Journal of Technology Law & Policy

Volume 23 | Issue 2 Article 4

January 2019

A New Age of Authentication

Abraham Oxner

A NEW AGE OF AUTHENTICATION

Abraham Oxner[*]

INTRODUCTION

The American justice system is predicated upon proving the validity of your argument to a trier of fact. It is apparent that proving your argument requires evidence. This is the challenge that all trial attorneys face. However, before evidence can be presented to a fact finder, it must be admitted.[1]

In general, the admission of evidence is a long and complex process. There are several hurdles in place that an attorney must overcome before a piece of evidence is ever placed in front of a jury. A full-length discussion of those hurdles is beyond the scope of this Note. What is important to note, however, is that all evidence must be authenticated.[2] Authentication, in many cases, forces the entering party to prove the evidence is what they claim it to be.[3] This evidentiary hurdle is so obvious that it is often overlooked. However, in scholarly literature or legal jurisprudence, this seemingly simple requirement is a quagmire when applied to purely digital evidence or electronically stored information (ESI).

The timeliness of this discussion is influenced by the Amendment to the Federal Rules of Evidence on December 1, 2017.[4] One of those amendments added two ESI-specific provisions to Rule 902 to allow more types of evidence to be "self-authenticating."[5] This Note will examine how the legal system has navigated the newest hurdle of

---

* J.D., University of Florida Levin College of Law (2019); B.A., University of South Florida (2011).

1. *See* FED. R. EVID. 402.

2. *See id.* 401(a), 901(a).

3. *Id.* 901(a).

4. *See* Carl A. Aveni, *New Federal Evidence Rule Changes Reflect Modern World*, LITIG. NEWS, Spring 2018, at 10.

5. *Id.*; FED. R. EVID. 902(13), (14).

authenticating ESI and to determine what other solutions may lay on the horizon.

Section I will give a historical background as to how courts have previously handled the growth of ESI and the unique challenges it presents. Section II will outline the most recent adaptation directly related to authentication and explain how the changes were meant to work. Finally, Section III will assess the implementation of the amendments, identify remaining issues, and suggest solutions.

I. THE ISSUE

Historically, the amount of evidence produced and used in court had been organically capped at a manageable amount due to the physical limitations of paper-documents, both in storage space and transmission.[6] Today, however, the world communicates digitally. The failure to adapt to this considerable shift in the character of evidence was a major critique of the Federal Rules of Evidence.[7]

A digital wave of data swept the globe and had a profound impact on how courts had to handle the use and storage of this potential evidence. In 1999, a University of California study found that 93% of information was created digitally in that year.[8] In 2000, the approximate cost to store 1GB of data electronically was $14.[9] That price plummeted to 75¢ by 2005.[10] In 2015, the cost was around 3¢.[11] With such stunning reduction in storage costs, the presumption would be that the promulgation of ESI has made litigation cheaper. Yet, the cost of preserving this information grew exponentially, and by 2014, larger companies reported spending upwards of $40 million on simply maintaining this data.[12]

The reason for this inverse increase in cost relates to the first and most prominent challenge in dealing with ESI: volume.[13] Companies today deal in terabytes of data as the majority of companies' stored information

---

6. *See* Kenneth J. Withers et al., *Panel One: Technical Aspects of Document Production and E-Discovery*, 73 FORDHAM L. REV. 23, 25 (2004).

7. AM. COLL. OF TRIAL LAWYERS TASK FORCE ON DISCOVERY & INST. FOR THE ADVANCEMENT OF THE AM. LEGAL SYS., FINAL REPORT ON THE JOINT PROJECT OF THE AMERICAN COLLEGE OF TRIAL LAWYERS TASK FORCE ON DISCOVERY AND CIVIL JUSTICE AND IAALS 2 (2009), https://iaals.du.edu/sites/default/files/documents/publications/actl-iaals_final_report_rev_8-4-10.pdf.

8. MICHAEL R. ARKFELD, ARKFELD ON ELECTRONIC DISCOVERY AND EVIDENCE § 1.1 (4th ed. Supp. 2019).

9. Andrew Bartholomew, *Rethinking "Cheap" Data Storage*, EXTERRO (June 10, 2015), https://www.exterro.com/blog/rethinking-cheap-data-storage/.

10. *Id.*

11. *Id.*

12. *Id.*

13. *See id.* and accompanying text.

is electronic.[14] Additional sources, such as Facebook and Twitter posts or cell phone text messages, add to the volume of discovery. UC Berkeley's School of Information Management and Systems reported five exabytes of data were created globally in 2002.[15] By 2006, that number grew to 161 exabytes.[16] Research shows that approximately 124.5 billion business emails were sent each day in 2018, with that number expected to grow by 3% in 2019.[17] It is society's overwhelming dependence upon technology— especially in business—which has exacerbated the growth of ESI each year and compounded the difficulties faced in authenticating such data.

A second feature of ESI that poses particular difficulty for authentication is its complexity. Traditionally, the authentication of paper evidence was a matter of reading what was written on the page. The Rules of Evidence were devised to determine the reliability and authenticity of this type of information.[18] However, ESI is deceptively detailed as it contains layers of embedded metadata, which can sometimes be its most valuable asset.[19]

Third, ESI is subject to, and almost completely dependent upon, the devices within which it is stored. For example, emails and text messages are not stored in printed form but through a systems inbox. This creates a subset of problems for all phases of admissibility because it creates more chains of custody as the data can be manipulated, deleted, or lost due to imprecise system storage or user error.[20] ESI is frequently destroyed inadvertently by being deleted or overwritten as a routine, good faith business practice.[21] Ironically, the opposite problem of being able to locate or recreate deliberately deleted data can also give rise to

---

14. Damian Vargas, *Electronic Discovery: 2006 Amendments to the Federal Rules of Civil Procedure*, 34 RUTGERS COMPUTER & TECH. L.J. 396, 398 (2008).

15. PETER LYMAN & HAL R. VARIAN, U.C. BERKELEY, SCH. INFO. MGMT. SYS., HOW MUCH INFORMATION? (2003), http://groups.ischool.berkeley.edu/archive/how-much-info-2003/execsum.htm.

16. Geoff Duncan, *Study: 161 Exabytes of Digital Data in 2006*, DIGITAL TRENDS (Mar. 6, 2007, 3:00 AM), https://www.digitaltrends.com/computing/study-161-exabytes-of-digital-data-in-2006/.

17. Andrea Robbins, *The Shocking Truth About How Many Emails Are Sent*, CAMPAIGN MONITOR (Mar. 19, 2018), https://www.campaignmonitor.com/blog/email-marketing/2018/03/shocking-truth-about-how-many-emails-sent/.

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

19. *See* Withers et al., *supra* note 6, at 24.

20. Adam Stone, *How to Ensure Digital Evidence Stands Up in Court*, GEN. DYNAMICS INFO. TECH. (Sept. 17, 2015), https://www.govtechworks.com/chain-of-custody-how-to-ensure-digital-evidence-stands-up-in-court/.

21. BARBARA J. ROTHSTEIN ET. AL., FED. JUDICIAL CTR., MANAGING DISCOVERY OF ELECTRONIC INFORMATION: A POCKET GUIDE FOR JUDGES 19–20 (2007).

complications for authentication.[22] Additionally, because ESI does not stand alone, it requires potentially expensive or inaccessible computing systems to present all the information in a way that is understandable and reasonable for judges and juries.

These features of ESI create complications that implicate more than just the Evidence Code. Though authentication is the current topic of discussion, the Federal Rules of Civil Procedure were amended when ESI first burst onto the legal landscape.[23] The primary concern was the confusion and cost involved when handling large quantities of ESI in the discovery phase.[24] How did the Federal Rules of Civil Procedure regarding discovery handle unduly burdensome obligations of businesses and individuals to store and preserve ESI and the accompanying hefty sanctions when they erred? The response came in 2006 with an amendment to the Federal Rules of Civil Procedure, which recognized ESI as distinct from paper-based document discovery, and created methods of reducing discovery costs and sanctions.[25] The background and resolution of the early 2000s ESI challenges for discovery provide a useful comparison to the authentication challenges and subsequent 2017 amendments to the Federal Rules of Evidence that address them.

The groundbreaking series of opinions in 2003 from *Zubulake v. UBS Warburg LLC* demonstrated the need for the 2006 amendments to the Federal Rules of Civil Procedure.[26] Briefly, the *Zubulake* case dealt with a discrimination suit against a former employer in which the plaintiff requested hundreds of email records that the defendant only partially complied with.[27] The attorney for the defense mistakenly believed that the emails in question had been "archived" when, in reality, the employee who wrote the emails had simply saved them to a folder where they were later deleted.[28] The defendant then claimed that the cost and volume of the documents had created an undue burden as many were inaccessible or deleted, and the cost of finding and reviewing the backups was over $300,000.[29] Ultimately, the court modified the existing "inaccessibility"

---

22. *See id.* at 10.

23. Samantha V. Ettari, *Sanctions Under Amended FRCP 37(e): One Year In*, PRAC. L., Dec. 2016/Jan. 2017, at 14, https://www.kramerlevin.com/images/content/1/7/v4/1748/Sanctions-Under-Amended-FRCP-37-e-One-Year-In-Sam-Ettari.pdf.

24. *See* Kenneth J. Withers, *Electronically Stored Information: The December 2006 Amendments to the Federal Rules of Civil Procedure*, 4 NW. J. TECH. & INTELL. PROP. 171, 181–183 (2006).

25. *Id.* at 172–73.

26. Zubulake v. UBS Warburg LLC, 217 F.R.D. 309 (S.D.N.Y. 2003).

27. *Id.* at 312.

28. *Id.* at 311–12.

29. *Id.* at 313.

test and created a new seven-factor test for e-discovery disputes.[30] It then found that many of the undisclosed emails were not inaccessible and instructed the jury that they were permitted to assume the missing emails would not have favored the defendant.[31] The court also imposed monetary sanctions on the defendant and, in combination with the damages, the plaintiff won almost $30 million.[32] This result epitomized the confusion on the applicable standard for ESI discovery. Thus, it is clear why the amendments to the Federal Rules of Civil Procedure—arriving one year after *Zubulake*—focused on "parties' legitimate worries about sanctions, production costs, and the burdens and expenses of privilege review."[33]

The 2006 amendments created ESI as an independent form of discovery evidence.[34] They further developed new rules of procedure to govern ESI discovery, including an exception for ESI if the court deems the requested ESI to be not reasonably accessible to the producing party.[35] The remaining changes attempted to clarify the obligations of companies in preserving and later producing requested ESI.[36] The amendments created "safe harbor" periods for ESI that was destroyed or lost in the regular course of business by a data storage system.[37]

The early 2006 amendments to the Federal Rules of Civil Procedure were an acknowledgement by the Advisory Committee of the expanding use of ESI. Courts attempted to work around the outdated rules and create common law that could process electronic evidence. Instead, confusion abounded, and it took formal amendments to standardize and stabilize the courts. Today, the admissibility of ESI is similarly hindered by the antiquity of the Evidence Code. In the case law that follows, attempts are made to create common law to authenticate ESI for admissibility, and these attempts are similar to those discussed above relating to discovery.

One of the earlier examples of courts fitting ESI into the boundaries of the Rules of Evidence is *In re Vee Vinhnee*.[38] In the opinion, the court stated that "[a]uthenticating a paperless electronic record, in principle,

---

30. *Id.* at 321–24.

31. Zubulake v. UBS Warburg LLC, 229 F.R.D. 422, 439–40 (S.D.N.Y. 2004).

32. Eduardo Porter, *UBS Ordered to Pay $29 Million in Sex Bias Lawsuit*, N.Y. TIMES (Apr. 7, 2005), https://www.nytimes.com/2005/04/07/business/ubs-ordered-to-pay-29-million-in-sex-bias-lawsuit.html.

33. Rachel Hytken, *Electronic Discovery: To What Extent Do the 2006 Amendments Satisfy Their Purpose?*, 12 LEWIS & CLARK L. REV. 875, 880 (2008).

34. FED. R. CIV. P. 26(b)(2)(B).

35. *Id.*

36. *See id.* 34(b) advisory committee's note to 2006 amendment; *id.* 37(f) advisory committee's note to 2006 amendment.

37. *Id.* 37(e) (2006) (repealed 2015).

38. 336 B.R. 437 (B.A.P. 9th Cir. 2005).

poses the same issue as for a paper record . . . ."[39] However, the court then went into great detail as to how a proper foundation may be laid to authenticate ESI using principles from Rules 901 and 902.[40] For a point of reference, the court looked to Professor Imwinkelried's writings on digital paperless business records as scientific evidence and lists eleven steps that are generally appropriate to lay foundation.[41] Many of these steps, however, are deceptively simple, such as a showing that "the computer" from which the ESI is pulled "is reliable."[42] Thus, the *In re Vee Vinhnee* court minimized the unique challenge of authentication rather than relying on a workable, scientific approach for future guidance.[43] This analysis shows the striking incongruity between a perceived simplicity of handling ESI with the current Rules and the attempt at creating a new scientific methodology to accomplish this goal.

The landmark case of *Lorraine v. Markel American Insurance Co.* reflects the continued entanglement of the Rules of Evidence when applied to ESI.[44] The key issue dealt with the language of an arbitration agreement to settle an insurance claim on a destroyed yacht.[45] The judge dismissed both the plaintiff's and defendant's motions for summary judgment, stating that neither party had entered enough evidence.[46] In summary judgment, only evidence that would be admissible in court can be relied upon, but neither party offered anything to support the authentication of the emails.[47] *Lorraine* was a realization of the extra steps required for authentication when dealing with ESI.[48] The failure of either side to fit ESI into the Rules of Evidence as they existed at the time—particularly Rule 901—was a major contributor to the ultimate inadmissibility of the parties' evidence.[49]

As ESI has developed, the rules governing it have been slow to evolve alongside it. Before discussing the 2017 amendments to the Rules of Evidence, it will be useful to give context for the previously detailed irregularities of ESI by noting the Rules of Evidence regarding authentication as they existed prior to the 2017 amendments. Following this, the 2017 additions and any potential implications they may have concerning Rule 902 will be analyzed.

---

39. *Id.* at 444.
40. *Id.* at 446–47.
41. *Id.*
42. *See id.* at 446.
43. *Id.* at 444–45
44. *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534 (D. Md. 2007).
45. *Id.* at 535.
46. *Id.* at 537.
47. *Id.* at 535.
48. *See id.* at 542–43.
49. *See id.* at 541–42.

II. THE EVOLUTION

As with anything involving the Federal Rules of Evidence, the authentication process is a multi-layered interplay between several different rules. To best understand the process, it will be helpful to start broadly with the language of Rule 104. Rule 104(a) states: "The court must decide any preliminary question about whether a witness is qualified, a privilege exists, or evidence is admissible. In so deciding, the court is not bound by evidence rules, except those on privilege."[50] Generally, Rule 104(a) means that a judge makes the first determination of admissibility based on the offered support of authenticity, and the question goes to a jury only if it becomes reasonable to believe that the condition has not been met.[51]

The difficulty begins with Rule 104(b), which reads: "When the relevance of evidence depends on whether a fact exists, proof must be introduced sufficient to support a finding that the fact does exist. The court may admit the proposed evidence on the condition that the proof be introduced later."[52] This has been interpreted to mean that when the fact used to prove authenticity under Rule 104(a) is disputed, extrinsic evidence must be brought in.[53] This may sound like a niche scenario, but this situation occurs much more frequently when dealing with ESI. For example, an email or text message can fall under 104(b) if the authorship is asserted by one party but denied by the other.[54] No evidence of handwriting analysis or possession of a physical copy is available. In this situation, a judge may allow the evidence before the jury and hear testimony as to its authenticity while instructing the jury to disregard it if they are not convinced.[55]

More commonly, judges may require additional authenticity support for ESI evidence even if it is not a Rule 104(b) fact issue due to the skepticism of this form of information.[56] It is important to note that this form of proving authentication is distinct from that of a Rule 104(b) factual dispute. In the latter situation, the trial judge is still the decision-maker.[57] However, when the judge has allowed the evidence before a jury to hear testimony as to its authenticity, the party attempting

---

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

51. *Id.* 104 advisory committee's notes to 1972 proposed rule.

52. *Id.* 104(b).

53. *See id.* 104 advisory committee's notes to 1972 proposed rule.

54. *See id.*

55. *See* Paul W. Grimm et al., *Authenticating Digital Evidence*, 69 BAYLOR L. REV. 1, 5 (2017).

56. *See id.* at 6.

57. *See* Symposium, *The Challenges of Electronic Evidence*, 83 FORDHAM L. REV. 1163, 1175–76 (2014).

to enter the exhibit must turn to Rule 901.[58] Rule 901(a) states: "To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is."[59] Rule 901(b) offers a list of ways in which a party may authenticate its evidence to the judge.[60] Which of the listed methods is most appropriate depends on what type of evidence the party is attempting to admit.[61] Rule 902 also plays a role here, as it provides a list of things that are considered "self-authenticating."[62] This will be explored later due to its importance to the 2017 amendment.

In relation to the differences in ESI and traditional evidence discussed in Part I, many digitally created documents fall under Rule 901.[63] It is uncommon that a piece of ESI would be deemed inadmissible by a judge because the threshold for authenticity is low.[64] However, costs can become very burdensome when there is a high volume of ESI and the authentication is at issue.[65] ESI, like social media postings or chat room conversations, are often created through anonymous usernames or third parties.[66] Emails are at a notoriously high risk of being hacked and may require testimony towards authorship.[67] Similarly, text messages require testimony of authorship and are easily deleted.[68] The number of witnesses required to prove a threshold level of authenticity has become increasingly cumbersome and expensive as the world becomes increasingly more digitized.

When the Advisory Committee on Evidence met in 2017, there was once again an emphasis on reducing the costs associated with handling ESI.[69] Primarily, this meant reducing the number of witness testimonies required.[70] As previously mentioned, Rule 902 also governs the authentication of evidence.[71] Rule 902 lists several different types and methods of self-authenticating evidence, which require no extrinsic evidence, such as testimony, to support them.[72] Before the 2017

58. *See id.* at 1173.
59. FED. R. EVID. 901(a).
60. *Id.* 901(b).
61. *See id.*
62. *Id.* 902.
63. *Id.* 901(a).
64. Grimm et al., *supra* note 55, at 11–12.
65. *See id.* at 12.
66. *Id.* at 22.
67. *Id.* at 12–13.
68. *Id.* at 19.
69. *Id.* at 38.
70. *Id.*
71. FED. R. EVID. 902.
72. *Id.*

amendments, Rule 902 had only limited use for ESI. For example, Rule 902(11) often admitted emails as regularly conducted business activity, similar to the business record exception to hearsay.[73]

However, the Rule 902 options did not neatly identify any types of ESI and frequently led to unworkable results. In *United States v. Browne*, incriminating messages were sent on Facebook and the prosecutor sought to admit them.[74] In order to authenticate these messages, the prosecutor brought in a certification of a records custodian from Facebook.[75] The custodian testified to the fact that storing Facebook messages was a regularly conducted activity as allowed in Rule 902(11).[76] The court held that this testimony made no showing that the defendant was actually the one who authored the messages as the custodian had no personal knowledge.[77] The court noted that this form of testimony would authenticate the metadata in the messages and the timestamp of when they were sent and received, but not the content of the messages.[78]

Similarly, some of the provisions of Rule 902 have had their language stretched to adapt to and include more reliable forms of ESI.[79] This had been the pre-2017 amendment trajectory to ease ESI litigation expenses without having to change or alter the Federal Rules of Evidence. For example, in *Williams v. Long*, the plaintiffs submitted printed webpages from a government website as evidence and offered no support for their authentication.[80] When determining whether to admit the webpages, the court turned to Rule 902(5) and summarized that Rule as allowing "extrinsic evidence of authenticity as a condition precedent to the admissibility of evidence is not required if the evidence is a book, pamphlet, or other publication purporting to be issued by a public authority" to be self-authenticating.[81] The court latched on to the words "public authority" and "other publication,"[82] interpreting these phrases to mean that "if information is published on a website by a public authority and that information is obtained through the FOIA (or, as in this case, an equivalent state act), then that printed information would be self-authenticating under Rule 902(5).[83]" Thus, websites from legitimate

73. Kevin F. Brady et al., *The Sedona Conference Commentary on ESI Evidence & Admissibility*, 9 SEDONA CONF. J. 217, 220–21 (2008).

74. United States v. Browne, 834 F.3d 403, 405–06 (3d Cir. 2016).

75. *Id.* at 408.

76. *Id.*

77. *Id.* at 410.

78. *Id.* at 411.

79. *See* Grimm et al., *supra* note 55, at 11–33.

80. Williams v. Long, 585 F. Supp. 2d 679, 682 (D. Md. 2008).

81. *Id.* at 686.

82. *Id.*

83. *Id.* at 690.

government agencies have traditionally been found to be self-authenticating under Rule 902(5).[84]

Similarly, courts have interpreted Rule 902(6) to allow self-authentication of online newspaper articles.[85] Rule 902(6) allows "[p]rinted material purporting to be a newspaper or periodical."[86] However, Rule 101(b)(6) permits any mention of printed materials within the Rules to also mean and relate to comparable information in electronic form.[87] Thus, there is no requirement that the online newspaper have ever been printed.[88]

These complex solutions to fit ESI into the Rules of Evidence serve as a backdrop for the 2017 amendments, which made multiple additions to the Federal Rules of Evidence.[89] However, this Note focuses on the addition of two new subsections of Rule 902, which deal directly with self-authenticating ESI. The new additions read as follows:

> **(13) Certified Records Generated by an Electronic Process or System.** A record generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent must also meet the notice requirements of Rule 902(11).
>
> **(14) Certified Data Copied from an Electronic Device, Storage Medium, or File.** Data copied from an electronic device, storage medium, or file, if authenticated by a process of digital identification, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent also must meet the notice requirements of Rule 902(11).[90]

In their simplest form, these additions were made to alleviate much of the interpretive tap-dancing described above.[91] While very little is ever

---

84. *See id.*; FED. R. EVID. 902(5).

85. *See, e.g.*, White v. City of Birmingham, 96 F. Supp. 3d 1260, 1274 (N.D. Ala. 2015) (admitting newspaper articles from the *Huntsville Times* website into evidence as self-authenticating); *see also* PAUL W. GRIMM ET AL., BEST PRACTICES FOR AUTHENTICATING DIGITAL EVIDENCE 17 (2016).

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

87. *Id.* 101(b)(6).

88. GRIMM ET AL., *supra* note 85, at 17.

89. Carey Busen, *It's the End of Authentication (of ESI) as We Know It*, DISCOVERY ADVOCATE (Nov. 29, 2017), https://www.discoveryadvocate.com/2017/11/29/its-the-end-of-authentication-of-esi-as-we-know-it/. In addition to changes to Rule 902, the Amendment also changed portions of the hearsay exception for ancient documents under Rule 803. *Id.*

90. FED. R. EVID. 902(13)–(14).

91. *See supra* Part II.

easy in the Rules of Evidence, the understanding was that, at this point in technological usage, not all ESI is created equal. The allowance of certain more obvious or credible ESI to fit into Rule 902 provisions, such as those discussed above, are an acknowledgment of that fact.

The largest effect these amendments were meant to accomplish relates back to the 2006 amendments. Previously, the 2006 amendments sought to shift the burden of e-discovery costs and ESI litigation back to the requesting party.[92] In a similar fashion, the 2017 amendments have shifted the burden of authentication back to the party opposing the admission.[93] Traditionally, the party seeking to admit ESI had the burden of producing testimony to show authenticity; however, this was considered inefficient.[94] Often, "the expense and inconvenience of producing a witness to authenticate an item of electronic evidence is often unnecessary because the adversary either stipulates to authenticity before the witness is called or fails to challenge the authentication testimony once it is presented."[95] Now, with the mechanisms discussed below, most types of ESI can be more easily authenticated prior to trial and the party opposing it may object if they can show the ESI is not authentic. It is also important to note that the processes used for self-authentication in Rules 902(13) and (14) only work towards certifying authenticity; the evidence is still subject to all other appropriate objections.[96]

This discussion has provided a look at the Rules of Evidence related to ESI, an explanation of how they operate, and early attempts to make ESI conform to them. This discussion demonstrated the necessity of the two added provisions to Rule 902 presented and analyzed above. Part III will focus on projecting how these new Rules will work with the old ones and suggest implementation strategies.

III. THE IMPLEMENTATION

The primary mechanism to the new provisions of Rule 902 is a certificate of authenticity that complies with the three certification requirements of Rule 902 under sections (11) and (12)[97]: "First, the record was made at or near the time by, or from information transmitted by, someone with knowledge. Second, the record was kept in the course of a

92. Bradley T. Tennis, Comment, *Cost-Shifting in Electronic Discovery*, 119 YALE L.J. 1113, 1113–14 (2010).

93. *See* Paul W. Grimm, *Recent Changes to Federal Rules of Evidence: Will They Make It Easier to Authenticate ESI?*, 19 SEDONA CONF. J. 707, 709 (2018).

94. *See id.*

95. *Id.* at 715.

96. Ramona L. Lampley, *Something Old and Something New: Exploring the Recent Amendments to the Federal Rules of Evidence*, 57 WASHBURN L.J. 519, 528 (2018).

97. FED. R. EVID. 902(13)–(14).

regularly conducted activity of a business, organization, occupation, or calling. Third, making the record was a regular practice of that activity."[98] However, due to the nature of ESI, the affiant must additionally certify aspects of the electronic storage and transmission processes involved in obtaining the ESI to meet the chain of custody requirements under Federal Rules of Evidence 401 and 901.[99] This certificate does not alleviate any of the actual requirements to show authenticity—it merely allows parties to prove authenticity before any hearings and without the need to bring in witnesses.[100] A more detailed discussion of what types of information should be included in the certification of ESI under the new Rules is provided below.

Rule 902(13) deals more specifically with the certification of the electronic process or system that stores ESI.[101] The proponent of the evidence must have a qualified person certify that the system is reliable and can accurately store the information.[102] Generally, the certificate should describe the system that generated the ESI, the process used to collect and preserve the data within the system that eventually produced the ESI, and the method used to take the ESI from the system to present it for evidence.[103]

Rule 902(14) uses a similar method for proving authenticity but for a different purpose. The focus of Rule 902(14) is to authenticate ESI that is a copy of a paperless digital information source.[104] One of the most important aspects to understanding how anyone can verify a digital copy of digital information is through the use of "hash values."[105] These hashes serve as digital fingerprints: when a document matches the hash value of its proposed source, it is an exact duplicate.[106] Thus, hash values should be included in the certification affidavit along with a description of the recording time and date, the method used to make the copy, and any software used.[107] If a qualified person verifies this information under oath, a judge can properly assume that the ESI is authentic without the

98. Edward T. Kang et al., *Self-Authentication of ESI Under Federal Rule of Evidence 902*, LEGAL INTELLIGENCER (June 21, 2018), https://www.law.com/thelegalintelligencer/2018/06/21/self-authentication-of-esi-under-federal-rule-of-evidence-902/.

99. *Id.*

100. *See* Carl Aveni, *New Federal Evidence Rule Changes Reflect Modern World*, LITIG. NEWS, Sping 2018, at 10.

101. FED. R. EVID. 902(13).

102. *Id.*

103. Grimm, *supra* note 93, at 720–21.

104. FED. R. EVID. 902(14).

105. *See id.* 902(14) advisory committee's note to 2017 amendment; Dennis Martin, *Demystifying Hash Searches*, 70 STAN. L. REV. 691, 700 (2018).

106. Martin, *supra* note 105, at 695, 699.

107. *See* Kang et al., *supra* note 98.

need for witness testimony. While these steps sound simple, the practice of preserving and collecting this information is complicated and easily ruined if not handled properly.

Furthermore, under Rules 902(13) and (14), the offering party must meet Rule 902(11) requirements for giving notice to opposing counsel of their intent to offer ESI at trial.[108] The opposing counsel may choose not to challenge the certification, thus eliminating the need for the qualified person who wrote the affidavit to be brought to court and questioned. However, there is still the opportunity to challenge authenticity or the described system.[109] If the certificate is challenged, the qualified person will be required to testify at trial and is subject to cross-examination as a witness.[110] Thus, many, if not all, of the original hurdles for authenticating ESI still exist, but the work can be done in a more efficient and inexpensive way.

These amendments should streamline the authentication of ESI, and their implementation can be illustrated using two separate examples. In the first example, the cellphone of a criminal defendant is seized and properly searched, resulting in the recovery of incriminating text messages. Prior to the amendments, the prosecutor would have to bring in a forensic technician to testify as to the way cellphones track and store messages with timestamps and metadata.[111] With the newly added Rule 902(13), the court should allow the forensic technician to provide the same information in an affidavit certifying the authenticity.[112]

Similarly, in the second example, if a forensic technician instead made a copy of the cellphone's text message logs, Rule 902(14) could be implemented.[113] Again, prior to these amendments, the technician would have to testify as to how the copies are authentic duplicates.[114] However, Rule 902(14) now allows this to be done well before trial and enables the authentication of the evidence while barring any objection from opposing counsel.[115]

With these new amendments in place as of December 2017, many aspects of the Federal Rules of Evidence have been altered to accommodate ESI. The specific focus of this Note has been the authentication issue revolving around ESI. Much has been written here and elsewhere as to why the use of ESI in litigation is such a financial and time-consuming burden, but have these amendments done enough to

---

108. *See* FED. R. EVID. 902(13)–(14).
109. Grimm, *supra* note 93, at 721.
110. *Id.*
111. *See id.* at 718–19.
112. *Id.*
113. Lampley, *supra* note 96, at 531–32.
114. *See id.*
115. FED. R. EVID. 902(14) advisory committee's note to 2017 amendments.

resolve these problems? The answer is that same repeated law school phrase: "it depends."

These amendments are still very new, but they will likely have a positive influence on authenticating ESI. In a situation where one party offers a relatively routine type of electronic data as evidence and the other party does not plan to challenge it, these amendments will save both sides time and money. They serve as a useful primer for the discussion of this Note. However, they are not the final solution. These amendments resolve only a niche set of circumstances. The answer cannot be to add self-authenticating provisions in an exhaustive list to all varieties of ESI. Technology will continue to advance, and attempting to make a comprehensive authentication list will only become a more complex proposition. Inevitably, the Rule amendments will lag behind the advancements in ESI usage as data storage further evolves.

One thing these amendments have not fixed is the chain of custody problem, which still exists. The chain of custody shows all the places a piece of evidence has been stored and who has had access to or control of the evidence, how it got to be stored where it is, and the condition it is in compared to its original form.[116] Chain of custody becomes even more complex when dealing with ESI.[117] The primary difference between ESI and paper documents is that ESI often deals with copies and almost never originals.[118] A single file such as an email or PDF can be copied hundreds of times—through routine backups, for example—before it becomes relevant evidence. Each time a piece of ESI is copied, its integrity is threatened—authentication not only becomes more important, but also more difficult. When a piece of ESI must be certified, having it collected by a client or improperly transmitted between hardware systems could ruin the hash value or invalidate the accuracy of the system in which it was stored.[119] Clients may unwittingly create such interference before they ever consult with an attorney. Unfortunately, once this chain has been "tampered" with, it may effectively be permanently broken.[120]

In actuality, the solution to litigating with ESI cannot be contained within a rule change—the problems are not solely a product of antiquated rulemaking. An almost equal contributing factor lies in the antiquated practice methods of ESI. Too often, attorneys will request more

116. Helen Geib, *Chain of Custody and Its Critical Role in Authenticating Electronic Evidence*, QDISCOVERY, https://qdiscovery.com/chain-of-custody-critical-role-authenticating-electronic-evidence/ (last visited Oct. 21, 2018).

117. *See id.*

118. *See id.*; DANIEL GARRIE & YOAV M. GRIVER, DISPUTE RESOLUTION AND E-DISCOVERY § 5:2 (2013).

119. *See* U.S. DEP'T OF JUSTICE, FORENSIC EXAMINATION OF DIGITAL EVIDENCE: A GUIDE FOR LAW ENFORCEMENT 11 (1994), https://www.ncjrs.gov/pdffiles1/nij/199408.pdf.

120. *See* Busen, *supra* note 89.

e-discovery documents than they require to elevate costs of litigation.[121] Parties will also challenge the obvious authenticity of evidence to force opposing counsel to prepare and present a witness.[122]

The resolution must come from a more comprehensive and fundamental approach to the treatment of ESI. These rules represent the end handling of ESI when the emphasis should be more on the preliminary phases of authentication. Companies who frequently endure litigation and already direct large amounts of funds to the use of ESI can take several steps to avoid authentication issues.

One of the most important steps that a company can take is to create a team of people trained to handle ESI. With so many complexities to the preservation and use of ESI, a team with diverse expertise could better approach the task. Members from the information technology department, legal offices, and management can all offer insight into this process. Anyone who handles ESI without expertise could invalidate easy methods of authentication, so this team could reduce the risk of mishandling or ruining ESI.

As part of this team's responsibilities, the team members should create a written policy for the proper storing of ESI. The moving, copying, or collection of ESI should be monitored and tracked by an appointed employee. These uses should be recorded either in written form or through software designed to make similar recordings. The rights to alter or forward emails can be managed to prevent email tampering or distribution to unauthorized personnel, which would diminish authenticity.[123] Similarly, systems such as Microsoft Azure Information Protection keep backup files secure and reliable on a cloud server so that copies can be accurately compared to the stored originals for authentication.[124] Further, companies should be concerned with the security of their ESI and future review processes. Finally, firewalls and

---

121. *See* Jayme L. Walker & Tilak Gupta, *E-Discovery for Plaintiffs' Lawyers*, PLAINTIFF, Nov. 2015, at 39, https://www.plaintiffmagazine.com/images/issues/2015/11-november/Plaintiff-Nov15-issue.pdf.

122. *See* Busen, *supra* note 89.

123. ORACLE, INFORMATION RIGHTS MANAGEMENT—MANAGING INFORMATION EVERYWHERE IT IS STORED AND USED 10 (2009), https://www.oracle.com/technetwork/middleware/webcenter/content/irm-10g-technical-whitepaper-129901.pdf; Ajmal Kohgadai, *What Is Information Rights Management (IRM)?*, MCAFEE, https://www.skyhighnetworks.com/cloud-security-blog/what-is-information-rights-management-irm/ (last visited May 14, 2019) (describing IRM as a category of software that allows assignment of permissions to certain employees for use of certain types of ESI within a company).

124. *See* LOGIKCULL, THE ULTIMATE GUIDE TO EDISCOVERY 47, 52, https://www.logikcull.com/public/files/The-Ultimate-Guide-to-eDiscovery.pdf (last visited June 9, 2019).

antivirus software can be employed to prevent outside intrusion into ESI and maintain its reliability.[125]

Companies should look at how and where their ESI is being stored to effectively tailor these protections and procedures to the specific medium being used. For example, documents accessible to the internet should be given protections like Network Access Protection (NAP) to ensure they are not corrupted.[126] Meanwhile, ESI stored on disks or portable hard drives should use the most secure file systems.[127]

One of the most difficult aspects of ESI is related to how difficult it can be to review the sheer volume of all the available documents.[128] Today, there are several different data forensic programs developed for the specific purpose of reviewing ESI electronically to reduce the cost and time it takes when documents are requested in discovery.[129] Some of these programs, such as LexisNexis Concordance, use keyword searches to quickly scan stored ESI.[130] When companies have made use of these types of services, courts have been more lenient and taken a reasonableness approach to the errors made when presenting all relevant ESI.[131]

One final solution involves coordination. As courts have begun to use a more case-by-case analysis of what is reasonable for accessibility and authentication,[132] companies should begin creating definitive boundaries for themselves. Similar industries should join one another in creating standards for the maintenance and use of ESI. In this way, a court may look more favorably upon ESI stored in compliance with these standards and be more likely to accept authentication proof for all types of ESI.[133] These industry guidelines would also help reduce the costs involved with ESI by eliminating disputes over authentication objections. Such coordination is not uncharted territory. Medical societies and the

---

125. Deb Shinder, *Documenting Authenticity of Evidence for the E-Discovery Process*, TECHGENIX (July 16, 2008), http://techgenix.com/documenting-authenticity-evidence-e-discovery-process/.

126. *See id.*

127. *Id.*

128. *See* GARRIE & GRIVER, *supra* note 118.

129. *See What Is eDiscovery Software?*, LOGIKCULL, https://www.logikcull.com/what-is-ediscovery-software (last visited June 9, 2019).

130. *See Faster, Easier E-Discovery Review: The New Concordance Desktop*, LEXISNEXIS (Feb. 1, 2016), http://businessoflawblog.com/2016/02/ediscovery-concordance-desktop/.

131. *See* Steven Bennett, *E-Discovery: Reasonable Search, Proportionality, Cooperation, and Advancing Technology*, 30 JOHN MARSHALL J. INFO. TECH. & PRIVACY L. 433, 453, 463 (2014).

132. *See id.* at 435 n.8.

133. *See id.* at 453, 463.

respective bar association committees have joined to create guidelines for the admission and use of medical experts and evidence in trials.[134]

CONCLUSION

The authentication of ESI is not a new challenge. Since the creation of digital information, the laws governing it have been struggling to keep up. It is simply too difficult for the rulemaking process to grow and evolve at the same rate as technology. The 2006 amendments marked an acknowledgement of the new form of paperless documents; the 2017 amendments are a concession to their growing prevalence.

As courts begin to implement these amendments and the full breadth of their impact becomes clear, litigators must also change. The proposed methods of use for the 2017 amendments discussed in this Note constitute the first step in solving ESI authentication challenges. However, the strategies given in the final portion of this Note describe a culture shift in how companies and their respective counsel use ESI. Understanding the unconventionality of ESI and its growing impact should be a goal of every litigation firm and is the main purpose of this Note.

134. *See generally* N.C. BAR ASS'N MEDICO-LEGAL LIAISON COMM., MEDICO-LEGAL GUIDELINES (2014), https://www.ncmedsoc.org/wp-content/uploads/2013/06/Medico-Legal-Guidelines-2014.pdf.