publications.

IV. THE HEARSAY RULE AND ITS EXCEPTIONS AS APPLIED TO ESI/DIGITAL EVIDENCE

Lorraine also discusses at length the special challenges presented by the hearsay rule when applied to ESI or digital evidence. As the opinion notes, the key to proper understanding of this issue hinges on a five-step analysis:

The fourth “hurdle” that must be overcome when introducing electronic evidence is the potential application of the hearsay rule.

214. *Id.* at *4 (emphasis added).

215. See *Goguen*, 234 F.R.D. at 17-18.

Hearsay issues are pervasive when electronically stored and generated evidence is introduced. To properly analyze hearsay issues there are five separate questions that must be answered: (1) does the evidence constitute a **statement**, as defined by Rule 801(a); (2) was the statement made by a **“declarant,”** as defined by Rule 801(b); (3) is the statement being offered to prove the **truth of its contents**, as provided by Rule 801(c); (4) is the statement **excluded from the definition of hearsay by rule 801(d)**; and (5) if the statement is hearsay, is it covered by one of the exceptions identified at Rules 803, 804 or 807. It is critical to proper hearsay analysis to consider each of these questions.²¹⁶

Lorraine explains that the core purpose of the hearsay rule is to ensure sufficient reliability of testimonial evidence that asserts the existence of facts and invites the finder of fact to accept them as true, and recognizes the four common law “testimonial risks” that the hearsay rule is designed to address: perception, memory, sincerity, and narration.²¹⁷ The hearsay rules accomplish this by insisting on the presence before the jury of the person making the assertions, so that his credibility may be assessed through testimony given under oath, tested by cross-examination, with the jury in a position to observe the demeanor of the witness during the process.²¹⁸ Central to this concept is the requirement in Rule 801(a) of a “statement,” which is a term of art with a specific meaning—written or spoken utterances (referred to as “verbal conduct”) as well as non-verbal conduct that is expressly intended by the actor to be assertive.²¹⁹ The *Lorraine* opinion notes the irony of the fact that despite its paramount importance to the operation of the hearsay rule, the word “assertion” is not defined by the Rule 801, but offers the following practical definition: “An assertion usefully may be defined as ‘to state as true; declare; maintain.’”²²⁰

The next requirement of the hearsay rule is that the statement be made by a human being, referred to by Rule 801(b) as the “declarant,” and this is particularly relevant to ESI/digital evidence, and the source of much confusion.²²¹ When ESI or digital evidence is produced from a computer or other electronic device, it may be either “computer

216. *Lorraine*, 241 F.R.D. at 562-63.

217. *Id.* at 563 (citing FED. R. EVID. 801 advisory committee’s note to the 1972 proposed rules).

218. *Id.*

219. *Id.* (citation omitted).

220. *Id.* (citing BLACK’S LAW DICTIONARY 106 (5th ed. 1979)).

221. *Id.* at 564-65.

generated” or “computer stored.”²²² The difference is significant for purposes of the hearsay rule, and George Paul’s recent treatise on digital evidence has explained it quite well:

[C]ourts and commentators have recognized a distinction between computer-generated and computer-stored evidence. If the system made the statement, it is “computer-generated.” If a person input a statement into the system that then preserved a record of it, it is “computer-stored” evidence. Underlying the distinction is the idea that computer-stored evidence is a repetition of data originally entered by a human language writer, while computer-generated evidence is the product of electronic processes, or the statements an information system makes in its reading and writing games.²²³

Thus, as *Lorraine* notes, if the electronic or digital evidence was not created by a human declarant, then it cannot constitute hearsay, and courts have repeatedly overruled hearsay objections aimed at excluding “assertive” statements generated by a computer or machine, not a human.²²⁴ Since *Lorraine*, courts have continued to recognize the requirement of a “human” declarant before factual statements generated by computers or other machines may be regarded as hearsay.²²⁵

While *Lorraine* and the cases cited in the opinion conclude that computer-generated statements do not constitute hearsay, they are quick to caution that this does not mean the evidence gets a “free pass” to admissibility. To the contrary, because the statements are computer- or machine-generated, they are only admissible if reliable, meaning that they must be the product of a system or process that is capable of

222. PAUL, *supra* note 5, at 115.

223. *Id.* at 115-16 (citing *Tatum v. Commonwealth*, 440 S.E.2d 133 (Va. Ct. App. 1994)).

224. *Lorraine*, 241 F.R.D. at 564-65 (citing *United States v. Khorozian*, 333 F.3d 498, 506 (3d Cir. 2003) (header of a faxed document not hearsay because hearsay rule requires that the statement be “uttered by ‘a person,’” so nothing “said” by a machine is hearsay); *United States v. Rollins*, No. ACM34515, 2004 WL 26780, at *9 (A.F. Ct. Crim. App. Dec. 24, 2003) (computer generated records are not hearsay), *rev’d in part on other grounds*, 61 M.J. 338 (C.A.A.F. 2005); *State v. Dunn*, 7 S.W.3d 427, 432 (Mo. Ct. App. 2000) (computer generated billing record not hearsay); *State v. Hall*, 976 S.W.2d 121, 147 (Tenn. 1998) (computer generated records are not hearsay because they are not statements of a witness)).

225. *See, e.g., United States v. Washington*, 498 F.3d 225, 230 (4th Cir. 2007) (holding machine-generated data produced by forensic laboratory equipment that reflected blood alcohol level of defendant and presence of PCP not hearsay because they were not made by human declarant, but rather were generated by machine’s diagnostic and technical analysis of defendant’s blood).

producing a reliable result,²²⁶ which is a function of the authentication rules, specifically Rule 901(b)(9).²²⁷

Despite the analysis in *Lorraine*, the cases cited therein, and the authorities referenced in this Article, not all courts are so quick to draw the admittedly subtle distinction between computer-generated and computer-stored statements for purposes of determining whether the records produced by the computer are “statements” made by a “human declarant” for purposes of application of the hearsay rule. Rather, they assume without analysis that the record generated by the computer is hearsay because it contains factual assertions, but then admit it under one of the many hearsay exceptions that cover various records or documents.²²⁸ As George Paul has observed:

However, in some cases, courts simply assume that computer-generated information is hearsay, without performing an analysis, seemingly avoiding the preliminary issue [of whether the information constitutes the “statement” of a “human declarant”]. These courts analyze objections to admissibility by searching for a hearsay

226. *Lorraine*, 241 F.R.D. at 565 (citing *Rollins*, 2004 WL 26780, at *9; *Dunn*, 7 S.W.3d at 432; *Hall*, 976 S.W.2d at 147).

Any concerns about the reliability of such machine-generated information is addressed through the process of authentication not by hearsay or Confrontation Clause analysis. When information provided by machines is mainly a product of “mechanical measurement or manipulation of data by well-accepted scientific or mathematical techniques,” reliability concerns are addressed by requiring the proponent to show that the machine and its functions are reliable, that it was correctly adjusted or calibrated, and that the data . . . put into the machine was accurate In other words, a foundation must be established for the information through authentication, which Federal Rule of Evidence 901(b)(9) allows such proof to be authenticated by evidence “describing [the] process or system used to produce [the] result’ and showing it ‘produces an accurate result.’”

Washington, 498 F.3d at 231. See also SEDONA CONFERENCE COMMENTARY, *supra* note 4, at 10 (“System metadata does not constitute ‘hearsay,’ at least not under the Federal Rules of Evidence, because system metadata is generated by a computer without human assistance. The reason is that under the Federal Rules of Evidence ‘hearsay,’ by definition, requires human input.”).

227. FED. R. EVID. 901(b) (“By way of illustration only, and not by way of limitation, the following are examples of authentication or identification conforming with the requirements of this rule: . . . (9) Process or system. Evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result.”).

228. *Lorraine*, 241 F.R.D. at 568 (noting the following hearsay exceptions recognized by FED. R. EVID. 803 for documents, records and other writings: 803(5) (past recollection recorded); 803(6) & (7) (business records); 803 (8) & (10) (public records); 803(9) (records of vital statistics); 803(11) (records of religious organizations); 803(12) (certificates of baptism, marriage, and related events); 803(13) (family records); 803(14) (records of documents affecting an interest in property); 803(15) (statements in documents affecting an interest in property); 803(16) ancient documents); 803(18) (learned treatises)).

exception, which they nearly always find. And courts that hold that computer-generated information is hearsay often complicate matters by using the term ‘computer-generated information’ loosely, lumping all evidence that comes from a computer together, and failing to focus on whether what is really at issue is computer-*stored* information—often usually hearsay under anyone’s definition.²²⁹

The take-away lesson from *Lorraine*’s discussion of Rule 801(b) as it applies to electronic or digital evidence is that adherence to the five step analysis the opinion describes will ensure that the correct result is achieved—proper distinction between computer-stored statements initiated by a human declarant, which are excluded unless covered by a hearsay exception, and computer-generated non-hearsay statements, that are not admissible unless authenticated by showing that they were generated by a system or process capable of producing a reliable result.²³⁰

The *Lorraine* opinion further notes that the third requirement of the hearsay rule is that the “statement” at issue be offered into evidence to prove its substantive truth, or as Rule 801(c) puts it, hearsay “is a statement, other than one made by the declarant while testifying at the trial or hearing, *offered in evidence to prove the truth of the matter asserted.*”²³¹ So, for example, if evidence that would constitute a “statement” under Rule 801(a), is made by a human declarant as required by 801(b) but is offered for some purpose other than its literal truth, it cannot be hearsay. Examples of when a statement is not offered for its substantive truth, but may be relevant for some other purpose, include those offered to prove the communicative or comprehensive capacity of the declarant, those offered as circumstantial evidence of the state of mind of the declarant, statements that are offered not for their truth but instead to show the conduct of someone who heard them, (to prove that they had knowledge of the information, or to explain what they did after having heard it), statements that constitute “verbal acts” or parts of acts, and statements that have relevance even if not true.²³²

The *Lorraine* opinion also cites examples where ESI/digital evidence that might at first blush be regarded as hearsay was found not to be: e-mail evidence between a co-worker and the defendant was held not to be hearsay because it was not offered for its truth, but merely to

229. PAUL, *supra* note 5, at 119 (citations omitted).

230. See FED. R. EVID. 901(b)(9).

231. *Lorraine*, 241 F.R.D. at 565 (quoting FED. R. EVID. 801(c)) (emphasis added).

232. *Id.* at 565-66.

demonstrate that a relationship existed between the sender and recipient;²³³ e-mails were admitted as non-hearsay in a criminal case because they were not offered for their substantive truth, but rather to show how a lobbyist attempted to influence a government official, and to prove the official's intent and state of mind;²³⁴ and exhibits showing the defendant's website content on a particular day were not hearsay, because they were not offered to prove their literal truth, but rather to prove that they infringed on plaintiff's trademark and copyright.²³⁵ Given the frequency with which circumstantial evidence is offered to prove a party's state of mind, it may be expected that ESI/digital evidence such as e-mail, instant messages, and text messages will be offered for this purpose, and if not also offered for the truth of these statements, such use would remove the evidence from the reach of the hearsay rule. Similarly, as the hypothetical at the start of this Article illustrates, evidence of the content of web sites also is likely to be offered into evidence for reasons other than its literal truth, for example, to prove that the contents were false, inaccurate, or misleading. Similarly, website content may also be offered to prove violations of copyright or trademark protection, to demonstrate unfair competition, or to prove the publication of defamatory statements. In each of these examples, the content of the website would not be offered for its substantive truth, and thus would not be hearsay.

Lorraine further notes that the final step to determining whether ESI/digital evidence is hearsay is to see if the evidence is exempted from the definition of hearsay by Rule 801(d). That rule identifies two categories of out of court statements: certain "prior statements" by witnesses who actually testify at trial and are susceptible to cross examination about the earlier statement, under Rule 801(d)(1), and admissions by party opponents, under Rule 801(d)(2).²³⁶ As for Rule 801(d)(2), it can be expected that admissions will frequently be proved by ESI/digital evidence, because the use of electronic communication is ubiquitous. Indeed, the spontaneity and informality of e-mail, text messaging, and instant messaging may make these forms of digital evidence especially good candidates for evidentiary admissions, and

233. *Id.* at 566 (citing *United States v. Siddiqui*, 235 F.3d 1318, 1323 (11th Cir. 2000)).

234. *Id.* (citing *United States v. Safavian*, 435 F. Supp. 2d 36, 44 (D.D.C. 2006)).

235. *Id.* (citing *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, 1155 (C.D. Cal. 2002)).

236. *Id.* at 567 (citing FED. R. EVID. 801(d)(1)-(2)).

courts are already familiar with the introduction of digital admissions such as e-mail.²³⁷

A. Rule 803 Hearsay Exceptions

While the *Lorraine* opinion stresses the importance of the four step analysis to properly determine whether digital evidence is hearsay in the first instance,²³⁸ it also reminds us that a determination that digital evidence is hearsay is, in a sense, only the start of the analysis, for there is no shortage of hearsay exceptions that courts have applied to ESI:

If, after applying the foregoing four-step analysis, it is determined that the electronic evidence constitutes a statement by a person that is offered for its substantive truth and is not excluded from the definition of hearsay by Rule 801(d)(1) or (2), then the evidence is hearsay and is inadmissible unless it qualifies as one of many hearsay exceptions identified by Rule 803, 804 and 807.²³⁹

Focusing first on Rule 803, the *Lorraine* opinion notes that there are twenty-three separate exceptions, sharing the common characteristic that “[a]ll twenty-three are admissible regardless of whether the declarant is available to testify.”²⁴⁰ The opinion points out that despite the large number of exceptions in Rule 803, they may usefully be grouped into three categories: (1) those dealing with perceptions, observations, state of mind, intent and sensation;²⁴¹ (2) exceptions that involve documents, records, and other writings;²⁴² and (3) statements

237. See, e.g., *Siddiqui*, 235 F.3d at 1323 (holding the e-mail defendant authored was not hearsay because it was an admission); *Safavian*, 435 F. Supp. 2d at 43-44 (holding the e-mail sent by defendant was an admission, therefore not hearsay); *Telewizja Polska USA, Inc. v. EchoStar Satellite Corp.*, No. 02 C 3292, 2004 WL 2367740, at *5 (N.D. Ill. 2004) (holding the images and text posted on defendant’s website were admissions, not hearsay); *Perfect 10, Inc.*, 213 F. Supp. 2d at 1153-55 (holding the e-mail sent by employees of defendant constituted admissions under Rule 801(d)(2)(D)); *Lorraine*, 241 F.R.D. at 568.

238. *Lorraine*, 241 F.R.D. at 562-63.

239. *Id.* at 568.

240. *Id.*

241. *Id.* (citing FED. R. EVID. 803(1), present sense impressions, FED. R. EVID. 803(2), excited utterances, FED. R. EVID. 803(3), then existing state of mind, condition or sensation, and FED. R. EVID. 803(4), statements in furtherance of medical diagnosis and treatment).

242. *Id.* (citing FED. R. EVID. 803(5) (past recollection recorded); FED. R. EVID. 803(6)-(7), (dealing with business records); FED. R. EVID. 803(8) & (10) (dealing with public records); FED. R. EVID. 803(9) (records of vital statistics); FED. R. EVID. 803(11) (records of religious organizations); FED. R. EVID. 803(12) (certificates of baptism, marriage, and related events); FED. R. EVID. 803(13), (family records); FED. R. EVID. 803(14) (records affecting an interest in property); FED. R. EVID. 803(15) (statements in documents affecting an interest in property); FED. R. EVID. 803(16) (ancient

dealing with reputation.²⁴³ With respect to these three categories of exceptions, the court observed:

Given the widely accepted fact that most writings today are created and stored in electronic format, it is easy to see that the many types of documents and writings covered in Rule 803 will implicate electronic writings. Similarly, given the ubiquity of communications in electronic media (e-mail, text messages, chat rooms, internet posting on servers like “Myspace” or “Youtube” or on blogs, voice mail, etc.), it is not surprising that many statements involving observations of events surrounding us, statements regarding how we feel, our plans and motives, and our feelings (emotional and physical) will be communicated in electronic medium.²⁴⁴

Despite the large number of exceptions contained in Rule 803, *Lorraine* notes only a handful of exceptions frequently have been invoked in connection with digital evidence, most of them found in Rule 803.²⁴⁵ One of these exceptions, 803(1), deals with present sense impressions, which are statements describing or explaining an event while it is being perceived, or immediately thereafter.²⁴⁶ Anyone who has ever had a telephone conversation with someone and heard them typing on a computer while they are talking, or sent an e-mail, instant message, or text message to another describing an event as it was happening or immediately thereafter can imagine how often this hearsay exception may be applicable to ESI/digital evidence. Similarly, *Lorraine* points out that Rules 803(2) (excited utterances) and 803(3) (then existing state of mind or condition) also can be expected to apply to digital evidence with some frequency.²⁴⁷ Courts can be expected to apply the same level of scrutiny to ESI/digital evidence as they had in the past applied to “paper” documents in determining whether the

documents); FED. R. EVID. 803(17) (market compilations and directories); FED. R. EVID. 803(18) (learned treatises); FED. R. EVID. 803(22) (dealing with judgments of conviction in criminal cases); FED. R. EVID. 803(23) (dealing with judgments in certain civil cases)).

243. *Id.* (citing FED. R. EVID. 803(19) (reputation regarding personal or family history); FED. R. EVID. 803(20) (reputation regarding land custom, use and practice associated with land, and historically significant facts); FED. R. EVID. 803(21) (reputation regarding character within the community and among associates)).

244. *Id.*

245. *Id.* at 569.

246. FED. R. EVID. 803(1).

247. *Lorraine*, 241 F.R.D. at 569-570.

foundational requirements of hearsay exceptions have been established.²⁴⁸

1. Business Records Exception under Rule 803(6)

The business records exception found at Rule 803(6) is another frequently used basis for admitting digital evidence:

The business record exception is one of the hearsay exceptions most discussed by courts when ruling on the admissibility of electronic evidence. The decisions demonstrate a continuum running from cases where the court was very lenient in admitting electronic business records, without demanding analysis, to those in which the court took a very demanding approach and scrupulously analyzed every element of the exception, and excluded evidence when all were not met.²⁴⁹

The *Lorraine* opinion concludes:

The lesson to be taken from these cases is that some courts will require the proponent of electronic business records or e-mail evidence to

248. *Id.* (citing *United States v. Ferber*, 966 F. Supp 90 (D. Mass. 1997) (concluding that an e-mail from employee to a supervisor qualified as a present sense impression under Rule 803(1), but did not qualify as an excited utterance under Rule 803(2), simply because the e-mail ended with the words “my mind is mush”); *New York v. Microsoft Corp.*, No. CIV A. 98-1233(CKK), 2002 WL 649951, at *2 (D.D.C. Apr. 12, 2002) (concluding that an e-mail that described the contents of a telephone conference sent several days after the call did not qualify as a present sense impression under Rule 803(1) because it was not made contemporaneously with, or immediately after the call); *but see Canatxx Gas Storage Ltd. v. Silverhawk Capital Partners, LLC.*, No. H-06-1330, 2008 WL 1999234, at *13 (S.D. Tex. May 8, 2008) (noting “[e]mail is admissible under the present-sense impression exception to the hearsay rule” if there is sufficient contemporaneousness of the event and the e-mail describing it).

249. *Lorraine*, 241 F.R.D. at 572; *see, e.g.*, *United States v. Kassimu*, 188 F. App’x 264, 265 (5th Cir. 2006) (holding that the business record exception was established for computer-generated records by the testimony of a witness familiar with the record keeping system of the business); *Sea-Land Serv., Inc. v. Lozen Int’l*, 285 F.3d 808, 819-20 (9th Cir. 2002) (holding that digital records were admissible as business records on showing that they had been produced from same electronic information generated at the time the contract was created, and noting that “it is immaterial that the business record is maintained in a computer rather than in company books”); *contra Microsoft Corp.*, 2002 WL 649951, *2 (holding that an employee e-mail did not qualify as business record without a showing that it was the regular practice of the employer to require the employee to make and maintain the e-mail for a business purpose, and requiring that, for e-mail chains, each participant must be acting in the regular course of the business in contributing to the e-mail chain); *Rambus Inc. v. Infineon Tech. AG*, 348 F. Supp. 2d 698, 706-707 (E.D. Va. 2004) (requiring that each participant in an e-mail chain must be acting in the course of the business’s regular activities in order for the chain to qualify as a business record); *In re Vee Vinhnee*, 336 B.R. 437, 445 (B.A.P. 9th Cir. 2005) (utilizing a very demanding approach in assessing whether computer generated credit card records were business records, and expressing concern about the possibility that records could have been altered or modified after being scanned into computerized database).

make an enhanced showing in addition to meeting each element of the business records exception. These courts are concerned that the information generated for use in litigation may have been altered, changed or manipulated after its initial input, or that the programs and procedures used to create and maintain the records are not reliable or accurate.²⁵⁰

Courts that appreciate that employees often use their business computer to send personal e-mails are more likely to be inclined to require strict adherence to each element of Rule 803(6) before they are willing to admit e-mail as a business record. A good example of such a case, decided after *Lorraine*, is *Canatxx Gas Storage Limited v. Silverhawk Capital Partners, LLC*,²⁵¹ where the court held:

Neither a paper document, such as a letter or memo or note, nor an email, falls within the business-records exception of Rule 803(6) simply because it concerns a business matter. Courts have held that conventional letters, memos, or notes are admissible under the business records exception if they are regularly made in furtherance of the employer's needs and not for the personal purposes of the employee who made them. Courts have applied a similar approach to emails. A party seeking to introduce an email made by an employee about a business matter under the hearsay exception under Rule 803(6) must show that the employer imposed a business duty to make and maintain such a record. Courts examine whether it was the business duty of an employee to make and maintain emails as part of his job duties and whether the employee routinely sent or received and maintained the emails.²⁵²

This is an important point. As demonstrated above, many forms of digital communication that are associated with personal communications have migrated into the business arena, including text messages, blogging, and instant messaging. Courts can be expected to require the proponent of such evidence to make a clear showing that the digital evidence relates to a regular activity of the business itself, as opposed to the personal use of its creator, and that the business imposed on the employee a requirement to make a digital record of the occurrence, and thereafter to maintain that record for purposes of the future use by the company. This raises an interesting issue. Many organizations and businesses have electronic records management systems in place that

250. *Lorraine*, 241 F.R.D. at 574.

251. 2008 WL 1999234.

252. *Id.* at *12 (citations omitted).

automatically delete e-mails after a specific period, such as ninety days.²⁵³ In such instances, unless the organization or business also requires that certain types of e-mail that are important to the effective operation of the organization are maintained in a saved file for future business purposes, then it may be difficult to prove that they constitute business records, because Rule 803(6) requires that they be “*kept* in the course of a regularly conducted business activity.”²⁵⁴ It may be difficult to show that the e-mail are “kept” for a “business activity” if they are routinely and automatically deleted without being saved to a file where they will continue to be available for business purposes.

In addition to the question of whether e-mail or other digital records meet the requirements of Rule 803(6) that they be made for a business purpose, a number of commentators have expressed grave concern that when it comes to computerized evidence, there has been a significant erosion of the requirement that a business record be the product of a trustworthy process. This requirement is explicit in the rule itself, which provides that even if the record is made for a business purpose, contemporaneously with the events described within, by someone with personal knowledge of those facts, and the regularity requirements are met, the record nonetheless must be excluded if “the source of information or the method or circumstances of preparation indicate lack of trustworthiness.”²⁵⁵ In his book, George Paul meticulously lays out exactly what the problem is when the trustworthiness requirement of the business record exception is overlooked and the regularity requirement is the only criterion for admissibility of digital evidence:

Now, *regularity* of preparation has become the key to admitting business records including records containing computer-generated information. And if regularity is the test, almost any computer-generated information qualifies, without any showing of reliability. Accordingly, both the hearsay rule—and the main exception used to test admissibility of statements of information systems under it—become trivial, without any meaningful competency determination by a court. The ability to exclude out-of-court statements, the hearsay rule, appears to have largely evaporated with regard to computer-generated information. Rather, in almost every case, all computer

253. See, e.g., FED. R. CIV. P. 37(f) advisory committee’s notes to the 2006 amendments (noting the revised rule “focuses on a distinctive feature of computer operations, the routine alteration and deletion of information that attends ordinary use”).

254. FED. R. EVID. 803(6) (emphasis added).

255. *Id.*

evidence is admitted and things go to weight of the evidence. That may be our final, preferred policy, after rule makers and thinkers address this issue during the coming years, but in the meantime practitioners should acknowledge the reality of where the law has drifted.²⁵⁶

George Paul further observes that:

[C]ourts also now overlook the caveat in Rule 803(6) that allows admission ‘unless the source of the information or the method or circumstances of preparation indicate lack of trustworthiness.’ Courts overwhelmingly find that problems concerning the accuracy of computer-generated evidence go to the weight of the evidence, not admissibility.²⁵⁷

There is, however, a problem with this approach:

When courts exclude both the trustworthiness caveat from their 803(6) foundational inquiry, and an explicit preliminary authenticity analysis as a prerequisite for admission, there is a high probability (if not certainty) that any out-of-court statement made by an information system will be admitted. This is significant, because jurors give computer-generated evidence a high level of credibility, much as scientific evidence is interpreted by jurors to have an “aura of credibility.”²⁵⁸

George Paul concludes with this cautionary observation:

Clearly, when applying the rationale of the business records exception to computer generated evidence, “important differences” have “eluded consideration.” For example, computer-generated evidence does not become more accurate from “regularity of preparation.” Unlike humans, where repeated action trains an individual ‘in habits of precision,’ computers do not become more accurate each time they produce a result. . . .

Just because businesses rely on faulty computer programs does not necessarily mean that courts should follow suit. Without requiring some preliminary showing of reliability, a court will simply have no idea what caliber of information system produced the result or what measures, if any, the business took to protect the integrity of the system. When considering the duty judges have to ensure the accuracy

256. PAUL, *supra* note 5, at 120.

257. *Id.* at 125 (citations omitted).

258. *Id.* at 125-26.

of evidence considered by the jury, blindly admitting computer-generated evidence without any foundation is a system that, in essence, does away with the hearsay rule and that allows everything to go to the weight.²⁵⁹

George Paul is not alone in his concern that courts have become too lax in admitting computer-generated evidence as business records without a sufficient showing of the reliability of the system that produced them. The Commentary of the widely respected Sedona Conference regarding ESI evidence and admissibility,²⁶⁰ also published after the issuance of the *Lorraine* opinion, raises similar concerns. It stresses the importance of being aware that ESI/digital evidence is prepared, stored and used within a “threat landscape” that includes the availability of “anti-forensics.”²⁶¹ The Commentary raises the following warning:

Courts and litigants need to become familiar with anti-forensic tools and not become bedazzled by technology, which some fear is occurring. In a paper that appeared in the *Journal of Digital Forensic Practice*, Vincent Liu and coauthor Eric Van Buskirk flout the U.S. courts’ faith in digital forensic evidence. Liu and Van Buskirk cite a litany of cases that established, as one judge put it, computer records’ “prima facie aura of reliability.” One decision even stated that computer records were “uniquely reliable in that they were computer-generated rather than the result of human entries.” Liu and Van Buskirk take exception to this viewpoint. The “unfortunate truth” they conclude, is that the presumption of reliability is unjustified and the justice system is “not sufficiently skeptical of that which is offered up as proof.”²⁶²

The *Lorraine* decision did not involve a challenge to the admissibility of ESI/digital evidence offered as a business record, and its discussion of the cases that had, to date, analyzed this important hearsay exception in the context of such evidence pointed out the continuum of cases where courts have shown, at times, both extreme deference as well as hostility to admitting digital evidence under this exception. The

259. *Id.* at 129.

260. SEDONA CONFERENCE COMMENTARY, *supra* note 4.

261. Anti-forensics is defined as “the employment of sophisticated tools and methods used for the intentional fabrication and/or manipulation of ESI on a computer system intended to thwart forensic examination. In short, anti-forensics is digital forgery.” *Id.* at 16.

262. *Id.* (quoting Eric Van Buskirk & Vincent T. Liu, *Digital Evidence: Challenging the Presumption of Reliability*, 1 J. DIGITAL FORENSICS PRACTICE 19, 25 (2006)).

important lesson to be learned for the future development of this critical area of evidence law is that the concerns raised by George Paul's book and the Sedona Conference Commentary generate a wake-up call to both judges and lawyers to more carefully consider these issues. The primary obligation for doing so rests with the lawyers, as they must be the ones to identify reliability/trustworthiness problems with digital business records, develop the facts to challenge them, and argue to the courts why the exception is inapplicable and why the proffered evidence should be excluded. As part of this process they must be able to distinguish those cases which have, as noted by George Paul and the Sedona Conference Commentary, unjustifiably assumed that the digital records were reliable and admitted them without skeptical analysis. Thereafter, it is the responsibility of the courts to carefully consider whether the challenges have merit, and address this on a case-specific basis, as opposed to adopting a categorical approach that assumes reliability simply because the evidence was computer-generated. The importance of making an objection in the first instance, however, cannot be underscored enough, as the *Lorraine* case noted:

What, then, is the effect of hearsay evidence that is admitted without objection by the party against whom it is offered? The general rule is that despite Rule 802, if hearsay is admitted without objection it may be afforded its "natural probative effect, as if it were in law admissible."²⁶³

2. Public Records Exception under Rule 803(8)

Another hearsay exception that the *Lorraine* opinion recognized as likely to be applied with regard to ESI/digital evidence is Rule 803(8), the public records exception.²⁶⁴ This is an important exception because of the ease with which it may be employed and the minimal foundation needed to establish it.²⁶⁵ As noted in, Williams, the rationale for the public records exception is as follows:

Justification for this exception derives from the trustworthiness of the documents themselves, having been made by a public office or agency, as well as the inherent necessity to avoid requiring public officials to needlessly testify as witnesses about reports, data compilations,

263. *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 575 (D. Md. 2007).

264. *Id.* at 574.

265. *See supra* Part III.

records or statements made in their official capacities. The documents are considered trustworthy due to the “duty that comes with public service,” and it is presumed that public officials execute their tasks “carefully and fairly, without bias or corruption, and this notion finds support in the scrutiny and risk of exposure that surround most government functions.” Absent the exception found at Rule 803(8), lawyers seeking to prove facts contained within official records would be forced to call public officials as witnesses to provide testimony regarding the contents of the official records. This would, of course, be burdensome and divert the efforts of officials called as witnesses from performing their public duties.²⁶⁶

In *Williams*, the public records that were determined to be admissible were websites from two state agencies.²⁶⁷ Because nearly all local, state, and federal agencies have their own websites these days, and those sites frequently contain significant amounts of factual information that may be relevant to the resolution of litigation involving those agencies, or private parties, it may be expected that Rule 803(8) will prove particularly useful as a hearsay exception to permit the admission into evidence of matters contained within those websites. Indeed, the hypothetical that started this Article illustrates this, and the postings on the FTC website regarding unfair business practices of ConsumerPro are likely to be relevant to consumer actions against that company and the contract claim filed against it by Tele-Sales. Other types of ESI/digital evidence that the *Lorraine* opinion noted had been admitted into evidence under the public records exception include e-mail from public agencies²⁶⁸ and computerized records of a public agency.²⁶⁹

B. Rule 804 Hearsay Exceptions

The *Lorraine* opinion did not discuss the potential applicability of the hearsay exceptions found at Rule 804 to ESI/digital evidence. These exceptions are far fewer in number than those found in Rule 803²⁷⁰ and

266. *Williams v. Long*, 585 F. Supp. 2d 679, 690-91 (D. Md. 2008) (quoting MUELLER & KIRKPATRICK, *supra* note 157, § 8:86, at 770-72) (citations omitted).

267. *Id.* at 682.

268. *Lorraine*, 241 F.R.D. at 575 (citing *Lester v. Natsios*, 290 F. Supp. 2d 11 (D.D.C. 2003)).

269. *Id.* (citing *United States v. Ocegerra-Aguire*, 70 F. App'x 473 (9th Cir. 2003)).

270. There are only five exceptions found in Rule 804. *See* FED. R. EVID. 804(b)(1) (former testimony of an unavailable declarant); FED. R. EVID. 804(b)(2) (dying declarations); FED. R. EVID. 804(b)(3) (statements against penal, pecuniary, or proprietary interest); FED. R. EVID. 804(b)(4) (statements of an unavailable declarant regarding his or her personal or family history); FED. R.

require an extra foundational step beyond those found in Rule 803. All of the Rule 804 hearsay exceptions require that the proponent demonstrate that the declarant is unavailable to testify at trial, and Rule 804(a) identifies five circumstances in which this can occur.²⁷¹ While research has failed to disclose examples of when courts have admitted ESI/digital evidence under the Rule 804 exceptions, it is not difficult to imagine circumstances in which they might be willing to do so. First, as most trials and depositions are recorded electronically, or on video, introduction of prior trial or deposition testimony of an unavailable declarant under Rule 804(b)(1) inevitably involves ESI/digital evidence. Similarly, given the ubiquity of cell phones and personal digital assistants, it is not difficult to imagine that a person who has been the subject of a fatal or near fatal assault would make a cell phone call that would meet the requirements of a dying declaration under Rule 804(b)(2). Further, the underlying facts in *Crawford v. Washington*,²⁷² the recent landmark confrontation clause case, involved a recorded statement of the defendant's wife, who later asserted the marital privilege and was unavailable for trial,²⁷³ and in the state court prosecution the state introduced the recorded statement into evidence under the state equivalent of Rule 804(b)(3), a statement against penal interest.²⁷⁴ And, finally, it would not be hard to imagine a situation in which a defendant in a criminal case sends a text message to a potential witness against him threatening the witness if she testifies, and the witness, in turn, sends a text message, or e-mail, or leaves a voicemail message to another person which details the threat, as well as the criminal activity of the defendant which led to it. In such a situation, the digital communication sent by the witness likely would be admissible under Rule 804(b)(6), if the witness was unavailable to testify at trial because of the defendant's threat.

EVID. 804(b)(6) (statements of an unavailable declarant that are admitted against a party whose wrongful conduct caused the declarant to be unavailable).

271. See FED. R. EVID. 804(a)(1) (declarant asserts a privilege and therefore cannot be compelled to testify); FED. R. EVID. 804(a)(2) (declarant refuses to testify, despite being ordered to do so by the court); FED. R. EVID. 804(a)(3) (declarant lacks sufficient memory to be able to testify fully and completely); FED. R. EVID. 804(a)(4) (declarant cannot testify because of death, illness, or incapacity); FED. R. EVID. 804(a)(5) (beyond the ability of the court to compel the declarant to appear and testify).

272. 541 U.S. 36 (2004).

273. *Id.* at 40.

274. *Id.*

V. THE ORIGINAL WRITING RULE AS APPLIED TO ESI/DIGITAL EVIDENCE

The *Lorraine* opinion also provides an analytical framework for how the collection of evidence rules commonly known as the “best evidence” or “original writing rules” operate in the realm of electronic or digital evidence.²⁷⁵ The opinion notes that the structure of the original writing rules is important to understand to ensure their proper application. Rule 1001 contains a series of definitions: “original,” “duplicate,” “writing,” “recording,” and “photograph,” and as they apply to ESI/digital evidence, the most important definition is found at Rule 1001(3), which states, “[i]f data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an ‘original.’”²⁷⁶ Thus, “the ‘original’ of information stored in a computer is the readable display of the information on the computer screen, the hard drive or other source where it is stored, as well as any printout or output that may be read so long as it accurately reflects the data.”²⁷⁷ Further, as a result of Rule 1003, which provides that duplicates are co-extensively admissible as originals, unless unauthentic or prepared under circumstances that would make it unfair to admit them, “the distinction between duplicates and originals largely has become unimportant.”²⁷⁸

Lorraine discusses when the original writing rule applies in the first instance—the rule is inapplicable unless a party is seeking to prove the “contents” of a writing, recording, or photograph.²⁷⁹ If a digital document describes an event the occurrence of which may be proved by the testimony of witnesses who observed it, the original writing rule is inapplicable, and would not require introduction of the document in lieu of the testimony of the witnesses.²⁸⁰ In contrast, if there is no non-documentary proof of the occurrence, and the only evidence of what transpired is contained in a writing, then the original writing rule applies.²⁸¹ Similarly, as in the hypothetical that began this Article, if the

275. *Lorraine*, 241 F.R.D. at 567-83.

276. FED. R. EVID. 1001(3).

277. *Lorraine*, 241 F.R.D. at 577-78 (citing WEINSTEIN & BERGER, *supra* note 78, § 900.07[1][d][iv]; PAUL R. RICE, ELECTRONIC EVIDENCE: LAW AND PRACTICE 194 (ABA Publishing 2005); *Laughner v. State*, 769 N.E.2d 1147, 1159 (Ind. Ct. App. 2002)).

278. *Id.* at 578.

279. *Id.*

280. *Id.*

281. *Id.*

contents of a website at a particular date are important to establish the false or inaccurate information that the consumers saw when they accessed the ConsumerPro website, then the original writing rule would apply, because the plaintiffs would be seeking to prove the “content” of the website at that particular time.

Lorraine notes that when the rule applies, it creates a hierarchy of evidence that may be used to prove the contents of a writing, recording, or photograph: an original or duplicate, and if not available, then by “secondary evidence,” which is defined as “any proof of the contents of a writing, recording or photograph other than an original or duplicate . . . [including] testimony from the author of the writing, or someone who read it, earlier drafts, copies, or an outline used to prepare the final [draft].”²⁸² Given the ephemeral nature of ESI, and the fact that it may be deleted, overwritten, or otherwise inaccessible, secondary evidence often must be used to prove the content of ESI/digital evidence. As the *Lorraine* opinion notes:

Given 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 time period) or otherwise unavailable means that the contents of electronic writings may have to be proved by secondary evidence.²⁸³

The *Lorraine* opinion explains that when secondary evidence must be used to prove the contents of ESI/digital evidence, then there are a series of rules that govern.²⁸⁴ The primary rule is Rule 1004, which permits secondary evidence to prove the contents of ESI in four circumstances: (a) when the originals or duplicates have been lost or destroyed, absent any bad faith by their proponent; (b) if the originals or duplicates are not obtainable by judicial process or procedure; (c) if the originals or duplicates are in the possession, custody or control of an adverse party who is on notice by the pleadings or otherwise that their contents would be the subject of proof at a trial or hearing and who does not bring them; or (d) the documents are “collateral” to the litigation, meaning that they do not closely relate to a controlling issue in the litigation.²⁸⁵ Other rules that permit secondary evidence to prove the

282. *Id.* at 576.

283. *Id.* at 580.

284. *Id.* at 576 (citing FED. R. EVID. 1004-07).

285. FED. R. EVID. 1004; *see also Lorraine*, 241 F.R.D. at 579-80.

contents of documents include Rule 1006, which permits the introduction of summaries of voluminous writings, recordings, or photographs, and Rule 1007, which allows the proof of the contents of a writing, recording, or photograph through the testimonial admission of an adverse party.²⁸⁶ Rule 1006 is especially important with respect to ESI/digital evidence, and the *Lorraine* opinion points out that “[b]ecause the production of electronically stored information in civil cases frequently is voluminous, the use of summaries under Rule 1006 is a particularly useful evidentiary tool, and courts can be expected to allow the use of summaries provided the procedural requirements of the rule are met.”²⁸⁷

Finally, the *Lorraine* opinion discusses an important, but frequently overlooked rule, Rule 1008, which is a particular application of the conditional relevance rule.²⁸⁸ The opinion notes that Rule 1008 “is a specialized application of Rule 104(b), and it allocates the responsibility between the trial judge and the jury with respect to certain preliminary matters affecting the original writing rule.”²⁸⁹ As the Advisory Committee Notes to Rule 1008 states,

Most preliminary questions of fact in connection with applying the rule preferring the original as evidence of contents are for the judge, under . . . Rule 104(a). Thus, the question whether the loss of the originals has been established, or of the fulfillment of other conditions specified in Rule 1004 . . . is for the judge.²⁹⁰

However, the Advisory Committee Notes also state:

Rule 1008 identifies three issues that are questions for the jury . . . (1) whether the writing, recording or photograph ever existed in the first place; (2) whether some other writing, recording, or photograph that is offered into evidence is in fact the original; and (3) whether ‘other’

286. *Lorraine*, 241 F.R.D. 580-82.

287. *Id.* at 581 (citing *Wapnick v. Comm’r of Internal Revenue*, T.C. Memo. 2002-45 (T.C. 2002) (holding that summaries of voluminous computer records were admissible under Rule 1006 even though they were prepared in anticipation of litigation, because the underlying documents had been admitted into evidence and reasonably had been made available to the opposing party to inspect).

288. *See supra* Part II (discussing the conditional relevance rule).

289. *Lorraine*, 241 F.R.D. at 582.

290. *Id.* at 582-83 (citing FED. R. EVID. 1008 advisory committee’s notes to the 1972 Proposed Rules).

(i.e. secondary) evidence of contents correctly reflects the content of the writing, recording or photograph.²⁹¹

In practice, these conditions frequently occur, such as when parties negotiate a contract and exchange successive revisions of it by e-mail. The plaintiff may contend that there was a written contract, and produce what she claims it is, while the defendant may deny that there ever was a meeting of the minds. Alternatively, they may agree that there was a contract, but offer different versions of it. Further, where secondary evidence is admissible, there may be conflicting versions of the content of a relevant document. When this occurs, then Rule 1008 requires the trial judge to submit to the jury the competing factual contentions, and it is up to the jury to decide which to accept, and which to reject. What counsel sometimes overlook is that if the dispute of fact concerns a document that is essential to the resolution of a claim or defense, then summary judgment will not be possible to resolve the dispute, as there is a genuine dispute of material fact that must be submitted to the jury. The hypothetical starting this Article shows how easily this can occur when ESI/digital evidence is involved. If witnesses from ConsumerPro and Tele-Sales disagree on which version of the ConsumerPro script appeared on the website when the Tele-Sales operators secured a particular consumer contract, then the jury will have to resolve which version is the operative one, and neither side will be able to avoid trial through summary judgment practice.

In its discussion of the original writing rule, the *Lorraine* opinion focused on the structure of the rule and how it has been applied thus far by courts to ESI/digital evidence. However, the court cases that have done so to date have not wrestled with some fundamental issues about just what constitutes the original of a computer generated or stored document. As noted above, the definition of an “original” found in Rule 1001 encompasses electronic documents, and the definition is extremely broad: “If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an ‘original.’”²⁹² This definition does not give much guidance about what to do with the components of an electronically generated document that are not visible when the document is “opened” on the computer and the screen-readable version is visible. Those familiar with electronic documents know that all documents contain

291. *Id.* at 583.

292. FED. R. EVID. 1001(3).

“metadata,” which, as *Lorraine* notes, has been usefully defined as follows:

Metadata, “commonly described as ‘data about data,’ is defined as ‘information describing the history, tracking, or management of an electronic document.’ . . . [Metadata includes] ‘all of the contextual, processing, and use information needed to identify and certify the scope, authenticity, and integrity of active or archival electronic information or records.’”²⁹³

To date, courts have not had to resolve the relationship that metadata has to the screen-readable version of a document in the context of the original writing rule. Expressed differently, is the metadata part of the “original” of the document under Rule 1001(3), or only the portion that is “readable by sight” when the document first is opened?

In a more robust fashion, George Paul describes this difference between a “digital” document and a “paper” document, the latter of which is three-dimensional. He observes:

Writings in the digital realm are different. . . . Such records are very close to “pure information,” and exist by virtue of a mere succession of the differentiation of 1s and 0s, distinguished by electricity flowing in machine systems. In writing today we deal in pure information objects, unfettered by matter. They can be whisked or shaken or rearranged in an instant. Such records are actually layers of abstraction, one view stacked on top of another. At the deepest layer is the world of bits, 1s and 0s. As one builds on top of this, the bits of information can carry letters and numbers. This collection of letters and numbers may be partitioned into smaller collections to represent, for example, such categories as “name” and “date of birth.” Then there are layers designed to be presentations of information to viewers of that data. Conjoined with this data is a collection of information about the other data, which collection is often called “metadata.” This metadata is information that software developers have designed to be recorded in a record and that is inserted there by the system itself. For example, even without making any entry or modifying any data, each time one saves a document one is editing on a word-processing program that program, and the system that supports that program, will record the date and time of that “save” event in the data being “saved.” This information then becomes a part of the record

293. *Lorraine*, 241 F.R.D. at 547 (quoting *Williams v. Sprint/United Mgmt. Co.*, 230 F.R.D. 640, 646 (D. Kan. 2005)).

There is also usually a top-layered presentation view that is normally viewed by the operator of the program in question. For example, in a word-processing application, such as Microsoft Word, one can view a page as it is being typed. *This view contains what the layperson normally considers the data of a file. Interestingly, although the view often looks very much like a page of paper, this is of course an illusion, something the application has designed to mimic old-style physical records. What we are viewing is simply the top-level view: the view of what the record normally shows to people who view it on a screen and also upon printing out the record onto paper.*²⁹⁴

To date, the courts that have considered the original writing rule as it applies to the admissibility of ESI/digital evidence have tended to view the “original” as the “top-level view” of “what the record normally shows to people who view it on a screen and also upon printing out the record onto paper.”²⁹⁵ Disputes about metadata have tended to focus on its discoverability,²⁹⁶ or its utility in authenticating a digital document.²⁹⁷ Whether they will continue to do so, or begin to expand their view of whether the original is to include the “hidden” or unseen digital components of a computer-generated or stored document remains to be seen. However, it may be predicted that for the foreseeable future they will continue to treat the “original” as the portion that is viewed when the digital document is opened or printed from a computer because that is the portion that is “readable by sight” as stated in Rule 1001(3), and because that is the component of the digital document that tends to be the version that is used or disseminated by its author, and hence most likely to be the legally operative version that figures into a future legal dispute.

294. PAUL, *supra* note 5, at 19-20 (emphasis added).

295. *Id.* at 20. *See, e.g.*, DIRECTV, Inc. v. Reyes, No. 03 C 8056, 2006 WL 533364, at *7 (N.D. Ill. Mar. 1, 2006) (holding that a computer printout of information that has been stored on the computer is an “original” under Rule 1001(3)); Con-Way Transp. Servs., Inc. v. Auto Sports Unlimited, Inc., No. 1:04-CV-570, 2007 WL 2875207, at *3-4 (W.D. Mich. Sept. 28, 2007) (noting that reprinted invoices based on information extracted from computer which generated the invoices originally sent to defendant constitute “originals” under Rule 1001(3)).

296. *See, e.g.*, FED. R. CIV. P. 34 (allowing a party to identify the form or forms of production in which an electronic document is to be produced, which can include its “native” form, containing metadata); *Lorraine*, 241 F.R.D. at 576-83; *Williams*, 230 F.R.D. at 646-55 (discussing the discoverability of metadata).

297. *Lorraine*, 242 F.R.D. at 547 (discussing how metadata may be used to authenticate ESI).

VI. PREJUDICIAL IMPACT

The final “evidentiary hurdle” to admissibility of ESI or digital evidence discussed in *Lorraine* is whether the evidence, if otherwise admissible under all of the previously discussed evidentiary rules, is excessively prejudicial when compared with its probative value. At the outset, it should be emphasized that the balancing that Rule 403 contemplates favors admissibility over exclusion. Under the rule, relevant and otherwise admissible evidence, including ESI, is only excluded if its probative value is substantially outweighed by the danger of unfair prejudice.²⁹⁸ Thus, the prejudice must be disproportionately greater than its probative value. And because all evidence offered by one party is prejudicial to the extent that it proves the proffering party’s case against the party to which the evidence is offered, the prejudice needed to justify exclusion under Rule 403 must be “unfair.”

VII. CONCLUSION

In conclusion, reflecting back on the *Lorraine* opinion two years after it was issued, *Lorraine* continues to be the only case to attempt a comprehensive analysis of evidentiary issues associated with admitting ESI. The opinion seems to have succeeded in its stated objective—to provide a useful and exhaustive guide to courts and lawyers regarding the rules and principles that must be applied to ensure admissibility of ESI or digital evidence, which increasingly accounts for all non-testimonial evidence offered as evidence at trial or in summary judgment. Further, following *Lorraine*, courts, both those which cite *Lorraine* and those which do not, have mainly adhered to the standards and principles that *Lorraine* advanced. As such, it continues to remain a useful resource, especially as a starting point in approaching this challenging area of evidence law. This Article has brought *Lorraine* forward, by discussing subsequent developments in digital evidence law, making observations about trends that can be expected to continue, and forecasting issues that await future development. Therefore, it was a worthwhile exercise to take a moment, and go back to the future.

298. FED. R. EVID. 403.