The Sedona Conference Commentary on ESI Evidence & Admissibility, Second Edition

The Sedona Conference

THE SEDONA CONFERENCE COMMENTARY ON ESI EVIDENCE & ADMISSIBILITY, SECOND EDITION

A Project of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1)

Author:

The Sedona Conference

Editors-in-Chief & WG1 Steering Committee Liaisons:

Kevin F. Brady
Heather Kolasinsky
Philip Favro

Drafting Team:

Carey Busen
Gita Radhakrishna
Holly Dyer
Kristin Walinski
Endel (Del) Kolde
Martin Wolf
Jonathan Le

Judicial Participants:

Hon. Ralph Artigliere (ret.)
Hon. Thomas Vanaskie (ret.)

Judicial Advisor:

Hon. Paul W. Grimm

Staff editors:

David Lumia
Susan McClain

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The

Sedona Conference Working Group 1. They do not necessarily represent the views of any of the individual participants or their employers, clients, or any other organizations to which any of the participants belong, nor do they necessarily represent official positions of The Sedona Conference.

We thank all of our Working Group Series Annual Sponsors, whose support is essential to our ability to develop Working Group Series publications. For a listing of our sponsors, just click on the "Sponsors" navigation bar on the homepage of our website.

This publication may be cited as follows:

> The Sedona Conference, *Commentary on ESI Evidence & Admissibility, Second Edition*, 22 SEDONA CONF. J. 83 (2021).

PREFACE

Welcome to the final, October 2020, version of The Sedona Conference C*ommentary on ESI Evidence & Admissibility, Second Edition*, a project of the Sedona Conference Working Group 1 on Electronic Document Retention and Production (WG1). This is one of a series of Working Group commentaries published by The Sedona Conference, a 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, intellectual property rights, and data security and privacy law. The mission of The Sedona Conference is to move the law forward in a reasoned and just way.

This is the second iteration of The Sedona Conference *Commentary on ESI Evidence & Admissibility.* The first edition was published in March 2008 to address a concern at that time about whether and how electronically stored information (ESI), once produced, can actually be authenticated and used as evidence at trial or in motion practice. The 2008 edition provided a framework, practical guidance, and a checklist for authenticating ESI and getting it admitted into evidence. That 2008 *Commentary* focused primarily on the applicability and application of the Federal Rules of Evidence and case law to the existing data sources at that time, as well as addressing the potential issues and pitfalls for data sources that were looming on the horizon. Much has changed in the past 12 years, and this second edition reflects those changes.

In 2017 and 2019, the Federal Rules of Evidence were amended. In contrast to the fanfare accompanying the changes to the Federal Rules of Civil Procedure in 2006 and 2015, little attention was paid to the 2017 changes to Federal Rules of Evidence 803(16), 807, and 902(13) and (14). Those changes are significant and intended to influence how parties manage ESI. For example, the changes to Rule 803(16) address authentication of

digital information that has been stored for more than 20 years, eliminating the concern that factual assertions made in massive volumes of ESI will be admissible for the truth simply because of their age. The concurrent addition of new subsections (13) and (14) to Rule 902 provide for streamlined authentication of ESI and potentially eliminate the need to call a witness at trial to authenticate the evidence. As we note at the end of this *Commentary*, future developments in the law and ever-changing landscape of technology may warrant another iteration.

An update to the 2008 edition of the *Commentary on ESI Evidence & Admissibility* was a topic of dialogue at the WG1 2018 Annual and 2019 Midyear meetings, and drafts of this *Commentary* were circulated for member comment at the 2019 Midyear Meeting and again in early 2020. This second edition was published for public comment in July 2020. Where appropriate, the comments received during the public-comment period have been incorporated into this final version of the *Commentary*. The Sedona Conference acknowledges the efforts of Editors-in-Chief and Steering Committee Liaisons Kevin F. Brady, Philip Favro, and Heather Kolasinsky, who were invaluable in driving this project forward. We also thank Drafting Team members Carey Busen, Holly Dyer, Del Kolde, Jonathan Le, Gita Radhakrishna, Kristin Walinksi, and Martin Wolf, as well as The Honorable Ralph Artigliere (ret.), The Honorable Thomas Vanaskie (ret.), and The Honorable Paul Grimm for their efforts and commitments in time and attention to this project.

We encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG1 and several other Working Groups in the areas of international electronic information management, discovery, and disclosure; patent damages and patent litigation best practices; data security and privacy liability; trade secrets; and other "tipping point" issues in the law.

The Sedona Conference hopes and anticipates that the output of its Working Groups will evolve into authoritative statements of law, both as it is and as it should be. Information on membership and a description of current Working Group activities is available at https://thesedonaconference.org/wgs.

Craig Weinlein
Executive Director
The Sedona Conference
October 2020

TABLE OF CONTENTS

I. INTRODUCTION

The ability to present admissible evidence is an essential skill for successful litigators. At its core, admissibility is about what evidence may be considered by the decision-maker. Many civil cases settle, but they settle at different stages of the litigation process. Summary judgment proceedings and pretrial motion practice often, if not always, require a party to offer admissible evidence for a proposition, claim, or defense. If a civil case is not resolved before trial, a judge or jury will decide the merits of the case, which will also require the presentation of admissible evidence. Criminal cases, on the other hand, which are more likely to go to trial, may result in a higher number of reported decisions regarding electronically stored information (ESI) evidence,[1] primarily due to the lack of pre-trial discovery of devices in criminal cases.[2]

The growth of electronic discovery reflects the increasing digitization of information in society, which also results in more relevant evidence being sourced from ESI. This phenomenon means that successful litigators must understand how to get ESI admitted into evidence, which is a different question than preserving or gathering it for discovery. As U.S. District Judge Paul W. Grimm noted in the seminal case *Lorraine v. Markel American Insurance Co.*, "it makes little sense to go to all the bother and

1. As used in this *Commentary*, evidence means "material presented to a competent legal tribunal to prove or disprove a fact." *See* BRYAN A. GARNER, GARNER'S DICTIONARY OF LEGAL USAGE 34 (1987). Most ESI that exists, or is collected and produced in discovery, will never be promoted to the status of evidence submitted before a tribunal. The focus of this *Commentary* is on the small subset of ESI that will be offered as evidence.

2. Criminal cases may also lead to more reported decisions because many defense counsel may perceive an ethical duty not to stipulate to the admissibility of ESI evidence that will be used to attempt to convict their client. Different incentives to cooperate may prevail in civil cases.

expense" of electronic discovery only to have that evidence excluded when it really matters.[3] This *Commentary* focuses specifically on that concern.

This *Commentary* is divided into three parts. First, there is a survey of the application of existing evidentiary rules and case law addressing the authenticity of ESI. Second, there are discussions about new issues and pitfalls that are looming on the horizon such as ephemeral data, blockchain, and artificial intelligence. Finally, there is practical guidance on admissibility and the use of ESI in depositions and in court.

While this *Commentary* primarily addresses the Federal Rules of Evidence, the overwhelming volume and the widest diversity in types and size of cases occur in state courts, where the subject-matter jurisdiction is much broader. Space prohibits state-by-state coverage, but this *Commentary* compares the federal law and principles to rules of evidence and admissibility arising in state court. Guidance for addressing state court admissibility occurs throughout this *Commentary*.

3. 241 F.R.D. 534, 538 (D. Md. 2007). *Lorraine* remains a frequently cited case on ESI admissibility, with nearly 1,600 citing references on WestlawNext.

II. APPLYING EXISTING RULES AND CASE LAW TO ESI EVIDENCE

A. Early Focus on Authentication and Evidentiary Issues

Judge Grimm's discussion in *Lorraine* makes it clear that parties should start to think about evidentiary issues much earlier than was the practice when dealing only with hard-copy evidentiary materials. Consideration should be given to how potential ESI evidence is handled by records management programs, and parties should be mindful of authentication possibilities throughout the discovery process. For example, under the pretrial disclosure provisions of Rule 26(a)(3), a party has 14 days to object to the admissibility of an opponent's proposed documents of other trial exhibits, and the failure to do so results in a waiver. Additionally, given the extent to which summary judgment has displaced trial as a procedure for resolving legal disputes, parties should be prepared to deal with evidentiary issues at the summary judgment stage.

B. Summary Judgment Motions and ESI Evidence

Summary judgment is a critical stage in any litigation and is likely the first time that issues of evidence admissibility, including authenticity, will be considered, because the court is only allowed to consider evidence that is admissible.[4]

This point was made clear in *Lorraine,* where the court rejected unsworn, unauthenticated documents from both parties. As the Judge Grimm explained, the court could only consider evidence at summary judgment that would be admissible at trial.[5] Judge Grimm also detailed how the Rules:

---

4. Celotex Corp. v. Catrett, 477 U.S. 317, 322 (1986); FED. R. CIV. P. 56(c); *see also* Gannon Int'l, Ltd. v. Blocker, 684 F.3d 785, 793 (8th Cir. 2012).

5. The Court in *Celotex* noted that under Rule 56(e), a party can oppose summary judgment using any of the evidentiary materials identified in Rule

> 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 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.[6]

56(c), except for the pleadings themselves, and it is from that list (which includes affidavits) that one would normally expect the nonmoving party to make that showing. *Celotex*, 477 U.S. at 324. However, that is not always the case. If the content of the affidavit would not be admissible if it is offered into evidence at trial by a live witness, then it is not considered admissible evidence for summary judgment purposes notwithstanding the fact that it is in an acceptable form for Rule 56(c) purposes. FED. R. CIV. P. 56(c).

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

C. Authentication Tools: Rules 104, 901, and 902

Authenticity is one part of admissibility, requiring that the proponent of an exhibit "make a prima facie showing that it is what he or she claims it to be."[7] The comparatively recent additions of Federal Rule of Evidence 902(13) and (14) provide additional tools for the authentication of ESI, including system metadata and files such as an email or an Excel spreadsheet.

1. Rule 104

There is a complex interplay between "preliminary rulings" on admissibility, governed by Rules 104(a) and (b), and the authenticity determination, governed by Rules 901 and 902. Rule 104(a) governs the admissibility of matters such as whether an expert is qualified and, if so, whether the expert's opinions are admissible; whether the evidence is privileged; and whether evidence is hearsay, and, if so, whether any recognized exception applies.[8] As explained in *Lorraine*, under Rule 104(a), the court, not the fact finder, makes the admissibility determination. In making that determination, the court is not bound by the restrictions of the rules of evidence except those concerning privileges.[9]

On the other hand, the authenticity of ESI and other evidence is governed by Rule 104(b), which affords the court a much narrower role. Under this rule, the court addresses only a threshold question of law: does the evidence have sufficient probative value to sustain a rational jury finding that the evidence is what the proponent claims it to be? The fact finder makes the ultimate determination of whether the evidence is authentic.

---

7. *Id.* at 542.
8. *See id*. at 539.
9. *Id*.

For example, if an email is offered into evidence, the jury makes the authenticity determination under Rule 104(b) using only admissible evidence.[10]

2. Rules 901 and 902

Examples of methods a proponent may use to authenticate ESI are set forth in Rules 901 and 902. Just as with hard-copy evidence, a "party seeking to admit an exhibit need only make a prima facie showing that it is what he or she claims it to be."[11] This is not a particularly high barrier to overcome.

In *United States v. Safavian*, the court analyzed the admissibility of email, noting that:

> [t]he question for the Court under Rule 901 is whether the proponent of the evidence has "offered a foundation from which the jury could reasonably find that the evidence is what the proponent says it is." The Court need not find that the evidence is necessarily what the proponent claims, but only that there is sufficient evidence that the *jury* ultimately might do so.[12]

---

10. *Id*. at 540.

11. *Id*. at 542.

12. United States v. Safavian, 435 F. Supp. 2d 36, 38 (D.D.C. 2006) (internal citations omitted) (emphasis in original); *see also* Dunn v. Hunting Energy Servs., 288 F. Supp. 3d 749, 764 (S.D. Tex. 2017) (citing *Lorraine* and admitting emails); United States v. Bertram, 259 F. Supp. 3d 638, 640, 642–43 (E.D. Ky. 2017) (citing *Lorraine* and *Safavian* and admitting emails).

The first edition of this *Commentary* included a discussion of an eleven-factor authentication test for computerized records adopted by the U.S. Bankruptcy Appellate Panel of the Ninth Circuit in *In re Vinhnee*, 336 B.R. 437, 446–47 (B.A.P. 9th Cir. 2005). The more stringent test applied in that case has been omitted from this edition of the *Commentary* because it has rarely been cited outside the Ninth Circuit, and the analysis is discussed in only a

It is important to note that the methods for authentication listed in Rules 901 and 902 are non-exhaustive and can be used in combination with each other, although, as discussed below, courts have identified particular provisions of 901 and 902 that are appropriate or most useful for specific types of ESI.

Rule 902[13] identifies evidence that is "self-authenticating," that is, information that can be admitted at trial without being authenticated by a witness. Self-authenticating evidence may be admissible without extrinsic evidence of authenticity "sometimes for reasons of policy but perhaps more often because practical considerations reduce the possibility of unauthenticity to a very small dimension."[14] Most, but not all, of the items listed in Rule 902 are self-authenticating on their face, thus requiring no extrinsic evidence of authenticity for the document to be admitted. There are sections of Rule 902—such as Rule 902(11) and Rule 902(12) (for records of regularly conducted activity, domestic and foreign, respectively), 902(13) (records generated by an electronic process or system), and 902(14) (data copied from an electronic device)—that are self-authenticating *only* to the extent the party seeking to introduce them into evidence submits a proper certification to their authenticity and provides notice to the opposing party to give it a fair opportunity to challenge the certification.

---

few reported decisions. Cautious practitioners may nevertheless want to be aware that *In re Vinhnee* can be cited to support a more stringent authentication standard, including proving the existence of access control and an audit trail. In general, however, the courts have become more comfortable with authenticating ESI over the past decade.

13. The following discussion (up to Section D) is taken with permission from Hon. Paul W. Grimm & Kevin F. Brady, *Recent Changes to Federal Rules of Evidence: Will They Make It Easier to Authenticate ESI?*, 19 SEDONA CONF. J. 707, 711–21 (2018).

14. FED. R. EVID. 902 advisory committee's notes to 1972 proposed rules.

3. Rules 902(13) and (14)

In 2017, the Advisory Committee supplemented Rule 902 by adding two subsections permitting similar certifications to authenticate electronic evidence. The amendments are intended to eliminate the need for a live witness to testify as to the authenticity of certain ESI, thereby streamlining the process at trial.

The new subsections to Rule 902 are:

> (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 by a qualified person that complies with the certification requirements of Rule 902(11) or Rule 902(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 by 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).

As with the provisions on business records in Rules 902(11) and 902(12), the Advisory Committee noted that 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.[15] Under the amendments to Rule 902, the parties are now able to determine in advance of trial whether a real challenge to authenticity will be made.

Note that Rule 902(11) relates "only to the procedural requirements" of authentication.[16] Likewise, new subsections 902(13) and (14) are designed to do "nothing more than authenticate" ESI.[17] Therefore, the proponent of the evidence sought to be admitted still must prove the requirements of Rule 803(6) after clearing the authenticity hurdle. What is important to note from Rules 902(13) and (14) is that the references to Rules 902(11) and (12) are simply to the form of the declaration: the affidavit the party wishes to introduce must have the same formality and style as the certifications referred to in Rules 902(11) and (12). Rules 902(13) and (14) do not require that the certification for subsections (13) and (14) to include the substantive certification of Rule 902(11), which is tied to Rule 803(6)(A)(B)(C) elements for the business-record exception.

New subsections 13 and 14, like Rules 902(11) and (12), permit a foundation witness or "qualified person" to establish the authenticity of information by way of certification.[18] Subsection 902(13) provides for self-authentication of machine-generated information—such as system metadata—upon the submission

---

15. FED. R. EVID. 902 advisory committee's notes to 2017 amendments ¶¶ 13 & 14.

16. *Id.*

17. ADVISORY COMMITTEE ON EVIDENCE RULES, MINUTES OF THE MEETING OF APRIL 29, 2016, https://www.uscourts.gov/sites/default/files/2016-04-evidence-minutes_0.pdf.

18. Pursuant to Rule 901(11) and 901(12), a "qualified person" is a custodian or other individual who has the ability to establish the authenticity of the ESI as if that person would have testified at trial such as under FED. R. EVID. 901(b)(1) (Testimony of a Witness with Knowledge) or 901(b)(4) (Distinctive Characteristics and the Like).

of a certification prepared by a qualified person. Subsection 902(14) provides for authentication of data copied from an electronic device, medium, or file—such as an email or Excel spreadsheet that was stored on a computer—through digital identification.

The Advisory Committee noted that in most instances, digital identification involves authentication of data copied from electronic devices by comparing the "hash value" of the proffered copy to that of the original document. A message-digest hash value is a unique alphanumeric sequence of characters that an algorithm determines based upon the digital contents of the device.[19] The hash value serves as the digital fingerprint that a qualified person uses to compare the numeric value of the proffered item with the numeric value of the original item. If the hash values for the original and copy are identical, the information can be proffered, and the court can rely on them as authentic copies.[20] The Advisory Committee also noted that "[t]he rule is flexible enough to allow certifications through processes other than comparison of hash value, including by other reliable means of identification provided by future technology."[21]

New Rules 902(13) and 902(14) have the same effect as other Rule 902 provisions of shifting to the opponent the burden of going forward—but not the burden of proof—on authenticity disputes regarding the electronic evidence at issue. Shifting the burden of questioning the authenticity of such records to the opponent who has a fair opportunity to challenge both the certification and the records streamlines the process by which these items can be authenticated, thereby reducing the time, cost, and

19. FED. R. EVID. 902 advisory committee's notes to 2017 amendments ¶ 14. *See* Section III.B.1, *infra*, for a more detailed definition of "hashing."

20. *Id*.

21. *Id*.

inconvenience of presenting this evidence at trial or summary judgment.

Rule 902(13) is designed to permit the proponent to show that the evidence in question is authentic by attaching an affidavit under oath by the person or people with the technical or specialized knowledge of how the system or process works, certifying that the evidence is reliable and accurate.[22]

Rule 902(14) allows for a certification that would explain the process by which that person took a forensic copy of the evidence such as a hard drive of a laptop, hashed it, and then compared the hash value of the forensic copy with the hash value of the original hard drive. Certification is an affidavit or declaration by someone with firsthand, personal knowledge or with qualified expertise under Rule 702. If the original hash value and the hash value of the forensic copy are the same, then the information in the copy is identical to the information in the original.

For example, if an individual takes a picture with a smartphone, embedded within the electronic metadata of that photograph are global positioning system (GPS) coordinates of the location where that photograph was taken. In a criminal case, where the prosecution must prove that the defendant was in a specific location by virtue of photographs taken from that defendant's mobile phone, the metadata from that electronic photograph that shows the GPS coordinates is evidence of where the smartphone and (by extension) the person were located when the picture was taken.

---

22. S*ee* United States v. Forty-Febres, No. 16-330, 2018 WL 2182653, at *2 (D.P.R. May 11, 2018) *appeal docketed*, No. 18-2106 (1st Cir. Nov. 17, 2018) (granting motion *in limine* to admit electronic records of the Puerto Rico Department of Transportation based upon a certification from the custodian of the records).

Under the Rule, the prosecutor can put that information in an affidavit and offer the affidavit to the defendant with the request to voice any objection regarding authenticity. If the defendant objects, the prosecutor must actually prove the authenticity and will need to bring one or more witnesses—persons with the scientific, technical, or specialized knowledge—to testify at trial how the system and processes produce reliable results.[23] If the defendant does not object, the prosecutor has established authenticity and no authenticating witness would be needed at trial. Unless qualified as an expert under Rule 702, the affiant must provide information based on direct personal knowledge. The affiant's testimony cannot be based on hearsay. Moreover, if the proponent has a system or process that requires explanation by multiple persons in order to be complete, affidavits are needed from each of those persons.

4. Rule 902(13) and (14) Certifications

A Rule 902 certification is intended to take the place of the testimony traditionally required to establish the authenticity of the ESI sought to be admitted; therefore, it should follow the same pattern as the testimony it is intended to replace.[24] The certification should start by establishing the background, education, training, and expertise of the affiant in order to establish

23. Criminal cases involving such certifications can also raise Confrontation Clause issues. *Compare* Melendez-Diaz v. Massachusetts, 557 U.S. 305, 329 (2009) ("The Sixth Amendment does not permit the prosecution to prove its case via *ex parte* out-of-court affidavits. . .") *with* United States v. Yeley-Davis, 632 F.3d 673, 681 (10th Cir. 2011) (Rule 902(11) certifications of authenticity concerning certified copies of telephone toll records are not testimonial and therefore do not violate the Sixth Amendment Confrontation Clause). Thus, there may be a distinction between records generated specifically for a prosecution and historic records that pre-existed a legal dispute.

24. *See* Grimm & Brady, *supra* note 13, at 740 for sample certifications under Rules 902(13) and 902(14).

that the affiant is a "qualified person" as required by Rules 902(11) and (12). Although Rules 902(13) and (14) do not refer to Rule 702, counsel would be wise to ensure that the affiant providing the certificate meets the requirements of an expert witness under Rule 702 if the underlying facts to be authenticated involve scientific, technical, or specialized knowledge. The added benefit of showing that the affiant meets these Rule 702 requirements is that the affiant may base the certification on information beyond personal knowledge, provided it is reliable, as described in Rule 703. The certification should then describe the affiant's role in the case, that is, that the affiant was retained by the party as a computer forensics expert to assist the party and its counsel in the identification, preservation, collection, and production of ESI. The certification should describe in detail the evidence in question and establish its authenticity consistent with the formality requirements of Rules 901(11) and (12). The certification need not meet the requirements of Rule 803(6)(A–C), unless the proponent also seeks to qualify the evidence as a business record. Instead, the certification must provide the information required by Rules 902(13) and (14), as discussed below.

If the certificate seeks to authenticate evidence under Rule 902(13), the affiant should describe in detail the "electronic process or system" that was used to generate the information in question. For example, if the information in question is a series of monthly sales reports, the affiant should describe: (i) the system from which the reports were generated; (ii) the process by which the data that was used to generate the statements was gathered, processed, and stored; and (iii) the process by which the statements or reports sought to be admitted were generated and produced for the litigation. The Rule 902(13) certificate should establish that the information sought to be admitted has not been altered from the form in which it was maintained in the ordinary course of business. While the process of preparing

a certification under Rule 902 is seemingly straightforward, the affiant must be careful to describe the "electronic process or system" with enough specificity to satisfy the court and the opponent of the evidence's authenticity. Doing so can help avoid a hearing during which the opponent of the evidence may cross-examine the affiant.[25]

If the certificate seeks to authenticate evidence under Rule 902(14), the affiant also should describe in detail the ESI that was copied from its original location and now offered into evidence. The affiant should additionally detail the steps taken by the affiant at the time of duplication (including recording the date, time, surrounding circumstances, and hardware and software tools as well as versions utilized). For example, if the information sought to be admitted comprises a series of Excel and PowerPoint files that were stored on the departmental file share for the client's accounting department, the affiant should list the files in question and include the hash value of each of the files as they existed on the file share. The affiant should also describe the hash value for the copy of each of the files sought to be admitted to establish that the files are authentic copies of the files as they were maintained in the ordinary course of business. The identical hash values will attest that the information sought to be admitted into evidence is a true and correct copy of the information as it existed in its original state.

D. Various Types of ESI Require Different Approaches

All ESI shares certain common characteristics, but some types of ESI present unique challenges to authentication, necessitating different approaches. For example, the creator of certain

25. *See* La Force v. Gosmith, Inc., No. 17-cv-05101-YGR, 2017 WL 9938681, at *3 (N.D. Cal. Dec. 12, 2017) (deeming an attorney's declaration submitted in support of printouts of web pages insufficient to meet the requirements of Rule 902(13)).

ESI types may be unidentifiable, and the ESI may be stored in various systems with different security measures. Some ESI may contain clues about its history, while other types are completely lacking in provenance. It is thus useful to quickly survey some representative categories of ESI.

1. Email

For many organizations, email remains the primary form of business communication.[26] Other forms of electronic communication, including various forms of instant messaging, are also increasingly part of the mix, but email is still predominant.

There are many ways in which email evidence may be authenticated:

- a witness with personal knowledge—Rule 901(b)(1)
- expert testimony or comparison with authenticated examples—Rule 901(b)(3)
- distinctive characteristics, including circumstantial evidence—Rule 901(b)(4)
- a system or process capable of proving a reliable and dependable result—Rule 901(b)(9)
- trade inscriptions—Rule 902(7)
- certified copies of a business record—Rule 902(11)
- certified records generated by an electronic process or system—Rule 902(13)

26. "The total number of business and consumer emails sent and received per day will exceed 306 billion in 2020, and is forecast to grow to over 361 billion by year-end 2024." THE RADICATI GROUP, INC., EMAIL STATISTICS REPORT, 2020-2024 EXECUTIVE SUMMARY 2 (FEB. 2020), https://www.radicati.com/wp/wp-content/uploads/2019/12/Email-Statistics-Report-2020-2024-Executive-Summary.pdf.

- certified data copied from an electronic device, storage medium, or file—Rule 902(14)[27]

The addition of two new subsections to Rule 902 gives practitioners additional options for authenticating emails or metadata associated with emails, although admissibility will still need to be established.[28] For example, under Rule 902(13), an email could qualify as data copied from a storage medium, which could be digitally authenticated by a qualified person. Similarly, under 902(14), system metadata could be used to authenticate an attachment to an email as a record generated by an electronic process or system.

(a) Email as a business record

In litigation involving business entities or government agencies, many emails will potentially qualify as business records, allowing a proponent to establish both authenticity and admissibility by meeting a single test. But it is insufficient to "simply [] say that since a business keeps and receives emails, then *ergo* all those e-mails are business records falling with the ambit of [the business records exception]."[29]

Longstanding Rule 902(11) is particularly "helpful in establishing the foundation elements for a business record without the need to call a sponsoring witness to authenticate the document and establish the elements of the hearsay exception." This, in turn, allows a proponent to establish both authenticity and a

27. *See* Appendix D: Checklist of Potential Authentication methods, *infra*.

28. *See* Section II.C, *supra*.

29. United States v. Cone, 714 F.3d 197, 220 (4th Cir. 2013) (ruling that emails concerning counterfeit goods were improperly admitted). *But see* Alig v. Quicken Loans Inc., No. 5:12-CV-114, 2017 WL 5054287, at *8 (N.D.W. Va. July 11, 2017) (finding that executives' emails qualified as business records).

major component of admissibility.[30] Rule 902(11) allows the self-authentication of a business record. The proponent must produce an original or 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.[31]

Because the elements for Rules 902(11) and 803(6) are essentially the same, they frequently are analyzed together when Rule 902(11) is the proffered means by which a party seeks to admit a business record.[32]

With respect to the "personal knowledge" component of Rule 803(6) (that there be personal knowledge of the entrant or of an informant who had a business duty to transmit the information to the entrant), it is relatively simple to prove personal knowledge if the author of the email is available to testify and

---

30. Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 571 (D. Md. 2007). Rule 803(6) is often referred to as the business-records exception to the hearsay rule and presents a common way for gaining admissibility of ESI evidence in civil cases involving companies and other organizations that maintain business records.

31. *Id*.

32. *Id*. at 572.

had personal knowledge of the contents. But in many instances, the email contains information from a source outside the business of the maker of the business record, which presents special evidentiary problems.

In *Lorraine*, the court noted that the majority view for meeting the requirements of the business-record exception in that situation is that the supplier or source of the information memorialized in the email must have had "a business duty to transmit the information to the maker of the record, if the maker, him or herself lacks personal knowledge of the facts or events."[33] "However, some courts have held that it may be possible to meet the requirements of the business-record exception even if the source of the information had no business duty to provide it to the maker of the record, provided the recipient of the information has a business duty to verify the accuracy of the information provided."[34]

In addition, it may be useful for litigants to establish the elements of the business-records exception for high-value emails during depositions, prior to offering them as evidence in a court. If a manager or party representative admits, in a deposition, to having sent or received an email in the course of regularly conducted business activity, that manager's employer will be hard-pressed to challenge authenticity at a later stage in the lawsuit.

---

33. *See id.* at 571 n.52 (citing FED. R. EVID. 803(3) advisory committee's note ("Sources of information presented no substantial problem with ordinary business records. All participants, including the observer or participant furnishing the information to be recorded, were acting routinely, under a duty of accuracy, with employer reliance on the result, or in short 'in the regular course of business.' If, however, the supplier of the information does not act in the regular course, an essential link is broken; the assurance of accuracy does not extend to the information itself, and the fact that it may be recorded with scrupulous accuracy is of no avail.")).

34. *Id*. (citing Rambus, Inc. v. Infineon Techs. AG, 348 F. Supp. 2d 698, 706–07 (E.D. Va. 2004)).

Depositions, however, may not always have taken place, and they would not ordinarily be available in criminal cases.

Finally, in civil cases, a party may be precluded from challenging the authenticity of ESI that it produced during discovery. Some courts have held that "[parties] cannot voluntarily produce documents and implicitly represent their authenticity and then contend they cannot be used by the [opposing party] because the authenticity is lacking."[35] In practice, however, this rule may not always apply, especially if a party is in possession of records it did not generate. For example, an email received from an outside entity might be subject to discovery and production, but it would not necessarily be appropriate to imply that the producing party had a definitive position on the identity of the sender or the authenticity of the document. Similarly, if a party originally received the ESI from an opposing party and then subsequently produced it back to the opposing party in accordance with a new discovery request or a duty to supplement, it would not necessarily follow that the party was claiming that the ESI was authentic.

(b) Authenticating emails using circumstantial evidence

In a nonbusiness context or other situations where an email does not qualify as a business record, practitioners can often authenticate emails with circumstantial evidence by reference to distinctive characteristics in the contents of the email.[36] For

35. Indianapolis Minority Contractions Ass'n, Inc. v. Wiley, IP 94-1175-C-T/G, 1998 WL 1988826, at *6 (S.D. Ind. May 13, 1998), *aff'd sub nom.* Indianapolis Minority Contractors Ass'n, Inc. v. Wiley, 187 F.3d 743 (7th Cir. 1999). *See also* Radiance Capital Receivables Eighteen, LLC v. MBO Investments, LLC, 4:16-CV-1921-SPM, 2019 WL 330463, at *4 (E.D. Mo. Jan. 25, 2019).

36. FED. R. EVID. 901(b)(4).

example, an email might contain "details known only to the sender and the person receiving the message."[37]

Thus, in *United States v. Safavian*, emails between the defendant and a lobbyist were sufficiently authenticated because both persons' names were part of the respective email user names. In addition, the contents of the emails referred to matters the lobbyist or defendant were known to be working on.[38]

Similarly, when it comes to the next step, admissibility, there are numerous options for nonbusiness records. Frequently, an email may be the statement of a party opponent, which is not hearsay.[39] Even where an email contains non-party statements, they might not be hearsay at all. For example, in *Safavian*, the court held that email content from a lobbyist was non-hearsay because the lobbyist asked questions, sought favors, or made requests for assistance rather than making declarative statements about the truth of a matter.[40] Likewise, in *United States v. Fluker*,

37. *Lorraine*, 241 F.R.D. at 554.

38. United States v. Safavian, 435 F. Supp. 2d 36, 40–41 (D.D.C 2006) (emails admissible as admissions of a party opponent and non-hearsay); *see also* United States v. Fluker, 698 F.3d 988, 998–1000 (7th Cir. 2012) (email addresses were consistent with purported senders and contents showed sender had knowledge of relevant issues); United States v. Bertram, 259 F. Supp. 3d 638, 642–43 (E.D. Ky. 2017) (witness with history of email exchanges with defendants could authenticate emails based on distinctive characteristics); Johnson v. State, 137 A.3d 253, 271–74 (Md. Ct. Spec. App. 2016), *cert. denied*, 146 A.3d 471 (Md. 2016) (email contents referred to personal and family circumstances specific to defendant).

39. FED. R. EVID. 801(d)(2); *see also Lorraine,* 241 F.R.D. at 568 (noting the universality of electronic communication and the application of the party opponent rule); *Safavian*, 435 F. Supp. 2d at 43–44 (admitting emails containing statements directly attributed to defendant and forwarded emails where context showed they were adoptive admissions).

40. *Safavian*, 435 F. Supp. 2d at 44–45.

the emails contained fraudulent statements that, by definition, were not offered for the truth of the matter asserted.[41]

2. Text Messages

Text messages are frequently used to communicate in business and nonbusiness settings but occupy a less formal space than email. This is because the communications are often shorter, may be sent and received on personally owned devices, and may exist outside of formal information governance policies. As a result, text messages may not be considered business records even if they relate to the business of a particular organization.

There are many ways in which text messages may be authenticated:

- a witness with personal knowledge—Rule 901(b)(1)
- expert testimony or comparison with authenticated examples—Rule 901(b)(3)
- distinctive characteristics, including circumstantial evidence—Rule 901(b)(4)
- a system or process capable of proving a reliable and dependable result—Rule 901(b)(9)
- trade inscriptions—Rule 902(7)
- certified copies of a business record—Rule 902(11)
- certified records generated by an electronic process or system—Rule 902(13)
- certified data copied from an electronic device, storage medium, or file—Rule 902(14)

41. 698 F.3d at 998–1000.

In practice, the authentication and admissibility of text messages are handled just like email. A key question is often whether the purported sender actually sent the text, which is a subset of authentication. In other words, is the text what its proponent claims: a message sent by a named person to another person at a specific date and time. Absolute certainty is not required. For example, in a criminal prosecution for gun running, the government used circumstantial evidence to authenticate texts that were taken off an iPhone, which was in the defendant's possession at the time of his arrest, and a Samsung device found in his room.[42] One phone listed the defendant's nickname—"Big Dave"—in the properties section, and both phones contained information in the contacts directory associated with the defendant, including the defendant's mother under the heading "Mom."[43] Moreover, the texts sent by him were nonhearsay admissions of a party opponent.[44] Similarly, in another case, the government authenticated text messages where a witness testified that although she was not certain that the defendant authored the messages, she had talked to him at the phone number that was the source of the texts, and the content indicated that they were from the defendant.[45]

Texts can also present unique questions of collection and preservation. Unlike emails, texts do not ordinarily reside on an enterprise server, nor are they typically foldered or archived for long-term retention. Often the simplest way to facilitate preservation of messages is for users to harvest or collect them from their own smartphones. Recipients wishing to retain texts in a legal dispute have resorted to various means of preservation,

42. United States v. Lewisbey, 843 F.3d 653, 657–58 (7th Cir. 2016).

43. *Id*. at 658.

44. *Id*.

45. United States v. Barnes, 803 F.3d 209, 217 (5th Cir. 2015).

including cutting and pasting screenshots into emails or word-processing files that are then offered into evidence. These methods predictably elicit an authentication objection. As long as a witness with personal knowledge can testify as to the process used to generate the secondary document or image and assert that it accurately reflects the content of the text messages, courts have tended to find that authenticity was sufficiently established for the issue to go the jury.[46] Similarly, courts in these situations have not usually required the presentation of reliable chain-of-custody procedures or elaborate forensic processes.

3. Websites

"Websites are inherently changeable," which can make them difficult to authenticate.[47] The most well-known approach to preserving web pages is the screen capture or variations on it, such as creating a PDF (portable document format) image or preserving a site through application programming interfaces (APIs). For static web pages—those that lack any interactive features or features personalized to the viewer, these methods might suffice; they do, at least, provide a view of what the web page looked like at that moment on that browser. However, it is easy to manually alter hypertext before capture or to manipulate PDF files and other screenshots after capture using software like Photoshop.[48] Moreover, API captures may miss significant

46. *See* United States v. Arnold, 696 F. App'x 903, 906–07 (10th Cir. 2017) (reflecting testimony from the witness who explained that he copied text messages into another document); United States v. Ramirez, 658 F. App'x 949, 952 (11th Cir. 2016) (memorializing testimony from a witness who indicated the photographs of text messages were pictures from her phone).

47. Supermedia LLC v. Law Firm of Asherson, No. 2:12-CV-03834, 2013 WL 12113386, at *3 (C.D. Cal. Feb. 13, 2013).

48. *See, e.g.*, Leidig v. BuzzFeed, Inc., No. 16 Civ. 542, 2017 WL 6512353, at *2 (S.D.N.Y. Dec. 19, 2017) (finding that the plaintiffs produced "documents

chunks of data, and many companies have withdrawn their APIs in response to data security threats and breaches.[49] Even so, if the court and parties can access the current version of the web page and it has not changed, then there is no authenticity issue.[50] But this is rarely the case given the dynamic nature of today's websites.[51]

Modern websites pose complicated authentication problems because no longer are they static pages of images and text. Today, 95 percent of websites incorporate JavaScript,[52] a tool that developers use to create interactive web elements such as chat boxes, dropdown menus, and other personalized content. To ensure that this interactive website evidence remains admissible, something more than screenshots or PDF captures is required to view, preserve, and authenticate it.

Authentication issues typically include what the actual content of the web page was at a particular point in time, whether the exhibit or testimony accurately reflects this content and, if

---

bearing no metadata, including manually manipulated PDFs, summaries of underlying documents not produced, and screenshots and other text files").

49. *See, e.g.*, Mike Schroepfer, *An Update on Our Plans to Restrict Data Access on Facebook*, FACEBOOK, (Apr. 4, 2018), https://newsroom.fb.com/news/2018/04/restricting-data-access/.

50. *See* United States v. Bari, 599 F.3d 176, 180 (2d Cir. 2010) (noting that a judge can conduct a "basic internet search" to confirm the authenticity of current website content).

51. *See, e.g.*, Adobe Sys. Inc. v. Christenson, No. 2:10-cv-00422-LRH-GWF, 2011 WL 540278, at *9 (D. Nev. Feb. 7, 2011) ("Although Defendants can probably determine, with little difficulty, whether a *current* Google search for the search terms 'software surplus' provides links on the first page for the 'resellerratings.com' and 'Eopinions.com' websites, this would not prove that such a search would have resulted in such a link at a prior point in time.").

52. *Usage of JavaScript for Websites as client-side programming language on websites*, W3TECHS, https://w3techs.com/technologies/details/cp-javascript (last visited May 5, 2020).

so, whether the content is attributable to the site owner.[53] Alternatively, parties can authenticate a web page through the personal knowledge of a person who created or who maintains the website.[54]

In addressing these evidentiary problems, the authentication rules most likely to apply include the following:

- a witness with personal knowledge—Rule 901(b)(1)
- expert testimony or comparison with authenticated examples—Rule 901(b)(3)
- distinctive characteristics, including circumstantial evidence—Rule 901(b)(4)
- a system or process capable of proving a reliable and dependable result—Rule 901(b)(9)
- certified records generated by an electronic process or system—Rule 902(13)
- certified data copied from an electronic device, storage medium, or file—Rule 902(14)

Typically, the witness will need to testify or certify that the witness typed in the web address at the date and time on an exhibit, that the witness reviewed the contents of the web page, and that the exhibit is a fair and accurate reflection of what the

53. *See* Supermedia LLC v. Law Firm of Asherson, No. 2:12-CV-03834, 2013 WL 12113386, at *3 (C.D. Cal. Feb. 13, 2013) ("A purported printout of the content of a website on a past date requires proof from someone with actual knowledge that the printout is in fact what would have been viewed if the website had been accessed at the stated time period.").

54. St. Luke's Cataract & Laser Inst., P.A. v. Sanderson, No. 8:06-cv-223-T-MSS, 2006 WL 1320242, at *2 (M.D. Fla. May 12, 2006) (finding that a webmaster's testimony can authenticate a website printout).

witness saw.[55] The exhibit should include two things: the web page's internet address and the date and time the web page contents were downloaded.[56]

A point of contention is "whether a website's owner, webmaster, or author is necessary to authenticate a web posting when its relevancy depends on its accuracy or its author."[57] In determining authenticity, courts may consider circumstantial evidence in determining whether the content of the website was posted by the site's owner under Rule 901(b)(4).[58] This evidence can include whether the website has a distinctive design or specific logos, photos, or images that are linked to the website or its

55. *See, e.g.*, SMS Audio, LLC v. Belson, No. 16-81308-CIV, 2107 WL 1533971, at *3 (S.D. Fla. Mar. 20, 2017) ("[C]ourts generally permit the authentication of web postings, bearing a web address and the date printed, by a witness who saw and printed the postings 'for the limited purpose of proving that the postings had appeared on the world wide web on the days that [the witness] personally saw the postings and printed them off the computer.'") (quoting Saadi v. Maroun, No. 8:07-cv-1976-T-24 MAP, 2009 WL 3736121, at *4 (M.D. Fla. Nov. 4, 2009)); Estate of Konell v. Allied Prop. & Cas. Ins. Co., No. 3:10-cv-955-ST, 2014 WL 11072219, at *1 (D. Or. Jan. 28, 2014) ("To authenticate a printout of a web page, the proponent must offer evidence that: (1) the printout accurately reflects the computer image of the web page as of a specified date; (2) the website where the posting appears is owned or controlled by a particular person or entity; and (3) the authorship of the web posting is reasonably attributable to that person or entity.").

56. *See, e.g.*, Foreword Magazine, Inc. v. OverDrive, Inc., No. 1:10-cv-1144, 2011 WL 5169384, at *3 (W.D. Mich. Oct. 31, 2011) (admitting website screenshots based on an attorney's sworn affidavit plus "other indicia of reliability (such as the Internet domain address and the date of printout)").

57. *SMS Audio, LLC*, 2017 WL 1533971, at *4; *see also* United States v. Browne, 834 F.3d 403, 413–15 (3d Cir. 2016) (ruling that Facebook chats are sufficiently authenticated by circumstantial evidence that the defendant was the author), *cert. denied*, 137 S. Ct. 695 (2017).

58. *See* Hon. Paul W. Grimm, et al., *Authenticating Digital Evidence*, 69 BAYLOR L. REV. 1, 26 (2017).

owner.[59] Courts may also evaluate whether the contents of the proffered web pages are of the kind typically posted on similar websites, whether the site owner wholly or partially published the website content elsewhere, whether the contents have been otherwise republished elsewhere and attributed to the proffered website, or the length of time that the website content was posted.[60]

Another popular—if limited—method of authentication is the Wayback Machine. Launched in 2001 by the nonprofit Internet Archive, the Wayback Machine is a digital archive of the web. Courts have occasionally taken judicial notice of the contents of these archived sites.[61] Some courts have permitted an Internet Archive witness to testify about the reliability of the Wayback Machine's results under 901(b)(9).[62] Now, the reliability of the Wayback Machine process may be established by a certificate of an Internet Archive official under Rule 902(13).

Although the Wayback Machine captures information, what it actually memorializes is inconsistent. The archive may not

---

59. *See, e.g.*, Metcalf v. Blue Cross Blue Shield of Mich., No. 3:11-cv-1305-ST, 2013 WL 4012726, at *10 (D. Or. Aug. 5, 2013) (finding that authenticity of website information of an organization's purported website was established by logos or headers matching those of the organization), *cited in* Grimm, et al., *supra* note 58, at 26.

60. *See* Grimm, et al., *supra* note 58, at 26.

61. *See, e.g.*, Under a Foot Plant, Co. v. Exterior Design, Inc., No. 6:14-cv-01371-AA, 2015 WL 1401697, at *2 (D. Or. Mar. 24, 2015) ("District courts have routinely taken judicial notice of content from The Internet Archive . . . .").

62. *See, e.g.*, Specht v. Google Inc., 747 F.3d 929, 933 (7th Cir. 2014) ("[T]he district court reasonably required . . . authentication by someone with personal knowledge of reliability of the archive service from which the screenshots were retrieved."); Open Text S.A. v. Box, Inc., No. 13-cv-04910-JD, 2015 WL 428365, at *2 (N.D. Cal. Jan. 30, 2015) (refusing to admit a Wayback Machine screenshot into evidence without testimony from an Internet Archive representative confirming its authenticity).

capture all of a website's content. Moreover, users can ask that the archive delete or change information. This led at least one court to find that a party could not show that data from the archive was "reliable, complete, and admissible in court."[63] As a result, the Wayback Machine is not accepted as a forensic evidence collection method.[64]

The ISO 28500 WARC (Web ARChive) standard, established by the International Internet Preservation Consortium, addresses authentication issues by making it possible to obtain an exact native file of the collected content of a website.[65] A WARC file is a container for all accessed web resources and metadata; it is a collection of records, each of which relates to an element of a web page. A web crawler or similar program captures the data, stores the data in a WARC file, and generates relevant metadata about the capture that confirms the data's integrity. The saved data is an identical replica of the website, with working links, graphics, and other dynamic content. The saved website also records every possible server request and the answer to that request, along with all of the supporting metadata to establish the authenticity of its information. Some software timestamps and hashes each event in the collection, simplifying the process of establishing a chain of custody and facilitating authentication.[66]

---

63. *See* Leidig v. BuzzFeed, Inc., No. 16 Civ. 542, 2017 WL 6512353, at *13 (S.D.N.Y. Dec. 19, 2017).

64. *Id*.

65. International Organization for Standardization, *ISO 28500:2017: Information and Documentation— WARC File Format*, https://www.iso.org/standard/68004.html (last visited May 5, 2020).

66. For example, Hanzo Archives offers a WARC native file copy of web content with its Preserve service. *See* Hanzo Archives, *eDiscovery for the Interactive Age*, https://www.hanzo.co/ediscovery-software-0 (last visited May 9, 2020).

For certain websites, authentication is a simpler matter. Three types of website evidence are self-authenticating under Rule 902. Under Rule 902(5), federal, state, local, and international government websites are self-authenticating, and courts typically take judicial notice of these sites.[67] Under Rule 902(6), online newspapers and periodicals are self-authenticating.[68] Finally, business records kept in the ordinary course of business that satisfy Rule 803(6) are self-authenticating.[69]

Courts may also take judicial notice of other reputable websites, such as internet maps,[70] calendars,[71] the publication of articles in newspapers and periodicals,[72] and online versions of textbooks, dictionaries, rules, and charters.[73] Note that courts

---

67. *See, e.g.*, Williams v. Long, 585 F. Supp. 2d 679, 686–88 & n.4 (D. Md. 2008) (collecting cases indicating that posts on government websites are self-authenticating).

68. *See, e.g.*, White v. City of Birmingham, 96 F. Supp. 3d 1260, 1274 (N.D. Ala. 2015) (noting that online news articles are "analogous to traditional newspaper articles and could be found self-authenticating at trial").

69. *See, e.g.*, United States v. Hassan, 742 F.3d 104, 132–34 (4th Cir. 2014) (finding social media posts, including links to videos, were self-authenticating under Rule 902(11) where accompanied by "certifications of records custodians of Facebook and Google, verifying that the Facebook pages and YouTube videos had been maintained as business records in the course of regularly conducted business activities."). *See* Section II.D.1.a, *supra*.

70. *See, e.g.*, United States v. Burroughs, 810 F.3d 833, 835 n.1 (D.C. Cir. 2016) (granting a motion to take judicial notice of a Google map).

71. *See, e.g.*, Tyler v. United States, No. 1:08-CR-165-CC & No. 1:11-LV-4592-CC, 2012 WL 6808525, at *3 n.6 (N.D. Ga. Dec. 6, 2012).

72. *See, e.g.*, Ford v. Artiga, No. 2:12-CV-02370, 2013 WL 3941335, at *7 n.5 (E.D. Cal. July 30, 2013) (taking judicial notice of the fact of publication but not of the articles' content).

73. *See, e.g.*, Williams v. Emp'rs Mut. Cas. Co., 845 F.3d 891, 905 (8th Cir. 2017) (taking judicial notice of a dictionary); Morgan Stanley Smith Barney LLC v. Monaco, No. 14-cv-00275-RM-MJW, 2014 WL 5353628, at *2 (D. Colo. Aug. 26, 2014) (taking judicial notice of FINRA rules).

have declined to accord the same courtesy to the crowdsourced Wikipedia, finding it "not sufficiently reliable."[74]

4. Social Media Sites

(a) What is social media?

"Social media" is a broad and imprecise term encompassing a range of platforms, applications, and tools that permit users to share information with others, typically in an internet-based environment.[75] Since their introduction in the early 2000s, social media applications and platforms have been constantly changing and expanding. Although even the traditional platforms differ from site to site, their basic feature is social networking—the ability to connect with other people and share content.[76] Platforms like Facebook, Twitter, and LinkedIn allow people to "friend," "follow," or "retweet" each other and to share comments, photos, videos, and events. YouTube, Snapchat, and Instagram provide for similar social interaction, with the focus on sharing photos and videos. Dating apps like Tinder, Bumble, and Grindr also provide opportunities for online (and real life) social connection.

Social media has expanded into territory previously occupied by SMS text messaging. Over-the-top (OTT) messaging applications use the internet and travel directly from device to device instead of going through servers belonging to SMS

74. *See, e.g.*, Blanks v. Cate, No. 2:11-cv-0171 WBS CKD P., 2013 WL 322881, at *3 n.3 (E.D. Cal Jan. 28, 2013). *But see* United States v. Bazaldua, 506 F. 3d 671, 673 n.2 (8th Cir. 2007) (court took judicial notice of an article in Wikipedia).

75. *See* The Sedona Conference, *Primer on Social Media, Second Edition*, 20 SEDONA CONF. J. 1, 10 (2019); Hon. Paul W. Grimm et al., *Authentication of Social Media Evidence*, 36 AM. J. TRIAL ADVOC. 433, 434 (Spring 2013).

76. *See Primer on Social Media*, *supra* note 75, at 10.

providers. Examples of OTT messaging applications include WhatsApp, Facebook Messenger, iMessage, Snapchat, and Kik.[77] Some messaging applications also give the user the ability to be anonymous or to send messages that will self-destruct.[78]

More recent additions to social media include applications for cloud-based messaging, collaboration applications, live-streaming video, health information sharing, wearable technologies, and location-based platforms.[79]

(b) Social Media Content as Evidence

It was not long after the advent of social media that participants in the justice system recognized it as a source of evidence. A Facebook comment could be an admission of a crime. A photo of a criminal defendant with known gang members could tend to show gang affiliation. A video of someone dancing exuberantly at his daughter's wedding reception could undermine a personal injury claim, the need for workers compensation, or long-term disability payments.[80]

The recognition of social media's evidentiary value also gave rise to admissibility challenges. These issues have arisen mostly in the authentication arena: whether the social media post, photo, video, message, or comment is what the proponent claims it to be.

77. *Id*. at 13–14.

78. *Id*. at 14–15; *see* Sect. II.D.8 (Digital Photographs), *infra*.

79. *Primer on Social Media*, *supra* note 75, at 15–20.

80. It is worth noting, however, that the vast majority of cases dealing with the admissibility of social media evidence are criminal in nature.

Social media evidence can come in a variety of forms. Often it will be presented in the form of screenshots or printouts.[81] Photos and videos can be downloaded in their native formats.[82] Content available through websites can be preserved through APIs.[83] Social media evidence can also be gathered using individual platform download tools.[84] Social media content also may contain metadata that might be relevant in legal disputes.[85]

---

81. *See, e.g.*, Hawkins v. State, No. S18A0886, 2018 WL 3965665, at *4 (Ga. Aug. 20, 2018); State v. Jones, No. 109,027, 2014 WL 802022, at *4 (Kan. Ct. App. Feb. 28, 2014).

82. *See, e.g.*, United States v. Farrad, 895 F.3d 859, 875–76 (6th Cir. 2018); Lamb v. State, 246 So. 3d 400, 404–05 (Fla. Dist. Ct. App. 2018).

83. *See* Sect. II.D.3 (Websites), *supra*.

84. *See How to Access Your Twitter Data*, TWITTER, https://help.twitter.com/en/managing-your-account/accessing-your-twitter-data (last visited May 5, 2020); *Accessing & Downloading Your Information*, FACEBOOK, https://www.facebook.com/help/1701730696756992/?helpref=hc_fnav (last visited May 5, 2020); *see also* Katie Canales, *Instagram is rolling out a feature that will let you download all of your photos and past searches in one fell swoop*, BUS. INSIDER (Apr. 24, 2018, 5:48 PM), https://www.businessinsider.com/instagram-data-download-feature-gdpr-privacy-photos-searches-2018-4; Abby Ohlheiser, *Here's how to download all your data from Facebook. It might be a wake-up call*, WASH. POST (Mar. 27, 2018, 9:23 a.m.), https://www.washingtonpost.com/news/the-intersect/wp/2018/03/27/heres-how-to-download-all-your-data-from-facebook-it-might-be-a-wake-up-call/?utm_term=.1b84ec6553f2; *see, e.g.*, Ehrenberg v. State Farm Mut. Auto. Ins. Co., No. 16-17269, 2017 WL 3582487, at *3 n.2 (E.D. La. Aug. 18, 2017) (refusing to decide whether request seeking plaintiff's Facebook, Twitter, and Instagram accounts via "data link" was appropriate).

85. *See In re* Adoption of Nash, No. 15-P-1302, 2016 WL 2755864, at *3 (Mass. App. Ct. May 12, 2016) (holding Facebook messages were not authenticated based on metadata review that could not link them to mother).

(c) Authentication of Social Media Evidence

Generally, the standard for authentication of evidence, whether under Rule 901 and or its state counterparts, is low.[86] To authenticate evidence, "the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is."[87] This may be shown by either direct or circumstantial evidence.[88] A *prima facie* case is all that is necessary.[89]

In addressing these evidentiary problems, the authentication rules most likely to apply include the following:

- a witness with personal knowledge—Rule 901(b)(1)
- expert testimony or comparison with authenticated examples—Rule 901(b)(3)
- distinctive characteristics, including circumstantial evidence—Rule 901(b)(4)

---

86. United States v. Barnes, 803 F.3d 209, 217 (5th Cir. 2015) (stating that the authentication standard is not a burdensome one); United States v. Vayner, 769 F.3d 125, 130 (2d Cir. 2014) ("bar for authentication of evidence is not particularly high"); United States v. Hassan, 742 F.3d 104, 133 (4th Cir. 2014) ("the burden to authenticate under Rule 901 is not high"); United States v. Ortiz, 966 F.2d 707, 716 (1st Cir. 1992) (901(a) "does not erect a particularly high hurdle"); State v. Newman, 916 N.W.2d 393, 409 (Neb. 2018) (authentication statute "does not impose a high hurdle for authentication or identification"); State v. Adams, 161 A.3d 1182, 1199 (R.I. 2017) ("authentication is not a high hurdle to clear"); *see also* Grimm et al., *supra* note 75, at 458.

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

88. *Vayner*, 769 F.3d at 130; Tienda v. State, 358 S.W.3d 633, 638 (Tex. Crim. App. 2012) ("Evidence may be authenticated in a number of ways, including by direct testimony from a witness with personal knowledge, by comparison with other authenticated evidence, or by circumstantial evidence.").

89. Stout v. Jefferson Cty. Bd. of Educ., 882 F.3d 988, 1008 (11th Cir. 2018); *Hassan*, 742 F.3d at 133.

- a system or process capable of proving a reliable and dependable result—Rule 901(b)(9)
- certified records generated by an electronic process or system—Rule 902(13)
- certified data copied from an electronic device, storage medium, or file—Rule 902(14)

While these basic authentication standards have never changed, social media evidence nevertheless appeared to drive some courts to raise the evidentiary bar.[90] Commentators noted that courts appeared to fall into two camps.[91] In the beginning, courts were openly skeptical of social media and concerned about the possibility of forgery, falsification, and impersonation.[92] Other courts did not appear to share this skepticism and kept the bar low.[93] The low-bar approach was exemplified by courts that articulated a "reasonable jury" standard—authentication was shown if there was sufficient direct or circumstantial evidence to allow a reasonable jury to find that the evidence is what it is purported to be.[94]

More recently, some courts in the high-bar camp appear to have softened.[95] This is in line with other cases that show a growing comfort level among attorneys, litigants, and judges

---

90. *See Primer on Social Media*, *supra* note 75.

91. *Id*. *See generally* Grimm et al., *supra* note 75; Wendy Angus-Anderson, *Authenticity and Admissibility of Social Media Website Printouts*, 14 DUKE L. & TECH. REV. 33 (2015).

92. *See, e.g.*, Griffin v. State, 19 A.3d 415, 422 (Md. 2011); Smith v. State, 136 So. 3d 424, 432 (Miss. 2014); *see also* Grimm et al., *supra* note 75, at 441–49.

93. *See id*. at 449–54.

94. *See, e.g.*, Tienda v. State, 358 S.W.3d 633, 638 (Tex. Crim. App. 2012).

95. *See* Sublet v. State, 113 A.3d 695, 712–18 (Md. 2015) (distinguishing *Griffin* and applying a "reasonable juror" standard articulated in United States v. Vayner, 769 F.3d 125 (2d Cir. 2014), *Tienda*, and United States v. Hassan, 742 F.3d 104 (4th Cir. 2014)).

with the use of social media evidence.[96] The picture today is not so much one of division among courts based on different legal standards, but one of different outcomes based on different facts.[97]

Turning to the examples of authentication evidence in Rule 901(b), the typical or most likely to be used, whether alone or in combination, are 901(b)(1) (testimony of a witness with knowledge) and 901(b)(4) (distinctive characteristics).[98] Authentication can also be satisfied under 901(b)(3) by comparison to an already authenticated specimen by either an expert or the trier of fact.[99]

The issue of authorship and identity is usually critical because the identity of the author, creator, or owner of social media evidence is often essential to its relevance and its admissibility. It is in this context that judicial suspicions about the integrity of social media evidence are most evident, driven by the

---

96. *See* KENNETH S. BROUN ET AL., MCCORMICK ON EVIDENCE § 227 (Robert P. Mosteller ed., 7th ed. 2016) ("[T]he approach by courts imposing a heavier burden on social networking evidence is reminiscent of the conservative response many courts had to the advent of other technologies such as the telegraph, the computer, and the internet. With time the trend may well shift towards the second category of cases as courts become more familiar with the social networking medium and the perceived dangers of this evidence dissipate. Given that many of the cases taking a lenient approach to social networking evidence have arisen in only the last two to three years, this shift may already be occurring.").

97. *See id*. ("Despite the seeming novelty of social network-generated documents, courts have applied the existing concepts of authentication under Federal Rule 901 to them.").

98. *See id*. at 545–47; People v. Glover, 363 P.3d 736, 741 (Colo. App. 2015).

99. See Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 556; Patrick Marshall, What You Say on Facebook May Be Used Against You in a Court of Family Law: Analysis of This New Form of Electronic Evidence and Why It Should Be on Every Matrimonial Attorney's Radar, 63 ALA. L. REV. 1115, 1129 (2012).

perception that social media is more susceptible to forgery or falsification than hard-copy evidence.[100] The Mississippi Supreme Court described the issue this way:

> Not only can anyone create a profile and masquerade as another person, but such a risk is amplified when a person creates a real profile without the realization that third parties can mine their personal data. . . . Thus, concern over authentication arises because anyone can create a fictitious account and masquerade under another person's name or can gain access to another's account by obtaining the user's username and password, and, consequently, the potential for fabricating or tampering with electronically stored information on a social networking [website] is high and poses challenges to authenticating printouts from the website.[101]

When authorship is critical to the admissibility of social media evidence, courts have required "direct or circumstantial evidence that tends to corroborate the identity of the author of the communication in question."[102] This may include "testimony

---

100. *See* Commonwealth v. Mangel, 181 A.3d 1154, 1162–64 (Pa. Super. Ct. 2018) (trial court did not abuse its discretion in denying Commonwealth's motion *in limine* to admit social media posts and messages based in part on the concern about the ease with which social media accounts may be falsified or a legitimate account accessed by an imposter).

101. Smith v. State, 136 So. 3d 424, 432 (Miss. 2014) (internal citations and quotations omitted); *see also Mangel*, 181 A.3d at 1162 (raising similar concerns). For further discussion and cases see Section V.C.2 (State law application in federal cases), *infra*.

102. *Mangel*, 181 A.3d at 1162; *see also Glover*, 363 P.3d at 742; United States v. Recio, 884 F.3d 230, 236–37 (4th Cir. 2018) (authenticating Facebook posts through circumstantial evidence).

from the person who sent or received the communication, or contextual clues in the communication tending to reveal the identity of the sender."[103] Authorship of social media evidence is subject to authentication by the same "wide range of extrinsic evidence" [104] as traditional hard-copy evidence. But courts have still held that the proponent need not absolutely prove authorship.[105]

Not all social media evidence, however, presents an issue of identity or authorship. In some cases, courts have appeared to require either a lesser quantum of evidence, or no evidence, pertaining to the authorship or identity.[106] This is often seen in the admission of photos and videos posted to social media.[107]

In *Lamb v. State*, the Florida court permitted the introduction of a Facebook live video that purported to show the defendant driving the stolen vehicles.[108] The video had been posted to a co-defendant's public Facebook page and downloaded by a "digital forensic examiner" who simply visited the page. Beyond the examiner's testimony as to how he downloaded the video, the only other evidence was the testimony from two witnesses who

---

103. *Mangel*, 181 A.3d at 1162.

104. United States v. Browne, 834 F.3d 403, 411–12 (3d Cir. 2016), *cert. denied*, 137 S. Ct. 695 (2017).

105. *See* Gagliardi v. Comm'r of Children & Families, 110 A.3d 512, 518 (Conn. App. Ct. 2015) (only need to make a *prima facie* showing of authenticity and "once a prima facie showing of authorship is made to the court, the evidence, as long as it is otherwise admissible, goes to the [finder of fact], which ultimately will determine its authenticity.").

106. Beaty v. State, No. 03-16-00856-CR, 2017 WL 5560078 at *4–5 (Tex. App. Nov. 15, 2017).

107. *See, e.g.*, United States v. Broomfield, 591 F. App'x 847, 852 (11th Cir. 2014); Lamb v. State, 246 So. 3d 400, 409 (Fla. Dist. Ct. App. 2018); State v. Gray, No. 2016-KA-1195, 2017 WL 3426021, at *15–16 (La. Ct. App. June 28, 2017).

108. 246 So. 3d at 409 (Fla. Dist. Ct. App. 2018).

watched the video and identified the defendant as being in the video. This was a sufficient *prima facie* showing of authenticity.

The court cited the Eleventh Circuit for not requiring more authentication evidence:

> [T]he Eleventh Circuit and other courts . . . have permitted the admission of social media videos in criminal cases based on sufficient evidence that the video depicts what the government claims, even though the government did not: (1) call the creator of the videos; (2) search the device which was used to create the videos; or (3) obtain information directly from the social media website. *See, e.g., U.S. v. Washington*, 2017 WL 3642112, *2 (N.D. Ill. Aug. 24, 2017) (YouTube video which the government contended showed the defendant and several other men pointing firearms at the camera was sufficiently authenticated where law enforcement witness would testify that he watched this video on YouTube, recognized the defendant, and downloaded the video); *State v. Gray*, —— So.3d ——, ——, 2017 WL 3426021, *16 (La. Ct. App. June 28, 2017) (YouTube videos were sufficiently authenticated where the investigating officer's testimony provided sufficient support that the videos were what the state claimed them to be, that is, videos depicting the defendant and other gang members in a park and surrounding area). As the *Washington* court stated, "[w]hile a witness with [knowledge of the video's creation] *could* authenticate [the] video, Rule 901 does not *require* it." 2017 WL 3642112 at *2.[109]

109. *Id*. at 409–10.

The relevance of the video did not depend on who created the video or even who posted the video, even though it purportedly came from a co-defendant's Facebook page. Its relevance was in its content—that it depicted someone identified as the defendant with the stolen vehicle. In this respect, the Facebook Live video in *Lamb* was essentially no different than any other video.

In *Commonwealth v. Martin*, the Pennsylvania Superior Court distinguished the *Mangel* decision discussed above (which required evidence to tie social media messages to an individual) and held that Instagram posts depicting the defendant did not require evidence that he had made the posts.[110] In addition, the issue did not depend on whether the defendant made the posts, but on whether they accurately portrayed the defendant.[111]

Similarly, in *United States v. Thomas*, the Sixth Circuit upheld the admission of photos downloaded by law enforcement from Facebook and Instagram pages using a version of the name "Jabron Thomas," the same name as the defendant.[112] Thomas argued the photos were inadmissible because there was no evidence of who created the Facebook page or whether the page itself was authentic.

The court set out some hypotheticals to illustrate the authentication issue posed:

> In many contexts, the question could conceivably be quite interesting: what if, for example, the owner of a social-media profile (let's call him Alex) used a picture of someone else (say, Bob) as his profile picture? If Bob robbed a bank, Alex

110. No. 1962 MDA 2016, 2018 WL 3121766, at *9 (Pa. Super. Ct. June 26, 2018) (non-precedential decision).

111. *Id*.

112. 701 F. App'x 414, 419 (6th Cir. 2017).

> would not want to be implicated as the robber simply because he had Bob's picture on his social-media profile. Or, what if Bob fabricated a social-media profile under Alex's name, but with Bob's picture—and then Bob robbed a bank? Or, less convolutedly, what if there were allegations that the online photographs had been digitally manipulated or hacked in some way?[113]

But the court concluded that those questions weren't before it. Instead, the court saw "no reason to depart from the ordinary rule that photographs, including social-media photographs, are authenticated by 'evidence sufficient to support a finding that the [photograph] is what the proponent claims it is,' Fed. R. Evid. 901(a)."[114] As with *Lamb*, it was what was depicted in the photos, not necessarily who took them or to what social media site they were posted, that was relevant. The photos were offered to identify Thomas—they showed his distinctive tattoos on his hands and arms and that he was wearing Detroit Tigers gear similar to the hat worn by the robber.[115]

(d) Business Records

When social media posts or profiles are offered into evidence, Rule 902(11) may be unavailable because the evidence may not qualify as a business record.[116] Posts by users or user profiles are often not business activities—they are not records

---

113. *Id*.

114. *Id*.

115. *Id.*; *see also* Beaty v. State, No. 03-16-00856-CR, 2017 WL 5560078, at *4 (Tex. App. Nov. 15, 2017) (holding that Facebook photos offered to show defendant's clothing and appearance at the time of the shooting did not demand proof of identify of person who created the photos or the social media post).

116. People v. Glover, 363 P.3d 736, 741-42 (Colo. App. 2015).

that the social media site would use or rely on for a business purpose. Instead, they are declarations from the individuals who posted the information. As such, they are not usually admissible business records.[117]

(e) Other Social Media Admissibility Challenges

Authentication, however, does not guarantee admissibility. As with all evidence, to be admissible, social media evidence must also be relevant,[118] not inadmissible hearsay,[119] and not unduly prejudicial, confusing, cumulative, or misleading.[120] Some

117. *See* United States v. Farrad, 895 F.3d 859, 878–79 (6th Cir. 2018); United States v. Browne, 834 F.3d 403, 434–35 (3d Cir. 2016), *cert. denied*, 137 S. Ct. 695 (2017). *But see* United States v. Recio, 884 F.3d 230, 237–38 (4th Cir. 2018). In *Recio*, the Fourth Circuit found that authentication was achieved through a certification of a Facebook records custodian showing that the Facebook user in question had made the post at or near the time showed by the post. This was in addition to other (strong) evidence tying the defendant to the account, including that the name on the account was the same as the defendant, "Larry Recio"; an email address associated with the account was larryrecio20@yahoo.com; the defendant appeared in over 100 photos posted to the account; and one photo included the caption "Happy Birthday Larry Recio." *Id.* at 237.

118. FED. R. EVID. 402; *Recio*, 884 F.3d at 235–36 (holding that a lyric posted on Facebook was relevant because it matched the details of the alleged crime and illustrated the defendant's motive).

119. FED. R. EVID. 802; *Recio*, 884 F.3d at 234–35 (holding that a lyric posted on Facebook was admissible as an adoptive admission under Fed. R. Evid. 801(d)).

120. FED. R. EVID. 403; *Recio*, 884 F.3d at 236 (holding that the probative value of admitting a lyric posted on Facebook outweighed the risk of undue prejudice); United States v. Khoa, No. 17-4518, 2018 WL 2905432, at *3 (4th Cir. 2018) (holding that photos of victim posted to social media were not unduly prejudicial under Fed. R. Evid. 403).

courts have also applied the "best evidence" rule to social media evidence.[121]

5. Internet of Things

The Internet of Things (IoT) is a network of computing devices and sensors embedded in everyday objects that create, collect, and share data through the internet. Some examples include wearables that track our steps and sleep, appliances that track our consumption, and thermostats that adjust to our habits. The data that these devices create is often stored in structured databases and may be stored in multiple locations in the cloud.

IoT data is already playing a significant role in cases. For example, in one murder case, data indicating movement from a wife's fitness wearable convinced the police that her husband killed her.[122] In another, prosecutors used Fitbit data to show that a victim falsely accused a man of raping her.[123]

The risk that IoT data could be manipulated should not bar this evidence entirely. In the best-case scenario, the wearer or owner of an IoT device can testify to authenticate the device and its data (and metadata) as a witness with personal knowledge under Rule 901(b)(1). Any analysis of the data would need to undergo a separate process to authenticate the data produced and its accuracy using 901(b)(3) (expert testimony), 901(b)(4)

---

121. *See, e.g.*, Woods v. State, No. 11-15-00134-CR, 2017 WL 3711104, at *6 (Tex. App. Aug. 25, 2017) (holding that Facebook posts satisfied best evidence rule).

122. Christine Hauser, *In Connecticut Murder Case, a Fitbit Is a Silent Witness*, N.Y. TIMES (Apr. 27, 2017), https://www.nytimes.com/2017/04/27/nyregion/in-connecticut-murder-case-a-fitbit-is-a-silent-witness.html.

123. Jacob Gershman, *Prosecutors Say Fitbit Device Exposed Fibbing in Rape Case*, WALL ST. J.: L. BLOG (Apr. 21, 2016, 1:53 PM), https://blogs.wsj.com/law/2016/04/21/prosecutors-say-fitbit-device-exposed-fibbing-in-rape-case/.

(distinctive characteristics, including circumstantial evidence), 901(b)(9) (system or process capable of proving a reliable and dependable result), 902(13) (certified records generated by an electronic process or system), or 902(14) (certified data copied from an electronic device, storage medium, or file).

6. Ephemeral or Self-Destructing Photographs/Messages

Since the release of Snapchat in September 2011, the use of self-destructing messaging (also referred to as "ephemeral messaging") has increased exponentially. In 2019, over 200 million people were using Snapchat, creating over 3.5 billion snaps each day.[124] Additional ephemeral messaging providers have emerged, including Wickr,[125] Telegram,[126] Confide,[127] and Signal.[128] The default setting in ephemeral messaging applications is for messages and images to self-destruct after a limited amount of time.[129] Some applications claim to be "screen-shot

124. SnapChat Revenue and Usage Statistics (2020), BUSINESS OF APPS (Apr. 24, 2020), https://www.businessofapps.com/data/snapchat-statistics/.

125. WICKR, https://wickr.com/ (last visited May 6, 2020).

126. TELEGRAM, https://telegram.org/ (last visited May 6, 2020).

127. CONFIDE, https://getconfide.com/ (last visited May 6, 2020).

128. SIGNAL, https://signal.org/en/ (last visited May 6, 2020).

129. *When does Snapchat delete Snaps and Chats*, SNAPCHAT, https://support.snapchat.com/en-US/a/when-are-snaps-chats-deleted (last visited May 6, 2020); *see also Features,* CONFIDE, https://getconfide.com/ ("Messages disappear forever after they are read once, making them as private and secure as the spoken word.") (last visited May 6, 2020); *Set and manage disappearing messages*, SIGNAL, https://support.signal.org/hc/en-us/articles/360007320771-Set-and-manage-disappearing-messages ("Use disappearing messages to keep your message history tidy. The message will disappear from your devices after the timer has elapsed.") (last visited May 6, 2020). What sets these applications apart from SMS text messaging or OTT messaging applications is their ability to automate the destruction of content on the sender's *and* the recipient's devices. Another key aspect of ephemeral messaging is endpoint encryption of messages, which ostensibly prevents third parties from gaining

proof," and one even requires the receiver to scroll over redacted text with a finger to briefly unredact the text before it is permanently deleted.[130] Although not in the context of authentication or admissibility, ephemeral communications figured prominently in discovery disputes in recent trade secret matters.[131]

Given that Snapchat is currently one of the most prevalent ephemeral messaging applications, this *Commentary* analyzes authentication issues through Snapchat. In 2020, 78 percent of internet users aged 18 to 24 used Snapchat, with 71 percent of those users accessing the platform daily.[132]

Over time, Snapchat has evolved to allow users to save "snaps" as memories so that they do not self-destruct.[133] In those

---

access to message content. Philip Favro, *Ephemeral Messaging: Balancing the Benefits and Risks*, PRACTICAL LAW THE JOURNAL: LITIGATION (June/July 2019).

130. *See Features: Screenshot-Proof*, CONFIDE, https://getconfide.com/ ("For extra privacy on iOS and Android, our patented reading experience ensures that only one line of the message is unveiled at a time and that the sender's name is not simultaneously visible.") (last visited May 6, 2020). Use of such technology would present some interesting authentication challenges in court. Message recipients could film the temporary unredaction of a message with a second device while scrolling their finger over the text, avoiding the first layer of screen-shot protection, but with the sender's name invisible, there would be one less piece of information tying the message to the sender. But if the recipient was able to authenticate the video of the message, it might still be authenticated under the right facts, much like other electronic messages.

131. WeRide Corp. v. Kun Huang, No. 5:18-cv-07233, 2020 WL 1967209 (N.D. Cal. Apr. 24, 2020); Waymo LLC v. Uber Techs., Inc., No. 3:17-cv-00939, 2018 WL 646701, at *21 (N.D. Cal. Jan. 30, 2018); Waymo LLC v. Uber Techs., Inc., 3:17-cv-00939, 2018 WL 6501798, at *6–8 (N.D. Cal. Dec. 15, 2017).

132. *See Snapchat by the Numbers: Stats, Demographics & Fun Facts*, OMNICORE (Feb. 7, 2020), https://www.omnicoreagency.com/snapchat-statistics/.

133. *See, e.g.*, *How to Use Memories*, SNAPCHAT, https://support.snapchat.com/en-US/a/about-memories (last visited May 6, 2020). Snapchat is

situations, the "memories" are like any other social media posts. Thus, parties would need to authenticate snaps or analogous content from other ephemeral messaging applications in the same way.

Self-destructing snaps may need to be handled differently. Snaps that disappear have not necessarily been erased once Snapchat deletes them. A receiver of a snap can save the snap by taking a screenshot of the snap, taking a photograph of the screen, or using image-capture software or apps. A Snapchat user can adjust the privacy settings to determine who can send snaps to the user and who can view the user's "story" (other saved content on a user's application). If a recipient chooses to "screenshot" or "screen capture" a photo before it disappears, Snapchat will notify the sender that the recipient took a screenshot of the snap.[134] These types of saved snaps are likely to be authenticated using 901(b)(1) (personal knowledge) or 902(14) (certified data copied from device). Snaps saved in this manner are likely to be treated similarly to digital photographs or videos.

There is limited case law discussing the authentication of Snapchat messages. In one criminal matter, a defendant sought appellate review of a trial court order that admitted a video shared through Snapchat.[135] During the trial, two witnesses who had contemporaneously viewed the snaps testified that the videos played in the courtroom were the same videos posted to the defendant's account. One of the witnesses also remembered a

---

used as an example. The technology evolves rapidly and changes quicker than articles about technology.

134. Henry T. Casey & David Murphy, *How to Use the New Snapchat Like a Pro*, TOM'S GUIDE (Sept. 25, 2018), https://www.tomsguide.com/us/snapchat-tutorial,news-21216.html.

135. Schaffer v. State, No. 238, 2017, 2018 WL 1747793, at *1 (Del. Apr. 10, 2018).

caption on the video referencing the victim being scared. The defendant argued such testimony was insufficient to authenticate the video because the witnesses could not remember exactly when they watched the video and that the video apparently did not have a time stamp. The Delaware Supreme Court rejected the defendant's argument.[136]

7. Digitally Stored Data

The mere fact that information has been created and stored within a computer system does not make that information reliable or authentic. Electronic records are most frequently authenticated under Rule 901(b)(4), which permits authentication by "[a]ppearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances."[137] The primary authenticity issue in the context of computer-stored records and databases is chain of custody.

The methods of authentication most likely to be appropriate for computerized records are as follows:

- a witness with personal knowledge—Rule 901(b)(1)
- expert testimony or comparison with authenticated examples—Rule 901(b)(3)
- distinctive characteristics, including circumstantial evidence—Rule 901(b)(4)
- a system or process capable of proving a reliable and dependable result—Rule 901(b)(9)
- certified records generated by an electronic process or system—Rule 902(13)

136. *Id.* at *6 (observing as well that the defendant's arguments went "to the appropriate weight to be given the evidence, not its admissibility.").

137. Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 546 (D. Md. 2007).

- certified data copied from an electronic device, storage medium, or file—Rule 902(14)

8. Digital Photographs

Historically, photographs were authenticated by the person taking the photograph or the person who witnessed the event who can show that a photograph is a fair and accurate representation of the scene depicted.[138] However, when photographs were captured on film, there were fewer photographs, and it was much more difficult to alter or manipulate the photographs. Today, digital photographs are ubiquitous—both through cell phone and camera usage.[139]

Addressing the authenticity of photographs is not limited to the content of the photograph itself. The potential for altering or enhancing of the photograph must be considered.[140] In addition, the metadata of photographs could have an abundance of information relevant to a case, including date, time, location, and GPS coordinates. Additional issues may arise when a film photograph is converted to digital.

When authenticating digital photographs, the most likely Rules to apply are as follows:

---

138. People v. Goldsmith, 326 P.3d 239, 246 (Cal. 2014).

139. It is estimated that over one trillion digital photographs are now taken every year. Stephen Heyman, *Photos, Photos Everywhere*, N.Y. TIMES (July 29, 2015), https://www.nytimes.com/2015/07/23/arts/international/photos-photos-everywhere.html.

140. *See* Hines v. Carpenter, No. 3:05-0002, 2015 WL 1208684, at *19 (M.D. Tenn. Mar. 16, 2015) (quoting *Lorraine*, 241 F.R.D. at 561–62) ("enhancement consists of removing, inserting, or highlighting an aspect of the photograph that the technician wants to change."); Guarisco v. Boh Brothers Construction Co., LLC, No. 18-7514, 2019 WL 4881272 (E.D. La. Oct. 3, 2019) (imposing sanctions against the plaintiff for modifying a digital photograph to enhance her negligence claims against defendant and observing that the original unmodified photograph was still available on the plaintiff's Facebook page).

- a witness with personal knowledge—Rule 901(b)(1)
- a system or process capable of providing a reliable and dependable result—Rule 901(b)(9)
- official publications—Rule 902(5)
- certified records generated by an electronic process or system—Rule 902(13)
- certified data copied from an electronic device, storage medium, or file—Rule 902(14)

The leading authority on authenticating digital photographs remains *Lorraine*,[141] which considered the authentication issues surrounding digital photographs, digitally enhanced images, digitally converted images, and photograph metadata. As with film photographs, Rule 901(b)(1) is a viable option for authenticating a digital photograph if a witness with personal knowledge of the scene in the photograph is available. If such a person is not available, a digitally converted image requires testimony by someone knowledgeable about the film-to-digital conversion process.

Authentication of a digitally enhanced photograph likely implicates Rule 901(b)(9) because of the unlikelihood that a witness can testify regarding subtle differences in the original photograph as compared to the enhanced image.[142] Metadata of a photograph was not considered in depth a decade ago. Photographs taken with cell phones have information that may be important for multiple reasons. The metadata from a photograph

141. 241 F.R.D. at 561–62.

142. *Id.* at 560 (discussing State v. Swinton, 847 A.2d 921, 942 (Conn. 2004)).

taken with a cell phone may automatically capture the geographic coordinates of where a picture was taken.[143]

9. Group Collaboration Tools

Collaboration applications, such as Slack, Jive, Confluence, Microsoft Teams, Salesforce Chatter, and others, facilitate group discussions as well as message exchanges between users and in private channels.[144] These applications often store shared content in the cloud, though some are deployed on a company's servers.[145]

Bases for authentication will typically include the following:

- a witness with personal knowledge—Rule (901(b)(1)
- expert testimony or comparison with authenticated examples—Rule 901(b)(3)
- distinctive characteristics, including circumstantial evidence—Rule 901(b)(4)
- a system or process capable of proving a reliable and dependable result—Rule 901(b)(9)
- certified records generated by an electronic process or system—Rule 902(13)
- certified data copied from an electronic device, storage medium, or file—Rule 902(14)

143. *See* United States v. Post, 997 F. Supp. 2d 602, 603–04 (S.D. Tex. 2014) (discussing how image metadata can reveal the location where a digital photograph was taken).

144. *See Primer on Social Media*, *supra* note 75, at 16.

145. *Id*.

Collaboration tools typically offer programs that use APIs to access and share information with the application.[146] Using the API, some discovery review platforms can import machine-readable, searchable data that includes content and its metadata; some even collect metadata that can authenticate the content and may provide a message-digest hash for verification of the extracted data.

As noted with website collections, collecting data through an API can be problematic. An API collection lacks perfect synchronicity with the original content—it may change its context, format, or appearance—and it may be difficult to access. Moreover, provider restrictions may limit the amount of data that can be collected through an API.[147]

10. Computer Processes, Animations, Audio/Video, Virtual Reality, and Simulations

When machines are responsible for recording audio or video or implementing processes, authentication will be relatively simple, presuming that the recording device was in good working order, under 902(13) (certified records generated by an electronic process or system).

---

146. *Guide to Slack import and export tools*, SLACK, https://get.slack.help/hc/en-us/articles/204897248-Guide-to-Slack-import-and-export-tools (last visited May 6, 2020).

147. *Id*. For example, Slack only permits "Enterprise Grid" plan users to export all data from their accounts. *A guide to Slack's Discovery APIs*, https://slack.com/help/articles/360002079527 (last visited May 6, 2020). In contrast, Slack places restrictions on "Free," "Standard," and "Plus" plan users to export messages from "private channels" and "direct messages." Slack also forbids such plans from exporting files attached to user messages. *Guide to Slack Import and Export Tools*, SLACK, https://get.slack.help/hc/en-us/articles/204897248-Guide-to-Slack-import-and-export-tools (last visited May 6, 2020).

However, where a person is creating audio or video, virtual reality scenarios, or simulations, authentication becomes more complex. It may require testimony regarding the operation of the equipment, the accuracy of the data, and the motion and sound. Typical methods for authenticating this evidence are as follows:

- a witness with personal knowledge—Rule 901(b)(1)
- expert testimony or comparison with authenticated examples—Rule901(b)(3)
- a system or process capable of proving a reliable and dependable result—Rule 901(b)(9)[148]

Computer simulations, which are based on scientific principles and data and offered as substantive evidence, face a stiffer test for authentication, wrapped up in an analysis of their reliability.[149]

11. Cloud Computing

Cloud computing services often transfer ESI to servers other than the "original" server (i.e., the server on which it was stored in the first instance). The cloud computing service's servers may be located in various locations across the country or even around the world. It may be difficult, if not virtually impossible,

148. Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 559 (D. Md. 2007) (stating that computer animations offered to illustrate testimony 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.").

149. *Id*. at 560–61 ("[T]he most frequent methods of authenticating computer simulations are 901(b)(1) (witness with personal knowledge); and 901(b)(3) (expert witness). Use of an expert witness to authenticate a computer simulation likely will also involve Federal Rules of Evidence 702 and 703.").

to establish a chain of custody of a file, for example, that has been moved multiple times. Moreover, a single file may be disassembled and its parts stored on multiple servers. By analogy, this would be similar to cutting paper document into pieces, putting each piece in a separate file cabinet, and distributing the file cabinets to various warehouses around the world. To an end user, the service is seamless. When retrieved, the document pieces are reassembled from their various locations. How does a party establish that the reassembled document is identical to the "original" file before disassembly? Possible answers may be matching hash values or expert testimony about a process.

In addition, cloud computing services must duplicate and store copies of ESI on various servers to protect against loss from some catastrophic failure (e.g., fire, flood, etc.). It will be difficult, if not impossible, to know whether a particular file is the "original." This issue, however, may be more theoretical than practical. In any event, matching hash values may once again provide a sufficient basis to authenticate the "original" or "copy."

12. Emoji

Emoji, from the Japanese word meaning "picture character," are small pictographs.[150] These images are often used in text messages, social media, emails, and chat apps "to express the emotional attitude of the writer, convey information succinctly, [and] communicate a message playfully without using words, etc."[151] They are distinct from *emoticons*, which are letters, numbers, and other standard ASCII characters grouped into a

150. *Frequently Asked Questions: Emoji and Pictographs*, UNICODE, https://unicode.org/faq/emoji_dingbats.html#1.05 (last visited May 6, 2020).

151. Commonwealth v. Castano, 82 N.E.3d 974, 978 n.2 (Mass. 2017) (citing MERRIAM-WEBSTER ONLINE DICTIONARY, https://www.merriam-webster.com/dictionary/emoji).

pictograph, like a smiley face :-) or a heart <3, and are used to "represent[] a facial expression or suggest[] an attitude or emotion and that is used especially in computerized communications (such as e-mail)."[152]

Emoji have typically been used in consumer correspondence and have been increasingly a subject of evidence in criminal cases.[153] With emoji showing up now in business communications, they are also becoming a source of evidence in civil litigation. Despite their seemingly straightforward cartoonish appearance, emoji can be fraught with difficulty for the unwary practitioner given the rapid growth in emoji variety and depictions, together with the challenges of interpreting their meaning.[154]

First, the variety of emoji is continually expanding—and with it, the multiplicity of ways they are depicted. Over 3,000 emoji are now listed in the Unicode Standard.[155] Unicode is a computer-industry standard that assigns each letter, digit, and symbol, including emoji, a unique numeric value that will apply across different operating systems, devices, applications, and languages. Its purpose is to ensure the consistent encoding, handling, and representation of characters and emoji symbols. However, though a single code is assigned to Unicode emoji, that does not mean that there is a single depiction or meaning of each Unicode emoji. Instead, a platform can render emoji using

---

152. Emoticon, MERRIAM-WEBSTER ONLINE DICTIONARY, https://www.merriam-webster.com/dictionary/emoticon.

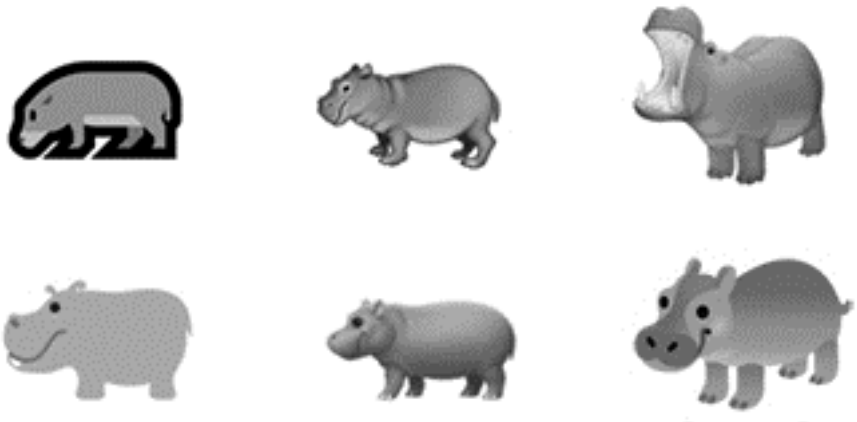
153. *See, e.g.*, *In re* JP, No. 344812, 2019 WL 4648450 (Mich. Ct. App. 2019) (memorializing in the court's opinion emoji the appellant exchanged with friends through Snapchat).

154. *See* Eric Goldman, *Emojis and the Law*, 93 WASH. L. REV. 1227, 1230 (2018).

155. *Full Emoji List, v 13.0*, UNICODE, http://unicode.org/emoji/charts/full-emoji-list.html (last visited May 6, 2020).

its own idiosyncratic color and shape choices.[156] Complicating this further is that the emoji intended by a sender may appear differently on the recipient's device.[157]

Take, for example, the hippopotamus emoji, which was approved as part of Unicode 11.0 in 2018. Here are some renderings of the hippo across various platforms (Microsoft, Samsung, Facebook, Twitter, Apple, and Google, respectively):



156. Hannah Miller et al., *"Blissfully Happy" or "Ready to Fight": Varying Interpretations of Emoji*, *in* PROCEEDINGS OF THE TENTH INTERNATIONAL AAAI CONFERENCE ON WEB AND SOCIAL MEDIA 259, 267 (2016) ("Unlike plain text where people view the same characters in their exchange, platforms effectively *translate* emoji: the emoji that the sender chose is translated to the receiver's platform's rendering.").

157. Further, since emoji render differently on different platforms, the emoji sent by one person from one device may differ markedly from what a recipient using a different device sees. *Id*. at 259. Such a phenomenon is apparent in the *In re JP* matter where the court inserted what appear to be Gmail emoji into its opinion to reflect the emoji exchanged by the appellant and her friends on Snapchat. *In re JP*, 2019 WL 4648450 at *2. *See* Eric Goldman, *More Teenagers Mistakenly Think "Private" Chat Conversations Will Remain Private–People v. JP*, TECHNOLOGY & MARKETING LAW BLOG (Oct. 7, 2019), https://blog.ericgoldman.org/archives/2019/10/more-teenagers-mistakenly-think-private-chat-conversations-will-remain-private-people-v-jp.htm.

Problematically, Unicode is not the only type of emoji. There are many more non-Unicode emoji that are idiosyncratic to different platforms. Often called "bespoke emoji" or "stickers," these are available on platforms like Facebook and Snapchat. Other apps also let users create their own custom emoji, such as avatars from the Bitmoji app. Since these emoji lack Unicode codes, they may not be compatible with other platforms, so they may not display properly—or at all—to recipients who are not using the same platform as the sender.

The differences in renderings have implications for discovery as well. When emoji are collected and processed, the image may very well appear differently—or as an empty rectangular box or space—for review.

A second hurdle to using emoji as evidence is the issue of interpretation. Emoji can be difficult to interpret on their own. Emoji are small and many appear similar with minor differences. For example, the Unicode crying face has a tear, but the Unicode downcast face has a similar shape indicating a bead of sweat (both shown in Apple renderings). Only the eyes and placement of the water drop clue the reader in as to the meaning.

Finally, while "a picture is worth a thousand words," those words may be different in the eye of the beholder. Face emoji can be particularly problematic because people have difficulty interpreting facial expressions and given the different ways that

platforms choose to depict those faces.[158] Moreover, facial expressions may be used to indicate irony: for example, a winking emoji may indicate a joking tone, but a recipient may perceive the joke differently—or more maliciously—than the sender intended.[159]

Additionally, some emoji have multiple meanings. For example, the alien emoji  may mean that something is out of this world or strange. Alternatively, it may be used to refer to someone who is an illegal alien. Meanings can also depend on the cultural background of the sender and recipient (as well as a judge or jury).[160] For instance, the angel emoji may denote innocence, but a Chinese reader may perceive an angel as a threatening sign of death.[161] As a result, it can be difficult from an evidentiary point of view for parties, courts, and juries to give proper meaning to emoji. Meanings can become especially muddled when emoji are grouped together: it may be unclear whether the emoji are

158. Miller et al., *supra* note 156, at 261, 263–67.

159. NEXUS Servs., Inc. v. Moran, No. 5:16-cv-00035, 2018 WL 1461750, at *4 (W.D. Va. Mar. 23, 2018) (interpreting a Hitler emoji as ironic, finding that "[w]hile any image evoking Hitler obviously can be offensive, the emoji was contained in an internal email between two work colleagues in which, taken in context, one was jokingly calling the other a 'meanie' and a taskmaster."); United States v. Christensen, No. CR 06-085-BLG-RFC, 2013 WL 1498950, at *2 (D. Mont. Apr. 11, 2013) ("Christensen claims Neuhardt violated attorney-client privilege and the Sixth Amendment by offering, in an e-mail to the prosecutor accompanied by an emoticon, to 'stipulate that my client is guilty. :)' No one took Neuhardt's frivolous e-mail as an actual stipulation.").

160. VYVYAN EVANS, THE EMOJI CODE: THE LINGUISTICS BEHIND SMILEY FACES AND SCAREDY CATS 102, 123 (2017).

161. Alex Rawlings, *Why emoji mean different things in different cultures*, BBC (Dec. 11, 2018), http://www.bbc.com/future/story/20181211-why-emoji-mean-different-things-in-different-cultures.

independent of each other, modify each other, or are lined up to tell a story.

Emoji are already finding their way into judicial opinions. In one criminal case involving allegations of drug trafficking, firearms offenses, and racketeering, the defendants argued that there was no probable cause to search their Facebook accounts.[162] The investigating ATF agent testified, using his investigative experience, that the emoji referred to illicit activity: namely, a cloud emoji referred to drugs, while a cloud-of-gas emoji symbolized a gang. The court permitted the agent to use his training to interpret the emoji and establish probable cause. In another criminal case, the jury used emoji in a text message to conclude that a killing was not accidental.[163] The defendant had texted a friend the victim's nickname along with an emoji face showing Xs instead of eyes. The prosecution argued that the text indicated the shooting had already occurred.

Presenting emoji as evidence presents several challenges for authentication and admissibility. Parties will need to consider the context of the emoji in the sequence of communications to help define their meaning as well as the platforms used to depict those emoji. In addition, because emoji evolve over time, parties will need to determine how the emoji was rendered on a particular platform and operating system at a particular time for both the sender and recipient.

To authenticate emoji, expert testimony may be particularly important. The authentication rules most likely to play a role are as follows:

- A witness with personal knowledge—Rule 901(b)(1)

---

162. United States v. Westley, No. 3:17-CR-171, 2018 WL 3448161 (D. Conn. July 17, 2018).

163. Commonwealth v. Castano, 82 N.E.3d 974, 982–83 (Mass. 2017).

- expert testimony or comparison with authenticated examples—Rule 901(b)(3)
- distinctive characteristics, including circumstantial evidence—Rule 901(b)(4)
- a system or process capable of proving a reliable and dependable result—Rule 901(b)(9)
- certified data copied from an electronic device, storage medium, or file—Rule 902(14)

E. Hard Copies

Lorraine contains numerous points of comparison between ESI and hard-copy record systems in resolving authentication and admissibility issues.[164] While comparisons to the familiar world of tangible evidence are a useful starting point in many legal analyses, it is important to note some key differences between the two systems.

With hard-copy record systems, the mechanics of creating, storing, managing, organizing, controlling, and securing records and the systems that maintain them are generally simple and easily understood. Control largely depends on physical access to the records, which are basically stable and durable; one would need to be physically present to manipulate, mutilate, or destroy a hard-copy record. Moreover, manipulation or mutilation of documents has the potential for leaving indications of the tampering. Control systems can be designed to take advantage of physical realities such as the contiguous nature of the environment in which the records persisted, including known points of ingress and egress and singularity (uniqueness, originality, and the fact that a hard-copy record cannot simultaneously be physically present in more than one location at the same time).

---

164. Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 537, 542, 561 (D. Md. 2007).

Further, a physical or hard-copy record cannot be accessed and used simultaneously by multiple people without those people also being physically present and aware that access and use are shared.

This is not the case with ESI, particularly with regard to the issues of controlling and securing records. Unlike paper documents, access to ESI is not naturally constrained. Most computers are members of networks (or are intermittently on and off networks), and these networks generally are internetworked. With the advent of cloud storage, ESI may no longer reside on a local hard drive or server but may be accessed by a user half a world away. Moreover, scarcely a month goes by without another serious data breach being reported.[165]

F. Potential Challenges to Using Rule 902(14)

1. The Requirement of a Process of Digital Identification

To take advantage of Rule 902(14), litigants should think ahead, as the rule requires proof of "a process of digital identification." Any counsel who waits until the eve of trial to ponder hash values may be out of luck—the benefits of self-authentication cannot be applied to electronic evidence retroactively. The time to consider Rule 902(14) begins at the collection phase.

The most common method for authenticating electronic evidence under Rule 902(14) is hash-value verification. This involves comparing the hash value of an original, native version of an electronic file to the hash value of the collected, copied version. If both hash values are identical, then the copied version

165. *See* The Sedona Conference, *Commentary on Privacy and Information Security*, 17 SEDONA CONF. J. 1, 5 (2015) ("Personal identities, privacy, confidential client information, work product, and even attorney-client communications have never been more vulnerable to unauthorized disclosures, breaches, loss, or theft than they are today.").

proffered at trial is self-authenticating, assuming that a qualified person explains the process by which the original and copied hash values were generated and compared.[166]

The challenge that litigants are most likely to encounter with Rule 902(14) will be their failure to prepare for the first step—that is, generating an original hash value for each native file they intend to collect. This is because many litigants "self-collect" by either copying and pasting or dragging and dropping ESI onto a storage device or platform. It is often the most cost-effective way to preserve or collect information, but depending on how this is done, it may preclude reliance on Rule 902(14) for authentication.

Litigants should consider that original hash values do not self-generate. Currently, only specialized, third-party software can assign the unique alphanumerical identifiers for the authenticity of original ESI. While these programs are widely available, the practical reality is that given time limits and other reasons, most litigants, including large organizations with sophisticated Information Technology (IT) departments, do not use hash values with regularity for certain types of collections; they simply collect the files without collecting hash values. However, other avenues of authentication may be available. For example, ESI may still be authenticated as a business record or by a sender or recipient with the requisite personal knowledge.

166. FED. R. EVID. 902 advisory committee's notes to 2017 amendments ¶ 14 ("If the hash values for the original and copy are different, then the copy is not identical to the original. If the hash values for the original and copy are the same, it is highly improbable that the original and copy are not identical. Thus, identical hash values for the original and copy reliably attest to the fact that they are exact duplicates. This amendment allows self-authentication by a certification of a qualified person that she checked the hash value of the proffered item and that it was identical to the original.").

Those entities wishing to rely on Rule 902(14) should consider developing their own hashing policies and procedures. Whether responsibility falls to outside counsel, a third-party vendor, in-house counsel, or internal IT specialists, such litigants will benefit from having given their teams clear direction on how ESI is to be collected and digitally identified.

Even if litigants are diligent about assigning original hash values, they should consider how they will prove compliance with Rule 902(14) and should consider generating, maintaining, and preserving hash-value logs. This approach regarding original and copied hash values is a new concept—one unlikely to be on litigants' radar—but it is now key to admissibility under Rule 902(14). Creating these logs is not difficult; the software that generates the hash values also generates the logs. But maintaining them could be a challenge for some. With many years passing between the collection of documents and the admission of evidence, counsel should consider this issue early in the discovery process.

2. Certification Hazard: The Potential Exposure of Electronic Discovery Protocols

While careful adherence to Rule 902(14)'s requirements can streamline authentication, litigants should be alert to one potential drawback: exposing their electronic discovery protocols to adversaries. Typically, the details of a litigant's preservation, collection, and processing methods fall outside the scope of permissible discovery under Rule 26(b)(1) as being unrelated to the parties' "claims or defenses."[167] But the best supported Rule 902(14) declarations will be based on thorough ESI-collection

167. The Sedona Conference, *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 19 SEDONA CONF. J. 1, 118–30 (2018) [hereinafter *The Sedona Principles, Third Edition*].

documentation. This could mean having to explain a litigant's electronic discovery procedures.

In preparing the certification, litigants may want to refer to documentation confirming the chain of custody, which might encompass a range of sensitive details about the evidence and the collection process. This may very well include a description of the ESI source, custodian information, identification of the party performing the collection, collection date, and the storage or transfer means for the copy. It could also identify the copying tools and methods.

G. Recent Changes to Rule 807 (Residual Exception to Hearsay Rule)

Federal Rule of Evidence 807, also known as the residual exception, provides that certain hearsay statements may be admissible, even if they do not fall into one of the other hearsay exceptions in Rules 803 or 804. A revised version of Rule 807 adding a totality-of-the-circumstances standard took effect on December 1, 2019.

Amended Rule 807 eliminates the requirement that the evidence must be material and the requirement that the proffered evidence must serve the interests of justice. Before the amendment, Rule 807 allowed admission only when notice of an intent to use was made before trial. Under amended Rule 807, the out-of-court statement must be trustworthy and be more probative than other reasonably available evidence. It also expands the procedure for admission of such evidence by permitting the trial court to admit hearsay "during the trial or hearing if the court, for good causes, excuses a lack of earlier notice."

In 2016 and 2017, the Advisory Committee on the Rules of Evidence debated whether to expand the Rule 807 exception to allow the admission of reliable hearsay even absent "exceptional circumstances." Ultimately, the committee decided

against expanding the exception; instead, it opted for an amendment to cure several problems with the current rule.[168]

The problems that the committee identified included the following:

- The requirement that the court find trustworthiness "equivalent" to the circumstantial guarantees in the Rules 803 and 804 exceptions is difficult to apply because these exceptions offer no single trustworthiness standard.
- The requirements in Rule 807 that the residual hearsay must prove a "material fact" and that admission of residual hearsay be in "the interests of justice" are superfluous because these issues are addressed in Rules 102 and 401.
- The requirement that the hearsay statement must be "more probative than any other evidence that the proponent can obtain through reasonable efforts" is unnecessary.[169]

After receiving public comments, the Advisory Committee approved and then submitted the proposed amendment to the Standing Committee for final approval. Under the amended rule, the proponent of the evidence must still establish that the hearsay statement is not otherwise admissible under Rule 803 or 804. Instead of equivalence, the new rule requires the court to analyze the totality of the circumstances surrounding the making of the statement, including any corroborating evidence, to

168. COMM. ON RULES OF PRACTICE AND PROCEDURE, JUDICIAL CONFERENCE OF THE U.S., AGENDA BOOK 99–100 (Jan. 4, 2018), http://www.uscourts.gov/sites/default/files/2018-01-standing-agenda-book.pdf.

169. COMM. ON RULES OF PRACTICE AND PROCEDURE, JUDICIAL CONFERENCE OF THE U.S., AGENDA BOOK 736–37 (June 12–13, 2017), http://www.uscourts.gov/sites/default/files/2017-06-standing-agenda_book_0.pdf.

assess whether there are sufficient guarantees of trustworthiness.

The following is the language of the amended Rule 807 (Committee Notes to amended Rule 807 are in Appendix B):

> Rule 807. Residual Exception
>
> **(a) In General.** Under the following ~~circumstances~~ conditions, a hearsay statement is not excluded by the rule against hearsay even if the statement is not ~~specifically covered by~~ admissible under a hearsay exception in Rule 803 or 804:
>
> > **(1)** the statement ~~has equivalent circumstantial~~ is supported by sufficient guarantees of trustworthiness—after considering the totality of the circumstances under which it was made and evidence, if any, corroborating the statement; and
> >
> > **(2)** it is offered as evidence of a material fact;
> >
> > **(~~3~~2)** it is more probative on the point for which it is offered than any other evidence that the proponent can obtain through reasonable efforts~~; and~~.
> >
> > **(4)** admitting it will best serve the purposes of these rules and the interests of justice.
>
> **(b) Notice.** The statement is admissible only if~~, before the trial or hearing,~~ the proponent gives an adverse party reasonable notice of the intent to offer the statement ~~and its particulars, including the declarant's name and address,~~ —including its substance and the declarant's name—so that the party has a fair opportunity to meet it. The notice must be provided in writing before the trial or

> hearing—or in any form during the trial or hearing if the court, for good cause, excuses a lack of earlier notice.[170]

170. COMM. ON RULES OF PRACTICE AND PROCEDURE, JUDICIAL CONFERENCE OF THE U.S., AGENDA BOOK 409–10 (June 12, 2018), https://www.uscourts.gov/rules-policies/archives/agenda-books/committee-rules-practice-and-procedure-june-2018. (new material is underlined; matter to be omitted is struck).

III. EMERGING ESI EVIDENTIARY ISSUES

A. Determining the Owner/Creator of ESI

ESI may be created by aggregating data from various sources, with various owners. With increasingly more complex interconnected systems, determining the actual owner or creator of ESI becomes more challenging. However, a custodian or other qualified witness must be able to testify as to the source of the information, circumstances associated with the record's creation, and the degree of regularity of the organization's practice and its record making and keeping. Therefore, it becomes imperative to determine who or what created the content to be able to authenticate it.

An individual may create various electronic documents that are in turn passed to others through various electronic mediums such as emails, collaborative environments, and other shared networks. These individuals may in turn modify the document either on the shared space or on their individual devices.

B. Understanding the Limits of Technology

The proliferation of technology has transformed the nature of "documents." What was once primarily in hard-copy, ink-and-paper format is now often in ESI format but is no less a document.[171] The overwhelming majority of documents generated today are ESI, including not only digital versions of those that are analogous to documents of the past (e.g., word processing and spreadsheets) but also an entirely new class of digital documents consisting of what were formerly verbal conversations:

---

171. Indeed, one of the most ubiquitous word-processing applications refers to individual files as "documents." *Create a document in Word*, MICROSOFT, https://support.office.com/en-us/article/create-a-document-in-word-aafc163a-3a06-45a9-b451-cb7250dcbaa1?wt.mc_id=fsn_word_quick_start (last visited May 6, 2020).

text messages, Skype, Voice over Internet Protocol (VoIP) calls, video conferences, and social media postings, to name a few.[172] Moreover, some technology—the IoT—has created an entire class of ESI that otherwise wouldn't exist, such as GPS location data and biological data from wearable devices.[173]

Given the proliferation in the volume of ESI and the changing nature of such "documents," actors in the legal system have and will continue to turn to technology for assistance in identifying, analyzing, and ultimately authenticating ESI for use as evidence in both civil and criminal cases. Such technology may also be important in establishing the closely related chain of custody.[174] While deficiencies in the chain of custody do not destroy the admissibility of the proffered evidence, they go to the weight that the jury may give to the evidence. In light of the interplay between Rule 104(a) and (b), however, deficiencies in either authentication or chain of custody may produce the same result.[175]

---

172. 2 RAYMOND T. NIMMER & HOLLY K. TOWLE, THE LAW OF ELECTRONIC COMMERCIAL TRANSACTIONS, *E-Mails and Evidence in E-Commerce Contexts* § 13.09, pt. C (2d ed. 2018).

173. *See* Section II.D.5, *supra*.

174. United States v. Blank, No. WDQ-14-10448, 2015 WL 4041408, at *8 (D. Md. June 30, 2015), *aff'd*, 659 F. App'x 727 (4th Cir. 2016) (quoting United States v. Howard-Arias, 679 F.2d 363, 366 (4th Cir. 1982)) (finding that, as a practical matter, chain of custody is a variation of the authenticity requirement).

175. *See* U.S. COURT OF APPEALS FOR THE THIRD CIRCUIT, MODEL CIVIL JURY INSTUCTIONS 1.5 (2015) ("Consider it in light of your everyday experience with people and events, and give it whatever weight you believe it deserves."); U.S. COURT OF APPEALS FOR THE SEVENTH CIRCUIT, FEDERAL CRIMINAL JURY INSTRUCTIONS 2.02 (2012) ("Give the evidence whatever weight you decide it deserves."); Pattern Instruction No. 2.02 ("It is up to you to decide how much weight to give to any evidence, whether direct or circumstantial."); U.S. COURT OF APPEALS FOR THE NINTH CIRCUIT, MODEL CIVIL JURY INSTRUCTIONS 1.12 (2017) ("It is for you to decide how much weight to give to any evidence."); Flores v. City of Westminster, 873 F.3d 739, 758 (9th

Although technology can provide many tools to assist in the process of authentication (including establishing the chain of custody), it is important to understand these tools and their potential role, including their limitations.

1. Hashing

One of the most important ways of authenticating ESI is through hash values:

> A hash value is a unique numerical identifier that can be assigned to a file, a group of files, or a portion of a file, based on a standard mathematical algorithm applied to the characteristics of a data set. The most commonly used algorithms, known as MD5 and SHA, will generate numerical values so distinctive that the chance that any two data sets will have the same hash value, no matter how similar they appear, is less than one in one billion. "Hashing" is used to guarantee the authenticity of an original data set and can be used as a digital equivalent of the Bates stamp used in paper document production.[176]

Cir. 2017), *cert. denied sub nom.,* Hall v. Flores, 138 S. Ct. 1551 (2018) (quoting Tortu v. Las Vegas Metro. Police Dep't, 556 F.3d 1075, 1084 (9th Cir. 2009)); United States v. Vidacak, 553 F.3d 344, 350 (4th Cir. 2009); United States v. Pantic, 308 F. App'x 731, 733 (4th Cir. 2009); United States v. Cardenas, 864 F.2d 1528, 1531 (10th Cir. 1989) ("[D]eficiencies in the chain of custody go to the weight of the evidence, not its admissibility; once admitted, the jury evaluates the defects and, based on its evaluation, may accept or disregard the evidence.").

176. *See* Grimm et al., *supra* note 58, at 17 n.47 (quoting BARBARA J. ROTHSTEIN ET AL., MANAGING DISCOVERY OF ELECTRONIC INFORMATION: A POCKET GUIDE FOR JUDGES 38 (2d. ed. 2007)).

There are three areas of concern regarding the use of hash algorithms: (i) encryption; (ii) known file identification; and (iii) file and or data authentication.[177] This *Commentary* focuses on the latter two concerns.

Hashing is based on algorithms that are essentially a set of rules for a mathematical process.[178] Herein lies its inherent weakness, because a mathematical process is based on rules that are predictable and repeatable.[179] Such predictability can lend itself to manipulation and cause either a "collision attack" of algorithms or result in a matching value. Such manipulation, however, is a complex process and has only been successfully accomplished in a laboratory setting where the manipulator must have physical possession of the target file and be able to alter the file before the hash algorithm is run. Outside the laboratory, for purposes of identifying and authenticating ESI (item iii, above), such a collision is statistically nearly impossible.[180] Nevertheless, a strict protocol for the chain of custody of files should be implemented to eliminate the opportunity to manipulate the target file. Further, for purposes of known file identification,[181] known file hash sets (known as Secure Hash

177. Don L. Lewis, *The Hash Algorithm Dilemma—Hash Value Collisions*, FORENSIC MAG. (Dec. 2008).

178. *Id*.

179. *Id*.; *see* FED. R. EVID. 902 advisory committee's notes to 2017 amendments ¶ 14.

180. Lewis, *supra* note 177 ("For use in file identification and authentication, there is a greater probability that [a] single individual, from a twelve member jury, will win the Power Ball Lottery sixty days in a row, than an accidental occurrence of two matching MD5 hash values from files that have not been manipulated to collide.").

181. *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 541 (2005); United States v. Reddick, 900 F.3d 636, 637 (5th Cir. 2018), *petition for cert. filed*, No. 18-6734 (U.S. Nov. 19, 2018); United States v. Borowy, 595 F.3d 1045, 1048 (9th Cir. 2010); United States v. Cartier, 543 F.3d

Algorithm) have been created independently by the National Institute of Standards and Technology and the National Software Reference Library. Although it is virtually impossible to create a hash value of a contraband image, even if it were possible, it would be traceable in the independent known data sets.[182] One important caveat: the research is based on current technology. It is possible that use of artificial intelligence and other advanced computing capabilities may produce tools to manipulate hashes in the future. There is likely to be a continuing technology race to further strengthen on the one hand, and manipulate on the other hand, the hashing algorithms.

Regardless of future possibilities of compromise, hashing can be a means of efficiently determining whether two files are exact duplicates of each other or whether a single file has been altered. The reliability and usefulness of hashing depends on a trustworthy reference. Either the subject file or the copy (or its hash value) must be preserved in a way that ensures there has been no tampering with that reference file.

2. Encryption

The use of encryption and digital signatures can also provide a basis for trust. At a simple level, encryption uses a secret key to scramble the contents of a file so that only those with access to the key may read the file. A digital signature uses the same technology to enable a party to use its secret key to indicate that

442, 445 (8th Cir. 2008); United States v. Miller, No. CV 16-47-DLB-CJS, 2017 WL 2705963, at *1 (E.D. Ky. June 23, 2017); United States v. Noden, No. 8:16-cr-00283-LSC-MDN, 2017 WL 1406377, at *1 (D. Neb. Apr. 20, 2017); United States v. Feldman, No. 13-CR-155, 2014 WL 7653617, at *4, (E.D. Wis. July 7, 2014); United States v. Woods, 730 F. Supp. 2d 1354, 1362 (S.D. Ga. 2010); United States v. Cartier, No. 2:06-cr-73, 2007 WL 319648, at *1 (D.N.D. Jan. 30, 2007).

182. *See* Lewis, *supra* note 177.

it has "signed" an electronic document. Well-established products enable these processes to work fairly seamlessly, although managing the keys used for encryption can become an issue, especially at an enterprise level.

Using these technologies, it is possible to assert that a person signing an electronic document has viewed and approved the document, much as someone would indicate their acceptance of a document (or indicate their authorship of a letter) by signing their name in ink. In legal circles, this is commonly referred to as "non-repudiation."

However, a digital signature actually indicates something slightly different: that someone with access to the key has signed the document. Keys can be stolen or borrowed (copied), frequently without the knowledge of the owner of the key. Similarly, one must link a key back to a specific individual, which generally requires an inquiry to the party that issued the key and an assessment of the veracity of the key issuer. And, even assuming a reputable issuer, that party may distribute keys under varying levels of scrutiny, requiring only an email address at the lower end all the way to requiring a passport or other official identification at the higher end.

For example, it may easily be proven that a key issued to John Smith by KeyCorp was used to sign an important document. However, upon inquiry to KeyCorp, it may be determined that the key was sent by email to JohnSmith@yahoo.com without any verification of John Smith's identity.

Additionally, there is nothing about a plain digital signature that can be used to prove when it was created. It is possible for a party in control of the digital certificate (cryptographic key) to falsify the value/appearance of time in conjunction with manipulated data and force a signing event that would be technically impossible to identify or distinguish from a legitimate digital signature. In such a scenario, the resulting data/signature

combination would be mathematically true but semantically false. However, digital signatures can be used in combination with alternative methods for establishing authenticity.

3. System Metadata

Metadata can be another useful checkpoint for determining authenticity.[183] For example, email messages generally contain a substantial amount of metadata information, including a unique message ID as well as information on the unique internet locations (IP addresses) where the message originated and was handled along the way to its destination. Similarly, operating system metadata can be a useful tool. Most operating systems maintain information about individual files: the dates that a file was created, last modified, and last accessed. For example, in a case where an individual claims that she did not create a document until July 1 but the system metadata shows that the document was created on May 1, this data may be helpful.

However, metadata can be unreliable and may be subject to manipulation and nonobvious deletion. A moderately sophisticated user may be able to manipulate system dates. Although traces of this manipulation may be left behind, detecting such traces can be extremely difficult and expensive or simply impossible. Worse, use of files after the fact, such as an investigator opening a file for review, can modify metadata and make it useless or misleading for authenticity purposes. Accordingly, careful attention should be paid to the methods used to authenticate metadata.

183. For a detailed discussion about metadata, *see The Sedona Principles, Third Edition*, *supra* note 167, Principle 12 at 169 *and* The Sedona Conference, *Commentary on Ethics & Metadata*, 14 SEDONA CONF. J. 169, 173–75 (2013).

4. Computer Forensics and Anti-Forensics

Computer forensics "is the art and science of applying computer science to aid the legal process. Although plenty of science is attributable to computer forensics, most successful investigators possess a nose for investigations and a skill for solving puzzles, which is where the art comes in."[184] Computer forensics involves the location, examination, identification, collection, preservation, and analysis of computer systems and ESI and often includes the rendering of a qualified expert opinion regarding those systems and ESI.

Computer forensics typically involves the employment of specialized and sophisticated computer-based tools to aid in the performance of the various investigation and documentation activities, which can be costly and time consuming. Use of forensic software to identify, acquire, analyze, and store ESI can generally be divided into two processes: (1) static environment and (2) live environment. In a static environment, a mirror image copy is made of the system or storage device (e.g., a hard drive). The accuracy of the copy is established by matching the hash values of the target drive, and each file on the drive, with the hash values of the copy. Then, forensic software can be used to extract evidence from the copy. In a live environment, the forensic software runs in the target system's environment, which in itself affects the system (e.g., changing system metadata, directories, etc.). While evidence from both processes has been admitted in court, evidence acquired from a live system can be vulnerable to attack, particularly if there is a break in the digital chain of custody.

Anti-forensics is the employment of sophisticated tools and methods used for the intentional fabrication and/or

184. CHRISTOPHER L.T. BROWN, COMPUTER EVIDENCE: COLLECTION & PRESERVATION 4 (2d ed. 2010).

manipulation of ESI on a computer system intended to thwart forensic examination. In short, anti-forensics is digital forgery.

The sophistication of anti-forensics may soon overtake (if it has not already) the ability to detect or defend against it. For example, in *United States v. Tippens*, the defendant proffered exhibits that he had acquired from Wikileaks that documented that agencies of the United States have the:

> ability to hack into a computer without leaving any trace that it had been hacked or that an exploit had been placed on it . . . [such] that even if Defendant completed a thorough forensic examination of Defendant's computer and devices, Defendant would not be able to determine whether child pornography had been planted or whether security settings had been modified.[185]

Such capabilities to thwart forensic detection of infiltration and tampering threaten the veracity of expert testimony regarding the results from a forensic examination. There will almost certainly be a race between forensic and anti-forensic capabilities as technology continues to advance.

5. Blockchain

Blockchain is a distributed digital ledger that maintains a continuously growing list of ordered records, called "blocks." It uses algorithms to encrypt data that is shared widely across numerous computers known as "nodes," so that no single person or organization controls that data. A hash is created to ensure trust on the network. Each signature is combined with others to form an unbreakable cryptographic chain that can be

185. No. CR 16-5110 RJB, 2017 WL 11511726, at *2 (W.D. Wash. Mar. 16, 2017).

independently tracked and its authenticity verified.[186] Transactions using a blockchain cannot be changed; they can only be reversed with another transaction. A block generally contains four pieces of information: (1) the hash of the previous block, (2) a summary of the included transaction, (3) a time stamp, and (4) the proof of work that went into creating the secure block.[187]

To authenticate the data stored in the blockchain, the veracity of the data must be established before it is added to the blockchain. Therefore, the electronic devices (e.g., IoT) capturing the data must each be certified and authenticated independently.[188] The human element involved in these processes means that authenticating the link between the physical data and the digital data cannot be done by the blockchain technology itself as yet.[189] However, once the link is established, the evidence from the blockchain will establish the chain of custody. The blockchain will reveal whether a document has been manipulated, whether it is what it purports to be, and whether all data that is supposed to come with the document is actually there.

A blockchain network lacks a centralized point of vulnerability, making it extremely difficult for hackers to exploit. Further, as each block includes the previous block's hash, any attempts to alter any transaction within the blockchain will be detectable. Because the blockchain is a decentralized network that connects multiple parties, it would act as a single digital

186. John McKinlay et al., *Blockchain: background, challenges and legal issues*, DLA PIPER, (Feb. 2, 2018), https://www.dlapiper.com/en/oman/insights/publications/2017/06/blockchain-background-challenges-legal-issues/.

187. *Id*.

188. Adrian Clarke, *The Blockchain Can Finally Secure Supply Chains Against Cyberattacks*, (Dec. 26, 2018, 7:00 AM), https://www.law.com/legaltechnews/2018/12/26/the-blockchain-can-finally-secure-supply-chains-against-cyberattacks/.

189. *Id*.

master ledger for an entire financial system, enabling any transaction to be tracked from beginning to end.

Reported opinions in which ESI derived from blockchain ledgers was admitted into evidence include: *United States v Ulbricht* and *Alibaba Group Holding Limited v. Alibabacoin Foundation*.[190] In *Ulbricht*, the Department of Justice was able to identify Ulbricht as "Dread Pirate Roberts," the operator of the online drug distribution system known as Silk Road. This was accomplished, in part, by tracing $18 million worth of Bitcoin on Ulbricht's computer to transactions on Silk Road servers using transaction history on Silk Road's blockchain ledger.[191] In *Alibaba*, the defendant attempted unsuccessfully to escape the reach of New York's long-arm statute by introducing evidence that the subject transactions linked to New York were found to be on blockchain servers outside the United States in Minsk, Belarus.[192]

Though blockchain can by itself be comparatively secure, it is not entirely invulnerable. It is only as secure as the system that it works on, the application that interacts with it, and the protocol that supports it (i.e., private and public keys), which are all vulnerable to attack resulting from human interaction. For example, blockchain is famously associated with Bitcoin and other cryptocurrency trading, which have been the subject of various reported scams. In February 2018, a complaint was filed in the Delaware Superior Court by Elizabeth White,[193] who was the

190. United States v Ulbricht, 858 F.3d 71 (2d. Cir. 2017); Alibaba Grp. Holding Ltd. v. Alibabacoin Found., No. 18-CV-2897 (JPO), 2018 WL 5118638 (S.D.N.Y. Oct. 22, 2018).

191. *Ulbricht*, 858 F.3d at 87–88.

192. *Alibaba Grp. Holding Ltd*., 2018 WL 5118638, at *3–4.

193. Rhys Dipshan, *Successful Fraud Case Breaks New Ground: Assistance from a Cryptocurrency Exchange*, LEGALTECH NEWS , (June 29, 2018 11:10 AM),

victim of cryptocurrency fraud in December 2017 by an anonymous man who contracted to trade Bitcoin for her XRP.[194] Instead, he manipulated the escrow and exchange platform Cointal to steal White's cryptocurrency. White was eventually able to trace her XRP to a digital wallet on the Delaware-registered cryptocurrency exchange platform Bittrex. An application was filed requiring Bittrex to disclose the identity of the anonymous fraudster and turn over White's stolen assets from his account. Default judgment was obtained against the anonymous fraudster and Cointal. With Bittrex's cooperation, she was able to recover her XRP.[195]

The admissibility of blockchain receipts as evidence of some underlying activity that was recorded on a blockchain could raise hearsay issues. It could probably be admitted through certification by a qualified person under a combination of the "business records" exception to hearsay under Rule 803(6) and Rule 902(13) on the reliability of the system or process that produced it. To qualify as a "business record," testimony would be required from a programmer-custodian or similarly knowledgeable person that the blockchain receipt was generated at the time of the transaction and kept in the course of a regularly conducted business activity.[196]

---

https://www.law.com/legaltechnews/2018/06/29/successful-fraud-case-breaks-new-ground-assistance-from-a-cryptocurrency-exchange/.

194. Jake Frankenfield, *Ripple (Cryptocurrency)*, INVESTOPEDIA (Aug. 11, 2019), https://www.investopedia.com/terms/r/ripple-cryptocurrency.asp ("Ripple is a technology that acts as both a cryptocurrency and a digital payment network for financial transactions. Ripple was released in 2012 and co-founded by Chris Larsen and Jed McCaleb. The coin for the cryptocurrency is premined and labeled XRP.").

195. Dipshan, *supra* note 193.

196. *See* 12 VT. STAT. ANN. § 1913. Blockchain enabling (2018) (providing rules for authentication, admissibility, and presumptions for blockchain records including that a blockchain digital record "shall be self-authenticating

Vermont recently implemented a statute to facilitate the authentication and admissibility of blockchain evidence.[197] The rule recognizes that blockchain can be self-authenticated under Vermont's version of Rule 902 if accompanied by the declaration of a qualified person. The text of the rule is provided in Appendix C, *infra*.

C. *Application of Federal Rules and Cases in State Court and Vice Versa*

1. Federal law application in state cases

Many states model their rules of evidence and procedure as much as possible after federal rules for many good reasons. The most prominent is that where a state and federal rule of evidence or procedure are the same or similar, most state court judges may use federal cases applying the equivalent rule in similar circumstances as guidance or persuasive authority.[198] In the case of electronic evidence, federal cases on discovery and admissibility issues are far more abundant than state cases, the latter of which normally remain unpublished unless a case is appealed. Federal district and magistrate judges also address ESI evidence and discovery issues far more often than state court judges, which adds to the quality and persuasiveness of federal decisions as a whole.

---

pursuant to Vermont Rule of Evidence 902, if it is accompanied by a written declaration of a qualified person . . . ."). *See also* Illinois Blockchain Technology Act, 205 ILL. COMP. STAT. 730/10 (2020) (permitted use of blockchain in a proceeding).

197. *Id*.

198. Ellis v. Toshiba Am. Info. Sys., Inc., 218 Cal. App. 4th 853, 861, n.6 (Cal. 2013) ("There is little California case law regarding discovery of electronically stored information under the act. 'Because of the similarity of California and federal discovery law, federal decisions have historically been considered persuasive absent contrary California decisions.'").

In addressing an admissibility issue involving ESI evidence, if there is no binding state authority on the issue, a comparison of the applicable Federal Rule of Evidence with the analogous state rule is the first step. If the rules are identical or similar in all respects material to the case at hand, the applicable principles and guidance in this *Commentary* as well as any relevant federal cases applying the rule may serve as persuasive authority.

2. State law application in federal cases

Given that new ESI admissibility issues emerge frequently as technology and the culture of information creation and communication evolve, finding binding precedent for the application of evidentiary rules can be difficult. Many regard state courts as a suitable laboratory for developing federal rules and case law, especially when the state courts are addressing issues frequently and in systematic fashion. While federal courts are not bound by state court precedent, there is no reason litigators should not identify and cite state court cases in the absence of direct federal authority. A federal court may accept or reject the reasoning of the state court cases, but, because many state court rules of evidence are identical or similar to their federal counterparts, guidance from state courts may be useful. This is especially true for cases from the same state in which the federal court sits.

Some admissibility issues are especially common in state court, where unique jurisdiction establishes common issues. One such example is foreclosure cases, in which state court judges and judicial officers frequently encounter the issue of ESI evidence of promissory notes that pass from entity to successor entity. When the lender forecloses, proving ownership of the note at the time the foreclosure is filed can be problematic when challenged by the debtor. This raises issues of authentication and hearsay. It also implicates the business-records exception to the hearsay rule.

Admissibility of bank records in an industry that frequently assigns mortgages and notes can be challenging. For example, in Florida foreclosure cases where a successor corporation takes custody of business records created by a predecessor organization and integrates them within its own records, the acquired records are treated as having been "made" by the successor business, such that both records constitute the successor business's singular "business record."[199] When introducing such records, a successor business may establish the trustworthiness of records under the business-records exception by independently confirming the accuracy of the third party's business records upon receipt and providing testimony setting forth the procedures used to independently verify the accuracy of the payment history records from the prior organization.[200]

Foreclosure cases and hearsay objections to documents presented in court play out in lower and appellate state courts. For example, *Jackson v. Household Financial Corporation III* held that introducing bank records through an employee who regularly reviewed home loans and claimed to be familiar with the bank's loan servicing practices was sufficient foundation under the business-records exception for the initial foundation burden, thus shifting the burden to the opposing party. In doing so, Florida's Supreme Court held that a qualified witness who testifies as to each element of the business-records exception for the admission of a business record lays sufficient predicate for admission of the document such that the document should be admitted unless the opponent establishes it to be untrustworthy.[201] However, *Knight v. GTE Federal Credit Union* held that the witness proffering a record was not competent to provide

199. *See* Deutsche Bank Nat'l Trust Co. v. Sheward, 245 So. 3d 890, 892–93 (Fla. Dist. Ct. App. 2018).

200. *See id*.

201. Jackson v. Household Fin. Corp. III, 298 So. 3d 531 (Fla. 2020).

foundation where he did not demonstrate that he was well enough acquainted with the entity's business practices to authenticate the letter. *Knight* premised its holding on the fact that the witness did not work for the servicing agent, never visited its facility, never spoke with its employee, and had no documents other than the servicer's letter log to support his testimony.[202]

In the context of a Florida foreclosure action, a representative of a loan servicer testifying at trial was not required to have personal knowledge of the documents being authenticated but did have to be familiar with and know how the company's data was produced.[203] The witness must ultimately be well enough acquainted with the activity to provide testimony.[204] *Wells Fargo Bank, N.A. v. Balkissoon* describes the qualifications needed for a witness qualifying records under the business-records exception to the hearsay rule.[205] If the witness is sufficiently familiar with the records to be admitted, the witness need not be familiar with the mechanics of actually typing the data into the system because there is no requirement that the witness have such knowledge.[206] However, in *Maslak v. Wells Fargo Bank, N.A.*, the opposite result occurred where a bank's witness did not know whether someone at outside counsel's office changed or modified a document; she failed to testify about how payments were received and processed or the bank's procedures for inputting

202. Knight v. GTE Fed. Credit Union, No. 2D16–3241, 2018 WL 844352, at *2–3 (Fla. Dist. Ct. App. Feb. 14, 2018).

203. *See* Sanchez v. Suntrust Bank, 179 So. 3d 538, 541 (Fla. Dist. Ct. App. 2015); Glarum v. LaSalle Bank Nat'l Ass'n, 83 So. 3d 780, 783 (Fla. Dist. Ct. App. 2011).

204. Cayea v. CitiMortgage, Inc., 138 So. 3d 1214, 1217 (Fla. Dist. Ct. App. 2014); Cooper v. State, 45 So. 3d 490, 493 (Fla. Dist. Ct. App. 2010).

205. 183 So. 3d 1272, 1275–77 (Fla. Dist. Ct. App. 2016).

206. FLA. STAT. § 90.803(6)(a) (2014).

payment information or the computer system the bank used.[207] Similarly, in *Cassell v. Green Planet Servicing, LLC*, testimony on the business-records exception was inadequate when the witness testified that she had no personal knowledge of the policies and procedures used by the entities that created the payment history and notice letters.[208] Published authority making close distinctions in such cases may provide guidance to federal courts and other state courts looking at similar admissibility issues.

Foreclosure cases have raised admissibility issues relating to ownership of e-notes. In *Rivera v. Wells Fargo Bank, N.A.*, the borrowers in a foreclosure case challenged the ownership and admissibility of an e-note, which was the only original, signed evidence of indebtedness in the case.[209] The appellate court affirmed the foreclosure, holding that the bank proved foundation for admissibility and ownership of the electronic document.

In *DiGiovanni v. Deutsche Bank National Trust Company*, a printout produced from the trial judge's own internet research during a foreclosure trial was held to be not properly authenticated.[210] Because websites are not self-authenticating, the party proffering the evidence had to produce some statement or affidavit from someone with knowledge of the website. The appellate court also held that it was improper for the judge to do *ex parte* fact research on the internet.

207. 190 So. 3d 656, 659–60 (Fla. Dist. Ct. App. 2016).

208. 188 So. 3d 104, 105 (Fla. Dist. Ct. App. 2016).

209. 189 So. 3d 323, 327–29 (Fla. Dist. Ct. App. 2016).

210. 226 So. 3d 984, 988–89 (Fla. Dist. Ct. App. 2017).

IV. PRACTICAL GUIDANCE ON THE USE OF ESI IN COURT

Judge Grimm's discussion in *Lorraine* makes it clear that parties should start to think about evidentiary issues much earlier than was the practice when dealing only with hard-copy materials. This is especially critical because parties will need to ensure they have defensible preservation and collection protocols in place to maintain the information that the amended Federal Rules of Evidence require in the certification. Thus, parties should approach the discovery of ESI by always keeping the end goal—the successful admission of evidence—in mind.

The first step is to assess what potentially discoverable information is available. Only with that understanding can parties determine the appropriate scope of discovery, the proper tools and resources required to harvest the ESI, and the proportionality—or lack thereof—of the cost of discovery compared to the needs of the case. To the extent possible, parties should strive to collect only that data that is necessary for the case, narrowing the scope of the collection as much as possible by using relevant file types, date ranges, and the like. The prerequisite steps here include identifying and interviewing custodians and determining where data is stored. Another is determining who owns that information. For example, if a social media platform owns information, or if an individual has potentially relevant information on a personal cell phone, special permission and methods may be needed to preserve and collect that data.

As parties collect data, they should take steps to ensure they maintain its integrity. To this end, they should use the appropriate approach, which could include using a write-blocking solution that avoids data alteration. The improper collection of data, including metadata, can lead to data loss, alteration, or manipulation.

Before and after collection, parties should engage in quality assurance to validate that the data's integrity is intact. One way

to do this is to perform a hash analysis, both before and after collection, to ensure that the collection process did not alter any files.

In assessing whether to self-collect or to outsource data collection entirely, a key consideration is how much cost and risk the organization is willing to bear in collecting the data. That may vary from case to case. Self-collection, which comes in different forms, is often the fastest and least expensive way to collect data, but the individuals doing the collecting may lack specialized training and tools. Outsourcing offers the benefit of allowing trained forensic data professionals with the proper tools to perform collections.

No matter the method of collection, an essential step is to document the chronology of the ESI, including details about its custody, control, transfer, and disposition, in a chain of custody that can be used to authenticate the evidence later in the case. The documentation should also log who collected and handled the data at each stage.

A. Use of ESI in Static vs. Native/Live Format

In the past, parties were limited to sharing exhibits in hard copy. Today, parties can instead choose between static format and native (or live) format—the format in which the ESI was created and maintained—when presenting ESI. Parties should evaluate the advantages and disadvantages of different formats early in discovery, as these decisions can later affect the evidence they are able to present at trial.[211]

Static ESI, often presented in TIFF (tagged image file format) or PDF file format, may be simpler and less expensive to produce than native images, because it does not require any special know-how or tools. Its simplicity also makes it easier to copy,

211. *See Primer on Social Media*, *supra* note 75, at 44.

share, and authenticate. But it has several drawbacks that can make it inferior to native format ESI in many cases, particularly when the ESI is dynamic and complex.

One clear advantage of native format ESI is that it maintains the characteristics of data that would be lost if we reduced the data to static form, such as by playing a video or sound recording, revealing the formulas behind spreadsheet cells, or running a process. Another advantage is that native format files allow parties to manipulate data for demonstrative purposes without destroying the underlying data. A static form of ESI may also lack metadata that may be helpful to interpreting the ESI's origin. Of course, with these benefits comes the hardship of ensuring that data does not become corrupted and the potential requirements for additional hardware or software as well as technical expertise.

B. Evidence to Assist the Jury on the Permissive Spoliation Inference

Spoliation occurs where "the evidence was in the party's control; the evidence is relevant to the claims or defenses in the case; there has been actual suppression or withholding of evidence; and, the duty to preserve the evidence was reasonably foreseeable to the party."[212] A range of sanctions is available when a party destroys ESI "with the intent to deprive another party of the information's use in the litigation."[213] The trial court

212. Pace v. Wal-Mart Stores East, LP, 799 F. App'x 127, 130 (3d Cir. 2020).

213. FED. R. CIV. P. 37(e)(2). The admission of relevant evidence of spoliation is also an option under Rule 37(e)(1) to address prejudice and without a finding of intent to deprive. Courts exercising that option have tried to explain why the evidence is admissible. *See* EPAC Techs., Inc. v. Thomas Nelson, Inc., No. 3:12-cv-00463, 2018 WL 3322305, at *3 (M.D. Tenn. May 14, 2018) *and* Karsch v. Blink Health Ltd., 17-CV-3880 (VM) (BCM), 2019 WL 2708125, at *27–28 (S.D.N.Y. June 20, 2019). The degree to which it makes a

may, for example, dismiss the action or impose default judgment. It may instead, however, instruct the jury that it may or must presume that the lost ESI was unfavorable to the spoliator.[214]

If the court elects to give a permissive inference instruction to the jury, evidence may be presented to the jury to aid in the determination of whether to draw the adverse inference while at the same time avoiding unfair prejudice confusion of the issues, misleading the jury, or undue delay.[215] This issue was addressed in *GN Netcom, Inc. v. Plantronics, Inc*.[216]

During the course of discovery in this antitrust action, plaintiff GN learned that defendant Plantronics had engaged in extensive destruction of ESI. GN moved for default judgment as a sanction. Following a hearing, the district court found that Plantronics had acted in bad faith with the intent to deprive GN of relevant evidence but declined to order default judgment.[217] Instead, the trial court opted to give the jury a permissive adverse inference instruction while fining Plantronics $3 million and directing "it to pay GN's spoliation-related fees."[218]

At trial, GN sought to introduce evidence of the spoliation, including testimony from an expert witness, Dan Gallivan, on

---

fact material to the claims or defenses "more or less probably" is crucial. *See* Duran v. County of Clinton, NO. 4:14-CV-2047, 2019 WL 2867273, at *5 (M.D.Pa. July 3, 2019).

214. FED. R. CIV. P. 37(e)(2).

215. Federal Rule of Evidence 403 provides that "[t]he court may exclude relevant evidence if its probative value is substantially outweighed by a danger of one or more of the following: unfair prejudice, confusing the issues, misleading the jury, undue delay, wasting time, or needlessly presenting cumulative evidence."

216. 930 F.3d 76 (3d Cir. 2019).

217. *Id.* at 81.

218. *Id*.

the extent of the spoliation. Concerned that the spoliation evidence would obscure the dispositive antitrust questions presented in the case, the court refused to allow Gallivan to testify. Instead, the court determined that the jury would consider 17 stipulations concerning the spoliation. The jury returned a verdict in favor of Plantronics.

On appeal, a divided Third Circuit concluded that the exclusion of the expert testimony was an abuse of discretion. Finding that the stipulation on the extent of the spoliation was extremely vague ("[I]t may be that several hundred or even up to 15,000 potentially responsive relevant emails were deleted or destroyed"[219]), the majority explained that the expert's proffered testimony was highly probative:

> Gallivan's expert testimony would have assisted the jury in narrowing that range, giving it evidence on which it could base an important decision: whether Plantronics engaged in a "massive cover-up." Without Gallivan's testimony, it is possible, if not entirely probable, that jurors concluded that only a few hundred emails were deleted, falling short of a massive cover-up; however, if they had evidence that fifteen, five, or even just one thousand emails had been deleted, they might have taken a very different view on whether to apply the adverse inference. . . . The "maximum reasonable probative force" of his testimony was high; therefore, the District Court could have properly excluded it only if that probative value was substantially outweighed by the

219. *Id.* at 87.

> evidence's potential prejudice or by other risks outlined in Rule 403.[220]

Observing that "highly probative evidence is 'exceptionally difficult to exclude,'"[221] the majority ruled that Gallivan's testimony was not unfairly prejudicial, was likely to clarify the stipulations, would not mislead the jury, and would not have unduly prolonged the trial.

The dissenting judge believed that the majority had assigned too little weight to the spoliation stipulations, stating that "[t]hese stipulations gave the jury an adequate basis to decide whether to adopt the permissive adverse inference."[222] The dissent also determined that "the majority fail[ed] to give the required deference to the District Court's reasonable conclusions that Gallivan's spoliation testimony posed a substantial risk of distracting the jury from the antitrust merits of the case and that such risk eclipsed the testimony's probative value."[223]

GN Netcom illustrates the delicate balancing of interests that must be undertaken when a jury is being asked to decide whether to draw an adverse inference against a bad-faith spoliator. On the one hand, there is a strong preference to have cases adjudicated on their merits. On the other hand, there is an equally strong concern that the jury should have an adequate presentation of the facts underlying the trial court's decision to give the permissive inference instruction. In some cases, that adequate presentation cannot be made by way of stipulations.

---

220. *Id*.

221. *Id.* at 85.

222. *Id.* at 91 (Smith, C.J., dissenting).

223. *Id*.

C. *Practical Tips for Administration of ESI as Evidence*

ESI admissibility issues should be addressed as early as possible. Consideration should be given to incorporating agreements regarding admissibility into production stipulations or submitting these agreements to the court for approval. This may not be available in criminal cases.

As the degree to which ESI is static decreases, the difficulties of replicating it increase. Therefore, care should be taken to choose the most replicable form of ESI that provides the necessary probative information (including metadata).

D. *Practical Tips for Seeking Authority on Admission of ESI as Evidence*

Finding case support for admissibility of ESI can be challenging because so few civil cases are actually tried.[224] However, the Federal Rules of Evidence are trans-substantive and apply in civil and criminal proceedings.[225] The only exceptions to the applicability in criminal cases are grand-jury proceedings and "miscellaneous proceedings" such as extradition or rendition;

---

224. *See Civil Jury Project at NYU School of Law*, https://civiljuryproject.law.nyu.edu/about/ (last visited May 7, 2020) ("[I]t is beyond dispute that the civil jury trial is a vanishing feature of the American legal landscape. In 2018 . . . 0.5 percent of federal civil cases were tried before juries—down from 5.5 percent in 1962. This amounted to an average of 2 civil jury trials per authorized federal judgeship in 2018—down from 10 in 1962. Similar trends are evident in states across the nation.").

225. FED. R. EVID. 1101(b) ("These rules apply in: civil cases and proceedings, including bankruptcy, admiralty, and maritime cases; criminal cases and proceedings; and contempt proceedings"); *see also* Stephan Landsman, *Are the Federal Rules of Evidence Dynamite?* 33 B.U. INT'L L.J. 343, 351 (2015) ("A fourth characteristic that strongly colors the FRE is its commitment to a 'trans-substantive' approach to the rules of evidence . . . . While that approach is open to a variety of criticisms, it expresses important values. Chief among them is a democratic impulse that all litigants be treated alike.").

issuing an arrest warrant, criminal summons, or search warrant; a preliminary examination in a criminal case; sentencing; granting or revoking probation or supervised release; and considering whether to release on bail or otherwise.[226] Far more criminal cases end up being tried, and the nature of criminal practice necessarily involves frequent challenges to admissibility and less formal discovery pathways to resolution of authenticity, such as civil requests for admission. Thus, criminal cases should be included in legal research on admissibility issues for civil cases. Criminal cases are creating authority on admissibility of social media,[227] digital security camera ESI,[228] text messaging,[229] emoji,[230] and other forms of ESI.

State court criminal cases may provide helpful or persuasive authority on specific issues of admissibility. For example, authentication of a Facebook video may be accomplished under Rule 901(b)(3) (comparison with an authenticated specimen by an expert witness or the trier of fact) and 901(b)(4) (appearance,

---

226. FED. R. EVID. 1101(d)(2)–(3).

227. *See, e.g.*, State v. Smith, 181 A.3d 118, 134–36 (Conn. App. Ct. 2018) (authenticating Facebook messages using circumstantial evidence); Lamb v. State, 246 So. 3d 400, 409–10 (Fla. Dist. Ct. App. 2018) (authenticating and admitting a Facebook Live video); State v. Hannah, 151 A.3d 99, 107 (N.J. Super. Ct. App. Div. 2016) (authenticating Twitter posting using circumstantial evidence and reply doctrine).

228. *See, e.g.*, People v. Taylor, 956 N.E.2d 431, 438–43 (Ill. 2011) (copy of motion-activated video in non-native format).

229. *See, e.g.*, State v. Papineau, 190 A.3d 913, 935–36 (Conn. App. Ct. 2018) (allowing circumstantial evidence of authorship to authenticate text messages); Pavlovich v. State, 6 N.E.3d 969, 978–79 (Ind. Ct. App. 2014) (using circumstantial evidence to authenticate text messages); State v. Young, 369 P.3d 205, 208–09 (Wash. Ct. App. 2016) (using content to authenticate text messages).

230. *See* Section II.D.12., *supra*.

contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances).

In *Lamb v. State*, a Florida criminal case, one of the defendant's phones contained a Facebook video posted twenty-one minutes after two crimes, showing the defendants with the two stolen vehicles and a stolen watch on a defendant's wrist.[231] Over objection, the appellate court applied equivalent Rule 901 principles and held that the prosecution sufficiently authenticated a social media video under Florida Statute § 90.901.[232]

Conversely, in a prosecution for aggravated assault, the Superior Court of Pennsylvania upheld the trial court's exclusion of Facebook postings that the prosecution attempted to use to link the defendant to the assault.[233] The prosecution could show that the account bore defendant's name, high school, and hometown but was unable to show that the defendant authored ambiguous chat messages or posted a photo of bloody hands because there were no contextual clues, and third persons were posting some of the information in question. Thus, the trial court did not abuse its discretion in finding that the social media evidence lacked authentication.[234]

At least one state has gone so far as adopting an evidence rule specifically dealing with authentication of emails. Washington Evidence Rule 901(b)(10) sets forth the factors that may be used to authenticate email:

> **(b) Illustrations.** By way of illustration only, and not by way of limitation, the following are

231. *Lamb*, 246 So. 3d at 408–10.

232. *Id.* at 410.

233. Commonwealth v. Mangel, 181 A.3d 1154, 1163–64 (Pa. Super. Ct. 2018).

234. *Id*. at 1164.

> examples of authentication or identification conforming with the requirements of this Rule:
>
> . . . .
>
> (10) *Electronic Mail (E-mail)*. Testimony by a person with knowledge that (i) the email purports to be authored or created by the particular sender or the sender's agent; (ii) the email purports to be sent from an e-mail address associated with the particular sender or the sender's agent; and (iii) the appearance, contents, substance, internal patterns, or other distinctive characteristics of the e-mail, taken in conjunction with the circumstances, are sufficient to support a finding that the e-mail in question is what the proponent claims.[235]

These factors have been applied by analogy to other forms of electronic communication.[236]

235. WASH. R. EVID. 901(b)(10).

236. *See* State v. Young, 369 P.3d 205, 208–09 (Wash. Ct. App. 2016) (text messaging); *In re* Detention of H.N., 355 P.3d 294, 302 (Wash. Ct. App. 2015) (authenticating emailed screenshots of text messages by analogy to Wash. R. Evid. 910(b)(10)).

V. ARTIFICIAL INTELLIGENCE USES IN BUSINESS AND LAW[237]

Artificial intelligence (AI) is making major inroads into many industries such as health care, automotive, fitness, financial services, and even litigation. This is and will continue to present significant legal, technological, and ethical challenges for lawyers.[238]

In late 2019, before Covid-19 became a pandemic, a Canadian-based company, BlueDot, used AI to identify an emerging health risk in Wuhan, China. That AI subsequently predicted the global spread of the disease.[239] Voice-controlled personal

237. The Editors wish to acknowledge the significant contribution of The Hon. Paul W. Grimm to this discussion and thank him for allowing us to borrow extensively from his forthcoming law review article on this topic. However, the final draft of this Commentary represents consensus of the drafting team and the Working Group 1 Steering Committee and should not be imputed to any individual contributor.

238. Under the Model Rules of Professional Conduct, lawyers must assess whether they have the requisite skill and knowledge, including *understanding the benefits and risks of the technology involved*, to perform the tasks (either by themselves or in collaboration with an experienced counsel or consultant) involving AI such as: (i) assisting their client in identifying sources (including custodians) of relevant ESI; (ii) engaging in meaningful meet-and-confer sessions with opposing counsel concerning an eDiscovery plan that targets AI as a data source; and (iii) advising a client about the proper method to collect responsive ESI in a manner that preserves the integrity of that ESI for evidentiary purposes when AI is the data source. These challenges will test a lawyer's ability to comply with, among others, Rule 1.1 (competence), Rule 1.3 (diligence), Rule 1.4 (Communications), Rules 5.1 and Rule 5.3 (Supervision), and Rule 5.4 (Professional Independence of a Lawyer).

239. Isaac I. Bogoch, et al., *Pneumonia of unknown aetiology in Wuhan, China: potential for international spread via commercial air travel*, 27(2) J. TRAVEL MED. (Mar. 2020), https://bluedot.global/. See also Cory Stieg, *How this Canadian start-up spotted coronavirus before everyone else knew about it*, CNBC (Mar. 3, 2020, 10:27 a.m.), https://www.cnbc.com/2020/03/03/bluedot-used-artificial-intelligence-to-predict-coronavirus-spread.html. BlueDot also has used its

assistants with evolving "personality" traits allow the "assistant" to use machine-learning algorithms to learn how to pattern its behavior after the "voice-controller." The assistant also has a visual component that allows it to use machine-learning algorithms to understand a voice-controller's facial expressions, voice inflections, and verbal patterns from conversations. Robotic vacuums use AI to scan room size, identify obstacles, and remember the most efficient routes for cleaning.

AI also is making major inroads into law-related activities beyond technology-assisted review.[240] A software program called COMPASS uses AI technology to assess the risk that defendants awaiting sentencing will re-offend, allowing sentencing judges to consider this risk in fashioning conditions of supervision. Similarly, facial recognition software, using AI algorithms, is being used by law enforcement agencies to identify suspects and fugitives in a crowd or captured on closed-circuit television videos (CCTV). Machine-learning algorithms can automatically analyze draft contracts and identify which portions of the contract are acceptable and which are problematic based on prior contracts. In addition, machine-learning models are being used to predict the outcomes of pending cases, using inputs from automated legal research and contextualization of the case's particular fact pattern.

Technology that employs AI programming also will present significant evidentiary challenges when it is offered at hearings and trials. Although, to date, no reported court decision has

---

AI to make early predictions about where the Zika virus and the Ebola outbreak would spread.

240. Ellen M. Gregg, et al., *How Artificial Intelligence is Impacting Litigators*, ALAS LOSS PREVENTION JOURNAL 49 (Summer 2019); and Rob Toews, *AI Will Transform the Field of Law*, FORBES (Dec. 19, 2019 2:09 p.m.), https://www.forbes.com/sites/robtoews/2019/12/19/ai-will-transform-the-field-of-law/#e1907ed7f01e.

been found that comprehensively explores the many evidentiary issues that surround determinations of admissibility of AI, there are a number of rules of evidence that are likely to figure prominently in any such determination. Although there is no single rule in the Federal Rules of Evidence that specifically addresses admissibility of AI technology, Rule 102 encourages counsel and courts to employ the existing rules of evidence to "administer every proceeding fairly, eliminate unjustifiable expense and delay, and promote the development of evidence law, to the end of ascertaining the truth and securing a just determination."[241] In essence, the existing rules of evidence are flexible enough to address novel evidentiary challenges not already directly covered in the rules. There are, however, several rules of evidence that offer great promise in connection with determining admissibility of AI evidence.

The starting place is Rule 401, which defines relevance.[242] Evidence is relevant if it has "*any* tendency to make a fact more or less probable than it would be without the evidence," and "the fact is of consequence in determining the action." [243] Relatedly, irrelevant evidence is never admissible. But relevant, and therefore presumptively admissible, evidence may nonetheless be excluded if precluded by the U.S. Constitution, a federal statute, the rules of evidence, or other rules promulgated by the Supreme Court.[244] Relevant evidence also is inadmissible if its probative value is substantially outweighed by the danger of unfair prejudice, confusing the issues, misleading the fact finder, wasting time, or is needlessly cumulative.[245] Finally, even if relevant

241. FED. R. EVID. 102.

242. FED. R. EVID. 401.

243. *Id*. (emphasis added).

244. FED. R. EVID. 402.

245. FED. R. EVID. 403.

and not otherwise excluded, the fact that evidence is relevant (i.e. may be considered by the fact finder) is no guarantee that it will be deemed credible or given much weight by the fact finder.[246]

In framing this discussion, there are some "big picture" evidentiary concepts to keep in mind when considering the admissibility of AI evidence. First, if a foundation cannot be established to show that the AI-powered technology produces accurate results, the evidence is unreliable and therefore has no relevance. Unreliable evidence has no tendency to prove or disprove facts that are of consequence to resolving a case or issue. But the challenge for lawyers and judges alike is that determining the reliability of AI evidence depends on understanding how the applicable algorithm works. Given the countless applications for AI technology in connection with doing a seemingly endless number of technical chores, the proponent, opponent, and judge deciding whether to admit this evidence must have sufficient information to understand how the technology works. While individuals technically trained in the operation of AI applications may be able to explain *what* the algorithm did and the results the algorithm obtained, those individuals may have difficulty explaining the complexity as to how the algorithm was programmed, or how it produces accurate results. For example, the algorithm developed by the Canadian company Blue Dot (mentioned above) to predict the origins and transmission of the Covid-19 virus took a year to develop and involved input from an "eclectic mix of engineers, ecologists, geographers, and veterinarians, all under one roof", and entailed "training" the computer to detect 150 deadly pathogens through use of thousands of examples.[247] Imagine the challenge a lawyer might face when

246. FED. R. EVID. 104(e).

247. *CBS 60 Minutes: The Computer Algorithm That Was Among the First to Detect the Coronavirus Outbreak* (Apr. 27, 2020).

trying to establish the reliability for this AI application and have evidence of the results of the Blue Dot technology admitted in a trial. Fundamentally, this is an issue of authentication—showing that the technology produces the results that its proponents claim it produces.[248]

Rule 901(b) provides ten nonexclusive examples of how authentication of nontestimonial evidence can be accomplished. Two of them are most likely to be helpful in authenticating AI evidence. First, Rule 901(b)(1) permits the authentication of evidence through "[t]estimony that an item is what it is claimed to be." If this rule is used, then the witness must either meet the conditions of Rule 602 (requiring that witnesses have personal knowledge of the matters they testify about) or meet the qualification requirements of Rule 702 (that the witness have sufficient expertise to testify to a matter requiring scientific, technical, or specialized knowledge, experience, or training, in which case the witness may testify in the form of an opinion, or otherwise). If the witness qualifies under Rule 702, then his opinion testimony may be based on information not personally known by the witness, so long as that information is of the type that similar experts reasonably would rely on.[249] Using the Blue Dot AI technology as an illustration, it is easy to see why a qualified expert would be the most useful person to authenticate that the Blue Dot algorithm produces accurate results, given that it was developed by multiple individuals with different specialties. And a single expert may be sufficient to base his testimony on reliable information provided by the many other experts who helped to develop the algorithm. The time-consuming, and likely expensive, alternative would be to call multiple witnesses

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

249. FED. R. EVID. 703.

to authenticate the algorithm if their testimony was limited to facts about which they have personal knowledge.

Rule 901(b)(9) is the second method of authentication that is likely to be most useful in authenticating AI evidence. It permits authentication by producing evidence "describing a process or system and showing that it produces an accurate result."[250] In this regard, authenticating AI evidence using Rule 901(b)(9) will usually, if not always, be done the same way described above for Rule 901(b)(1)—one or more witnesses with personal knowledge of the authenticating facts, or one or more witnesses meeting the qualifications of Rule 702.

There is an important feature of authentication that needs to be given careful consideration in connection with admitting AI evidence. Normally, a party has fulfilled its obligation to authenticate nontestimonial evidence by producing facts that are sufficient for a reasonable fact finder to conclude that the evidence *more likely than not* is what its proponent claims it is—by a mere preponderance.[251] This is a relatively low threshold—51 percent, slightly better than a coin toss. However, given the complexity of AI algorithms, and the tasks that they can accomplish that would be otherwise impossible, or nearly so, judges may be reluctant to allow a jury to consider AI evidence if its reliability has been established by little more than an

250. FED. R. EVID. 901(b)(9).

251. *See* 31A FEDERAL PRACTICE AND PROCEDURE, EVIDENCE, 2013 QUICK REFERENCE GUIDE, 383 ("Rule 901(a) prescribes that authentication or identification of an item requires only evidence sufficient to support a finding—a 'prima facie case'—that the item is genuine. A bona fide dispute as to authenticity or identity is not to be decided by the judge, but rather is to go to the jury . . . . In other words, conflicting evidence on genuineness goes to weight, not admissibility, so long as some reasonable person could believe that the item is what it is claimed to be."); Ricketts v. City of Hartford, 74 F. 3d 1397, 1411 (2d Cir. 1996); United States v. Johnson, 637 F. 2d 1224, 1247 (9th Cir. 1980).

evidentiary coin toss. Because the judge must act as the gatekeeper who determines whether the evidence that may be considered by the jury,[252] a party relying on AI evidence would be wise to provide as much evidence as possible to authenticate the AI.

One way a party can enhance the weight of the evidence it offers to authenticate AI applications is to clearly demonstrate how the results it produces are accurate. In this task, Rule 702 and the cases that have explored the criteria for admitting scientific or technical evidence provide helpful guidance. Rule 702 requires that expert testimony be based on sufficient facts and reliable methodology, reliably applied to the facts of the case.[253] These factors were added to the evidence rules in 2000[254] to bolster the rule in light of the Supreme Court's decisions in *Daubert v. Merrell Dow Pharmaceuticals, Inc.*[255] and *Kumho Tire Co. v. Carmichael*.[256] Therefore, while Rule 702 was not intended to codify the decision in *Daubert*, the factors discussed in that decision relating to determining the reliability of scientific or technical evidence are quite informative in showing that Rule 702's reliability factor has been met. As described in the Advisory Committee Notes to Rule 702, the "*Daubert* Factors" 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

252. *See* FED. R. EVID. 104(a) ("The court must decide any preliminary question about whether . . . evidence is admissible").

253. FED. R. EVID. 702(b)-(d).

254. FED. R. EVID. 702 advisory committee's notes to 2000 amendment.

255. 509 U.S. 579 (1993).

256. 526 U.S. 137 (1999).

> existence and maintenance of standards and controls; and (5) whether the technique or theory has been generally accepted in the scientific [or technical] community.

To authenticate AI technology, a proponent must show that the technology produces accurate, reliable results. When the accuracy of technical evidence has been verified by testing; the methodology used to develop it has been published and subject to review by others in the same field of science or technology; when the error rate associated with its use is not unacceptably high; when standard testing methods and protocols have been followed; and when the methodology used is generally accepted within the field of similar scientists or technologists; then it can be established as authentic because it does what its proponents say it does. Contrastingly, when the accuracy of evidence has not been tested; when its methodology has been treated as a trade secret by its developer, and not verified by others; when applied it produces an unacceptably high error rate; when standard procedures not followed when the methodology was developed or employed; or when the methodology is not accepted by others in the same field; then it would be challenging to maintain that the methodology does what its proponent claims it can do, which might render the evidence inadmissible. The bottom line is that if a proponent is going to rely on evidence produced by AI technology, he should consider these factors and marshal facts to show compliance with as many of factors as possible.

The final rule that is promising when authenticating AI technology is Rule 902(13), which permits the self-authentication of certified records generated by an electronic system or process shown to produce an accurate result.[257] In lieu of calling one or

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

more witnesses to establish the accuracy of the results of the AI technology, the party planning to introduce the AI evidence can prepare a certificate that meets the requirements of Rule 902(11). The records generated by the AI technology and the authenticating certificate are then produced in advance of the trial or hearing where the evidence will be introduced, and if there is no objection raised, the evidence is authenticated without the need to call live witnesses. This can significantly reduce the cost of authenticating AI evidence at a hearing or trial. But Rule 902(13) is no shortcut for completeness or accuracy in providing the facts necessary to show the accuracy of the AI technology. In fact, to succeed, the certificate must be as detailed and complete as live testimony by the witnesses with personal knowledge or technical expertise who would be called if the proponent of the AI evidence planned to authenticate it with witnesses. And the person or persons who provide the certificate must be similarly qualified (i.e., personal knowledge or scientific or technological expertise).

Given the rapid expansion of the use of AI in major industries and the evidentiary issues presented by AI, The Sedona Conference Working Group 1 will continue to watch this area of the law and update this *Commentary* as appropriate.

APPENDIX A: SUMMARY FEDERAL RULES OF EVIDENCE 901 AND 902 RULES FOR AUTHENTICATION

Type of e-Evidence: Email	
FRE Rules	**Methods**
Rule 901(b)(1): Testimony of a witness with knowledge that the document is what it purports to be. **Rule 901(b)(4):** Appearance, content. **Rule 901(b)(9):** System or process capable of proving a reliable and dependable result [902(13,14)]. **Rule 902(7):** Trade inscriptions. **Rule 902(11):** Self authenticating.	Witness testifies on process of creation, acquisition, preservation etc.: i. who sent: author, ii. who received, iii. someone who saw it being authored/received, iv. email chain recipient: accuracy of contents. Business records: Rule 803(6) certificate by a qualified witness. Production of document in discovery. Circumstantial evidence: about authorship, content, writing style, etc. Forensic information, hash values, etc.
Cases	
Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 538–39, 547 (D. Md. 2007) (noting that "[h]ash values can be inserted into original electronic documents when they are created to provide them with distinctive characteristics that will permit their authentication under Rule 901(b)(4).").	

<table>
<tr><th colspan="2">Type of e-Evidence: Email</th></tr>
<tr><td colspan="2">*United States v. White*, 660 F. App'x 779, 783 (11th Cir. 2016) (allowing a witness to authenticate an email chain with many emails sent between the defendant and the witness and holding the "anomalies and inconsistencies" in the email insufficient to affect the admissibility of the documents).

United States v. Cone, 714 F.3d 197, 220 (4th Cir. 2013) ("While properly authenticated e-mails may be admitted into evidence under the business records exception, it would be insufficient to survive a hearsay challenge simply to say that since a business keeps and receives e-mails, then *ergo* all those e-mails are business records falling within the ambit of Rule 803(6)(B).").

Broadspring, Inc. v. Congoo, LLC, No. 13-CV-1866 (JMF), 2014 WL 7392905, at * 3 (S.D.N.Y. Dec. 29, 2014) (holding that third-party emails sent to a party in the ordinary course of business and produced by the party in litigation are sufficiently authenticated).

Nola Fine Art, Inc. v. Ducks Unlimited, Inc., 88 F. Supp. 3d 602, 607 (E.D. La. 2015) ("[Defendant] produced the email to plaintiffs in discovery and therefore cannot seriously dispute the email's authenticity.").

United States v. Siddiqui, 235 F.3d 1318, 1322 (11th Cir. 2000) (holding that an email identified as originating from the defendant's email address and that automatically included the defendant's address when the reply function was selected was considered sufficiently authenticated).</td></tr>
<tr><th>FRE Rule</th><th>Method</th></tr>
<tr><td>Rule 901(b)(3): Comparison by trier or expert witness.</td><td>Expert witness may explain either the technology or the method.</td></tr>
<tr><th>FRE Rule</th><th>Method</th></tr>
<tr><td>Rule 901(b)(4): Distinctive characteristics and the like.</td><td>Appearance, content.</td></tr>
</table>

Type of e-Evidence: Text Messages	
FRE Rules	**Methods**
As above.	As above for 901(b)(1). Additionally: • the purported author's ownership of the phone or other device from which the text was sent, • the author's possession of the phone, • the author's known phone number, • the author's name, • the author's name as stored on the recipient's phone, and • the author's customary use of emoji or emoticons.
Cases	
United States v. Teran, 496 F. App'x 287, 292 (4th Cir. 2012) (holding that threatening texts were authenticated where recipient testified to personal nature of messages and texts aligned with defendant's knowledge of recipient's family). *United States v. Kilpatrick*, No. 10-20403, 2012 WL 3236727, at *3–6 (E.D. Mich. Aug. 7, 2012) (holding that texts were authenticated where SkyTel records-custodian verified that the texts had not been and could not be edited in any way because texts were automatically saved on SkyTel's server with no capacity for editing). *United States v. Ramirez*, 658 F. App'x 949, 952 (11th Cir. 2016) (admitting photos that were sent by text because the recipient testified she received them, an agent testified he was present when the	

Type of e-Evidence: Text Messages
texts were sent, and the defendant was listed as the owner of the phone number sending the texts). *United States v. Barnes*, 803 F.3d 209, 217 (5th Cir. 2015) (finding that government laid a proper foundation to authenticate Facebook and text messages as having been sent by the defendant where recipient testified she had seen the defendant use Facebook, she recognized his Facebook account, and the messages matched his manner of communicating; and further stating "[a]lthough she was not certain that [the defendant] authored the messages, conclusive proof of authenticity is not required for admission of disputed evidence").

Type of e-Evidence: Mobile Devices, Voicemail	
FRE Rules	**Methods**
Rule 901 (b)(1): Testimony of a witness with knowledge that the document is what it purports to be.	A witness who overheard the person leaving the message and can say the message being offered into evidence is the same message, or use chain of custody.
Cases	
Furlev Sales & Assocs., Inc. v. N. Am. Auto. Warehouse, Inc., 325 N.W.2d 20, 27 n.9 (Minn. 1982) (noting seven foundational elements for admission of a tape recording that have the potential to apply to ESI). *State v. Williams,* 150 P.3d 111, 118 n.7 (Wash. Ct. App. 2007) ("[i]dentification of a voice [whether firsthand or through mechanical or electronic transmission or recording] by opinion based upon hearing the voice at any time under circumstances connecting it with the alleged speaker") (quoting Wash. R. Evid. 901(b)(5)).	

Type of e-Evidence: Internet Websites/Web pages	
FRE Rules	**Methods**
Rule 901(b)(1): Testimony of a witness with knowledge. **Rules 902 (5), (7) and (11):** Public authorities' websites: self-authenticating official publication.	Follow Rules 104(a) and (b): i. What was actually on the website? ii. Does the exhibit or testimony accurately reflect it? iii. If so, is it attributable to the owner of the site? Consider the totality of the circumstances, e.g.: • "The length of time the data was posted on the site; • Whether others report having seen it; • Whether it remains on the website for the court to verify; • Whether the data is of a type ordinarily posted on that website or websites of similar entities (e.g., financial information from corporations); • Whether the owner of the site has elsewhere published the same data, in whole or in part;

Type of e-Evidence: Internet Websites/Web pages	
	• Whether others have published the same data, in whole or in part; • Whether the data has been republished by others who identify the source of the data as the website in question."[258]
Cases	
U.S. Equal Emp't Opportunity Comm'n v. E.I. DuPont de Nemours & Co., No. Civ. A. 03-1605, 2004 WL 2347559, at *1–2 (E.D. La. Oct. 18, 2004) (denying motion to exclude government website printout where date and domain were shown). *Telewizja Polska USA, Inc. v. Echostar Satellite Corp*, No. 02 C 3293, 2004 WL 2367740, at 6* (N.D. Ill. Oct. 15, 2004) (finding that Wayback Machine copies of website, verified by affidavit, met Rule 901's threshold requirements). *People v. Beckley*, 110 Cal. Rptr. 3d 362, 366–67 (Cal. Ct. App. 2010) (holding that prosecution failed to authenticate photograph downloaded from an internet website where "no expert testified that the picture was not a 'composite' or 'faked' photograph," and noting that "digital photographs can be changed to produce false images"). *United States v. Hassan*, 742 F.3d 104, 133 (4th Cir. 2014) (holding that Facebook posts, including YouTube videos, were self-authenticating under Rule 902(11) where accompanied by certificates from Facebook and Google custodians "verifying that the Facebook pages and YouTube videos had been maintained as business	

258 Gregory P. Joseph, *Internet and Email Evidence (Part 1)*, THE PRACTICAL LAWYER 19, 21 (Feb. 2012); *see also* Hon. Alan Pendleton, *Admissibility of Electronic Evidence: A New Evidentiary Frontier,* BENCH & B. MINN. 14, 15 (Oct. 2014).

<table>
<tr><th colspan="2">Type of e-Evidence: Internet Websites/Web pages</th></tr>
<tr><td colspan="2">records in the course of regularly conducted business activities. According to those certifications, Facebook and Google create and retain such pages and videos when (or soon after) their users post them through use of the Facebook or Google servers.”).

United States v. Jackson, 208 F.3d 633, 638 (7th Cir. 2000) (holding website postings were not properly authenticated because the proponent needed to show that the website postings were actually posted by a particular group and not the proponent herself).</td></tr>
<tr><th>FRE Rule</th><th>Method</th></tr>
<tr><td>Rule 901(b)(3): Comparison by trier or expert witness.</td><td>As above for 901(b)(3).

Archived internet content could be obtained through the Internet Archive’s Wayback Machine.</td></tr>
<tr><th colspan="2">Cases</th></tr>
<tr><td colspan="2">*St. Luke’s Cataract & Laser Inst., P.A. v. Sanderson*, No. 8:06-cv-223-T-MSS, 2006 WL 1320242, at *2 (M.D. Fla. May 12, 2006).

United States v. Gasperini, No. 17-2479-cr, 2018 WL 3213005, at *5 (2d Cir. 2018).

United States v. Bansal, 663 F.3d 634, 667–68 (3rd Cir. 2011).

Novak v. Tucows, Inc., No. 06-CV-1909(JFB)(ARL), 2007 WL 922306, at *5 (E.D.N.Y. Mar. 26, 2007) (holding that information about Wayback Machine was not properly authenticated pursuant to Fed. R. Evid. 901 because the plaintiff proffered neither testimony nor sworn statements attesting to the authenticity of the contested web-page exhibits by an employee of the companies hosting the sites from which the plaintiff printed the pages).</td></tr>
<tr><th>FRE Rule</th><th>Method</th></tr>
<tr><td>Rule 901(b)(4): Distinctive characteristics and the like.</td><td>As above for 901(b)(4).</td></tr>
</table>

Type of e-Evidence: Internet Websites/Web pages	
Cases	
Premier Nutrition, Inc. v. Organic Food Bar, Inc., No. SACV 06-0827 AG (RNBx), 2008 WL. 1913163, at *6 (C.D. Cal. Mar. 27, 2008) (noting that "[c]ourts consider the distinctive characteristics of a website in making a finding of authenticity," i.e., printouts of web pages with web addresses and dates).	
FRE Rule	**Method**
Rule 901(b)(7): Public records or reports.	Proof of custody needed; proof of reliability of system not needed.
Cases	
Williams v. Long, 585 F. Supp. 2d 679, 686–88, & n.4 (D. Md. 2008) (collecting cases indicating that postings on government websites are self-authenticating).	
FRE Rule	**Method**
Rule 901(b)(9): Process or system.	Proof that the process or system is trustworthy.

Type of e-Evidence: Chat Room, Blogs, and Other Social Media	
FRE Rules	**Methods**
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 902(b)(9):** System or process.	As above for 901(b)(1). As above for 901(b)(4). Showing that a posting appears on a particular user's webpage is insufficient to authenticate as written by account holder. Evidence: • testimony from a witness who identifies the social

Type of e-Evidence: Chat Room, Blogs, and Other Social Media	
Rule 902(5), (6): Official publications, newspapers etc. **Rule 902(13):** Certified records generated by an electronic process. **Rule 902(14):** Certified data copied from an electronic device, storage medium.	media account as that of the alleged author, on the basis that the witness on other occasions communicated with the account holder, • testimony from a participant in the conversation based on firsthand knowledge that the transcript fairly and accurately captures the conversation, • evidence from the hard drive of the purported author's computer reflecting that a user of the computer used the screen name in question, or • evidence that the chat appears on the computer or other device of the account owner and purported author. Social media as business records: • time stamps, metadata, etc. maintained by the owner, • testimony from the purported creator of the social network profile and related postings,

Type of e-Evidence: Chat Room, Blogs, and Other Social Media	
	• testimony from persons who saw the purported creator establish or post to the page, or • references or links to, or contact information about, loved ones, relatives, co-workers, others close to the purported author.
Cases	
Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 538–39 (D. Md. 2007). *Griffin v. State*, 19 A.3d 415, 427–28 (Md. 2011) (citing three methods of authentication) i. "[A]sk the purported creator if she indeed created the profile and also if she added the posting in question." ii. Search the computer of the alleged person and "examine the computer's internet history and hard drive to determine whether that computer was used to originate the social networking profile and posting in question." iii. "[O]btain information directly from the social networking website that links the establishment of the profile to the person who allegedly created it and also links the posting sought to be introduced to the person who initiated it." *State v. Eleck*, 23 A.3d 818, 821–25 (Conn. App. Ct. 2011) (affirming exclusion of printouts of Facebook messages for lack of authentication where defendant did not provide enough circumstantial evidence to prove who sent the Facebook messages). *United States v. Browne*, 834 F.3d 403, 410–14 (3d Cir. 2016), cert. denied, 137 S. Ct. 695 (2017) (holding that Facebook chats were sufficiently authenticated because witnesses testified they	

Type of e-Evidence: Chat Room, Blogs, and Other Social Media
communicated with the creator of the page through Facebook, they could identify the alleged creator of the page in court, and the available biographical data on Facebook matched the defendant). *United States v. Encarnacion-LaFontaine*, 639 F. App'x 710, 713 (2d Cir. 2016) (finding that threatening Facebook posts were properly authenticated where "the Government introduced evidence that (1) the Facebook accounts used to send the messages were accessed from IP addresses connected to computers near Encarnacion's apartment; (2) patterns of access to the accounts show that they were controlled by the same person; (3) in addition to the Goris threats, the accounts were used to send messages to other individuals connected to Encarnacion; (4) Encarnacion had a motive to make the threats[;] and (5) a limited number of people, including Encarnacion, had information that was contained in the messages.").

Type of e-Evidence: Computerized Records or Data	
FRE Rule	**Methods**
Rule 901(b)(1): Testimony of a witness with knowledge.	As above for 901(b)(1).
FRE Rule	**Methods**
Rule 901(b)(4): Distinctive characteristics and the like.	As above for 901(b)(4).
FRE Rule	**Method**
Rule 901(b)(9): Process or system.	As above for 901(b)(9).
Cases	
Liser v. Smith, 254 F. Supp. 2d 89, 94, 97–98 (D.D.C. 2003) (discussing significance of time lag between actual time and time indicated on surveillance tape in deciding summary judgment in false arrest case).	

<table>
<tr><th colspan="2">Type of e-Evidence: Computerized Records or Data</th></tr>
<tr><td colspan="2">State v, Chun, 943 A.2d 114, 120–21 (N.J. 2008) (concluding, after extensive testing for scientific validity, that new breathalyzer, Alcotest using New Jersey Firmware version 3.11, is "generally scientifically reliable" but ordering modifications to enable it to be admitted into evidence because results of third test indicated inherent errors).</td></tr>
<tr><th>FRE Rule</th><th>Method</th></tr>
<tr><td>Rule 902(13): Certification of records.</td><td>Affidavit by deponent:
i. with specialized or technical knowledge on how the system or process works. ESI was obtained from systems that produced reliable results.
ii. detailed description of what was done.
Notice under Rule 902(11).</td></tr>
<tr><th colspan="2">Cases</th></tr>
<tr><td colspan="2">Lamb v. State, 246 So. 3d 400, 408–09 (Fla. Dist. Ct. App. 2018) (upholding trial court's ruling that the Facebook Live video was properly authenticated and admissible to the jury). Authentication problem in the manner in which the prosecutor attempted to authenticate the Facebook Live video. FRE 902 (13) and (14) all provide parameters in which practitioners can easily present electronically stored information (ESI) as self-authenticating.</td></tr>
<tr><th>FRE Rule</th><th>Method</th></tr>
<tr><td>Rule 902(14): Certification of data copied or stored (e.g., metadata).</td><td>As above for 902(14).
By comparing the "hash value" of the proffered copy to that of the original document.
Notice under Rule 902(11).</td></tr>
</table>

<table>
<tr><th colspan="2">Type of e-Evidence: Audios and Videos</th></tr>
<tr><th>FRE Rule</th><th>Methods</th></tr>
<tr><td>Rule 901(b)(1): Testimony of a witness with knowledge</td><td>Testifies to personal observation of events

Forensic expert</td></tr>
<tr><th colspan="2">Cases</th></tr>
<tr><td colspan="2">United States v. Broomfield, 591 F. App'x 847, 848–49, 851–52 (11th Cir. 2014) (upholding trial court's admission, in possession of firearm case, of YouTube video showing defendant discharging an AR-15 rifle in front of Fowler Firearms where Fowler manager testified that: (i) defendant was a Fowler Firearms member; (ii) defendant purchased two boxes of PMC .223 ammunition at the time in question; (iii) he had not purchased the ammunition at any other time; and (iv) the only firearm Fowler rented that used PMC .223 ammunition was the AR-15).</td></tr>
<tr><th>FRE Rule</th><th>Method</th></tr>
<tr><td>Rule 901(b)(9): Process or system.

Digitally altered audios and videos.</td><td>Proof that the process or system is trustworthy. Integrity of the recording speaks for itself:
fidelity of equipment;
absence of modifications;
handling and storing procedure;
establishing the authenticity and correctness of the resulting recording;
time and date;
operating, testing and security procedures, chain of custody.</td></tr>
</table>

Type of e-Evidence: Audios and Videos	
	• Metadata should include time, date, geolocation, and device IDs of other devices in close proximity.
Cases	
U.S. v. Chapman, 804 F.3d 895, 902 (7th Cir. 2015). *People v. Jackson*, 994 N.Y.S.2d 438, 440–41 (N.Y. App. Div. 2014). Julia Day, *Reuters Drops Photographer over 'Doctored' Image*, THE GUARDIAN (Aug. 7, 2006 7:05 AM), https://www.theguardian.com/media/2006/aug/07/reuters.pressandpublishing. *Tillerson in Afghanistan: Photo of meeting apparently doctored,* BBC NEWS (Oct. 24, 2017), https://www.bbc.com/news/world-asia-41734559 (clock cropped out to conceal the true location of the meeting).	
FRE Rule	**Method**
Rule 902(13): Certification of records.	As above for 902(13).

Type of e-Evidence: Computer Simulations and Computer Animations	
FRE Rule	**Methods**
Rule 901(b)(1): Testimony of a witness with knowledge.	As above for 901(b)(1).
FRE Rule	**Methods**
Rule 901(b)(3): Comparison by trier or expert witness.	As above for 901(b)(3).
FRE Rule	**Method**
Rule 901(b)(9): Process or system.	As above for 901(b)(9).

Type of e-Evidence: Digital Photographs	
FRE Rules	**Methods**
Rule 901(b)(9): Process or system. **Rule 902(13):** Certification of records.	As above for 901(b)(9) and 902(13) Certification by a technician, metadata, GPS co-ordinates, camera log
Cases	
Rodd v. Raritan Radiologic Assocs., P.A., 860 A.2d 1003 (N.J. Super. Ct. App. Div. 2004) (computerized images of mammograms).	

Type of e-Evidence: Cloud	
FRE Rules	**Methods**
Rule 901(b)(1): Testimony of a witness with knowledge. **Rule 901 (b)(9):** Process or system.	Witness to testify on contractual service level agreements with cloud service providers that specify: i. data ownership, ii. confidentiality and non-disclosure requirements, iii. notification about third-party requests for access, iv. trusted third-party security audit or verification procedures, and v. intrinsic data protective controls directly given by the data holder before uploading to the cloud.

Type of e-Evidence: Cloud	
	Authenticate: i. proof of its origin by identifying its creator or authorized signatory; ii. content integrity, i.e., that the document has not been altered since its creation; iii. time of its creation and attestation, including proof of the implementation of effective safeguards by a reliable or trustworthy source to ensure its integrity; and iv. recordkeeping system, allocation of operational control and responsibility, and access control. Forensics can detect traces of the use of a cloud computing service stored in PCs and smartphones. (For example, Dropbox can be found in the Windows system. These traces can be located in the installation directory, registry changes on installation, network activity, database files, internet log files, and uninstallation data.)[259]
Cases	
Rearden LLC v. Rearden Commerce, Inc., 597 F. Supp. 2d 1006 (N.D. Cal. Jan. 27, 2009, *vacated*, 683 F.3d 1190 (9th Cir. 2012) (granting	

Type of e-Evidence: Cloud
summary judgment (later vacated and remanded) involving claims of trademark infringement of personal-assistant device between parties involved in cloud computing). *International Business Machines Corp. v. Johnson*, No. 09 Civ. 4826(SCR), 2009 WL 2356430 (S.D.N.Y. July 30, 2009) (noting, in noncompetition agreement case, requirement that vice president of corporate development advise on "enterprise services, servers, storage, so-called 'Cloud' computing and business analytics"). *State v. Bellar*, 217 P.3d 1094, 1110–11 & n.10–11 (Or. Ct. App. 2009) (discussing defendant's privacy rights relating to data stored in the cloud).

Type of e-Evidence: USB Device and Other Removable Storage Devices	
FRE Rule	**Methods**
Rule 902(13): Certification from a forensic technician.	As above for 902(13).

Type of e-Evidence: IoT	
FRE Rule	**Methods**
Rule 901(b)(1): Testimony of a witness with knowledge. **Rule 901(b)(9):** Process or system.	Expert witness: forensic analysis i. explain scope and nature of data collection and analysis; ii. security features; iii. devices: function, process, system; and

259. *See* Frank McClain, *Dropbox Forensics*, FORENSIC FOCUS (May 31, 2011), https://www.forensicfocus.com/articles/dropbox-forensics/.

Type of e-Evidence: IoT	
	iv. data stored in the cloud, as for cloud above.

APPENDIX B: COMMITTEE NOTE ON RULE 807[260]

Rule 807 has been amended to fix a number of problems that the courts have encountered in applying it.

Courts have had difficulty with the requirement that the proffered hearsay carry "equivalent" circumstantial guarantees of trustworthiness. The "equivalence" standard is difficult to apply, given the different types of guarantees of reliability, of varying strength, found among the categorical exceptions (as well as the fact that some hearsay exceptions, e.g., Rule 804(b)(6), are not based on reliability at all). The "equivalence" standard has not served to guide a court's discretion to admit hearsay, because the court is free to choose among a spectrum of exceptions for comparison. Moreover, experience has shown that some statements offered as residual hearsay cannot be compared usefully to any of the categorical exceptions and yet might well be trustworthy. Thus the requirement of an equivalence analysis has been eliminated. Under the amendment, the court should proceed directly to a determination of whether the hearsay is supported by guarantees of trustworthiness. See Rule 104(a). As with any hearsay statement offered under an exception, the court's threshold finding that admissibility requirements are met merely means that the jury may consider the statement and not that it must assume the statement to be true.

The amendment specifically requires the court to consider corroborating evidence in the trustworthiness enquiry. Most courts have required the consideration of corroborating evidence, though some courts have disagreed. The rule now provides for a uniform approach, and recognizes that the existence or absence of corroboration is relevant to, but not dispositive of,

260. COMM. ON RULES OF PRACTICE AND PROCEDURE, JUDICIAL CONFERENCE OF THE U.S., AGENDA BOOK 410–14 (June 12, 2018), http://www.uscourts.gov/sites/default/files/2018-06_standing_agenda_book_final.pdf.

whether a statement should be admissible under this exception. Of course, the court must consider not only the existence of corroborating evidence but also the strength and quality of that evidence.

The amendment does not alter the case law prohibiting parties from proceeding directly to the residual exception, without considering admissibility of the hearsay under Rules 803 and 804. A court is not required to make a finding that no other hearsay exception is applicable. But the opponent cannot seek admission under Rule 807 if it is apparent that the hearsay could be admitted under another exception.

The rule in its current form applies to hearsay "not specifically covered" by a Rule 803 or 804 exception. The amendment makes the rule applicable to hearsay "not admissible under" those exceptions. This clarifies that a court assessing guarantees of trustworthiness may consider whether the statement is a "near-miss" of one of the Rule 803 or 804 exceptions. If the court employs a "near-miss" analysis it should—in addition to evaluating all relevant guarantees of trustworthiness—take into account the reasons that the hearsay misses the admissibility requirements of the standard exception.

In deciding whether the statement is supported by sufficient guarantees of trustworthiness, the court should not consider the credibility of any witness who relates the declarant's hearsay statement in court. The credibility of an in-court witness does not present a hearsay question. To base admission or exclusion of a hearsay statement on the witness's credibility would usurp the jury's role of determining the credibility of testifying witnesses. The rule provides that the focus for trustworthiness is on circumstantial guarantees surrounding the making of the statement itself, as well as any independent evidence corroborating the statement. The credibility of the witness relating the statement is not a part of either enquiry.

Of course, even if the court finds sufficient guarantees of trustworthiness, the independent requirements of the Confrontation Clause must be satisfied if the hearsay statement is offered against a defendant in a criminal case.

The Committee decided to retain the requirement that the proponent must show that the hearsay statement is more probative than any other evidence that the proponent can reasonably obtain. This necessity requirement will continue to serve to prevent the residual exception from being used as a device to erode the categorical exceptions.

The requirements that residual hearsay must be evidence of a material fact and that its admission will best serve the purposes of these rules and the interests of justice have been deleted. These requirements have proved to be superfluous in that they are already found in other rules. See Rules 102, 401.

The notice provision has been amended to make four changes in the operation of the rule:

- First, the amendment requires the proponent to disclose the "substance" of the statement. This term is intended to require a description that is sufficiently specific under the circumstances to allow the opponent a fair opportunity to meet the evidence. See Rule 103(a)(2) (requiring the party making an offer of proof to inform the court of the "substance" of the evidence).
- Second, the prior requirement that the declarant's address must be disclosed has been deleted. That requirement was nonsensical when the declarant was unavailable, and unnecessary in the many cases in which the declarant's address was known or easily obtainable. If prior disclosure of the declarant's address is critical and cannot be obtained by the opponent

through other means, then the opponent can seek relief from the court.

- Third, the amendment requires that the pretrial notice be in writing—which is satisfied by notice in electronic form. See Rule 101(b)(6). Requiring the notice to be in writing provides certainty and reduces arguments about whether notice was actually provided.
- Finally, the pretrial notice provision has been amended to provide for a good cause exception. Most courts have applied a good cause exception under Rule 807 even though the rule in its current form does not provide for it, while some courts have read the rule as it was written. Experience under the residual exception has shown that a good cause exception is necessary in certain limited situations. For example, the proponent may not become aware of the existence of the hearsay statement until after the trial begins; or the proponent may plan to call a witness who without warning becomes unavailable during trial, and the proponent might then need to resort to residual hearsay.

The rule retains the requirement that the opponent receive notice in a way that provides a fair opportunity to meet the evidence. When notice is provided during trial after a finding of good cause, the court may need to consider protective measures, such as a continuance, to assure that the opponent is not prejudiced.

APPENDIX C: 12 V.S.A. § 1913. BLOCKCHAIN ENABLING

(a) As used in this section:

(1) "blockchain" means a cryptographically secured, chronological, and decentralized consensus ledger or consensus database maintained via Internet, peer-to-peer network, or other interaction.

(2) "Blockchain technology" means computer software or hardware or collections of computer software or hardware, or both, that utilize or enable a blockchain.

(b) Authentication, admissibility, and presumptions.

(1) A digital record electronically registered in a blockchain shall be self-authenticating pursuant to Vermont Rule of Evidence 902, if it is accompanied by a written declaration of a qualified person, made under oath, stating the qualification of the person to make the certification and:

(A) the date and time the record entered the blockchain;

(B) the date and time the record was received from the blockchain;

(C) that the record was maintained in the blockchain as a regular conducted activity; and

(D) that the record was made by the regularly conducted activity as a regular practice.

(2) A digital record electronically registered in a blockchain, if accompanied by a declaration that meets the requirements of subdivision (1) of this subsection, shall be considered a record of regularly conducted business activity pursuant to

Vermont Rule of Evidence 803(6) unless the source of information or the method or circumstance of preparation indicate lack of trustworthiness. For purposes of this subdivision (2), a record includes information or data.

(3) The following presumptions apply:

(A) A fact or record verified through a valid application of blockchain technology is authentic.

(B) The date and time of the recordation of the fact or record established through such a blockchain is the date and time that the fact or record was added to the blockchain.

(C) The person established through such a blockchain as the person who made such recordation is the person who made the recordation.

(D) If the parties before a court or other tribunal have agreed to a particular format or means of verification of a blockchain record, a certified presentation of a blockchain record consistent with this section to the court or other tribunal in the particular format or means agreed to by the parties demonstrates the contents of the record.

(4) A presumption does not extend to the truthfulness, validity, or legal status of the contents of the fact or record.

(5) A person against whom the fact operates has the burden of producing evidence sufficient to support a finding that the presumed fact, record,

time, or identity is not authentic as set forth on the date added to the blockchain, but the presumption does not shift to a person the burden of persuading the trier of fact that the underlying fact or record is itself accurate in what it purports to represent.

(c) Without limitation, the presumption established in this section shall apply to a fact or record maintained by blockchain technology to determine:

(1) contractual parties, provisions, execution, effective dates, and status;

(2) the ownership, assignment, negotiation, and transfer of money, property, contracts, instruments, and other legal rights and duties;

(3) identity, participation, and status in the formation, management, record keeping, and governance of any person;

(4) identity, participation, and status for interactions in private transactions and with a government or governmental subdivision, agency, or instrumentality;

(5) the authenticity or integrity of a record, whether publicly or privately relevant; and

(6) the authenticity or integrity of records of communication.

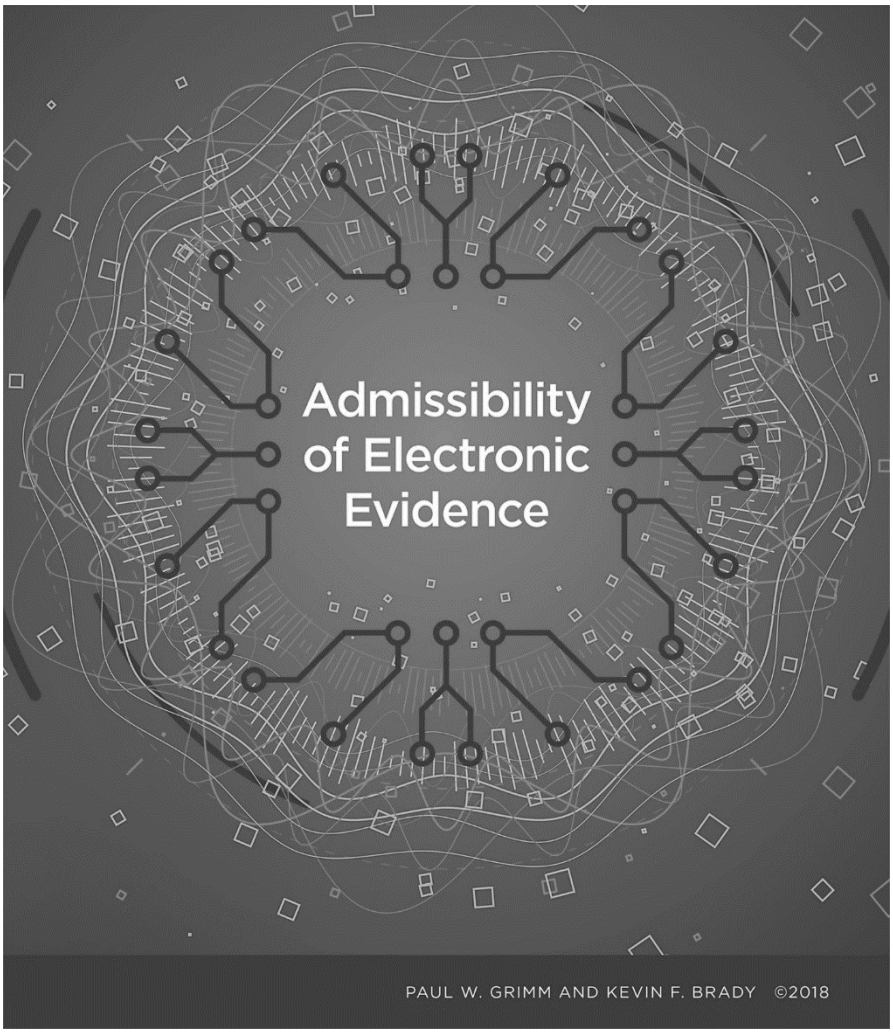
(d) The provisions of this section shall not create or negate:

(1) an obligation or duty for any person to adopt or otherwise implement blockchain technology for any purpose authorized in this section; or

> (2) the legality or authorization for any particular underlying activity whose practices or data are verified through the application of blockchain technology. (Added 2015, No. 157 (Adj. Sess.), § I.1.)[261]

261. *Id*.

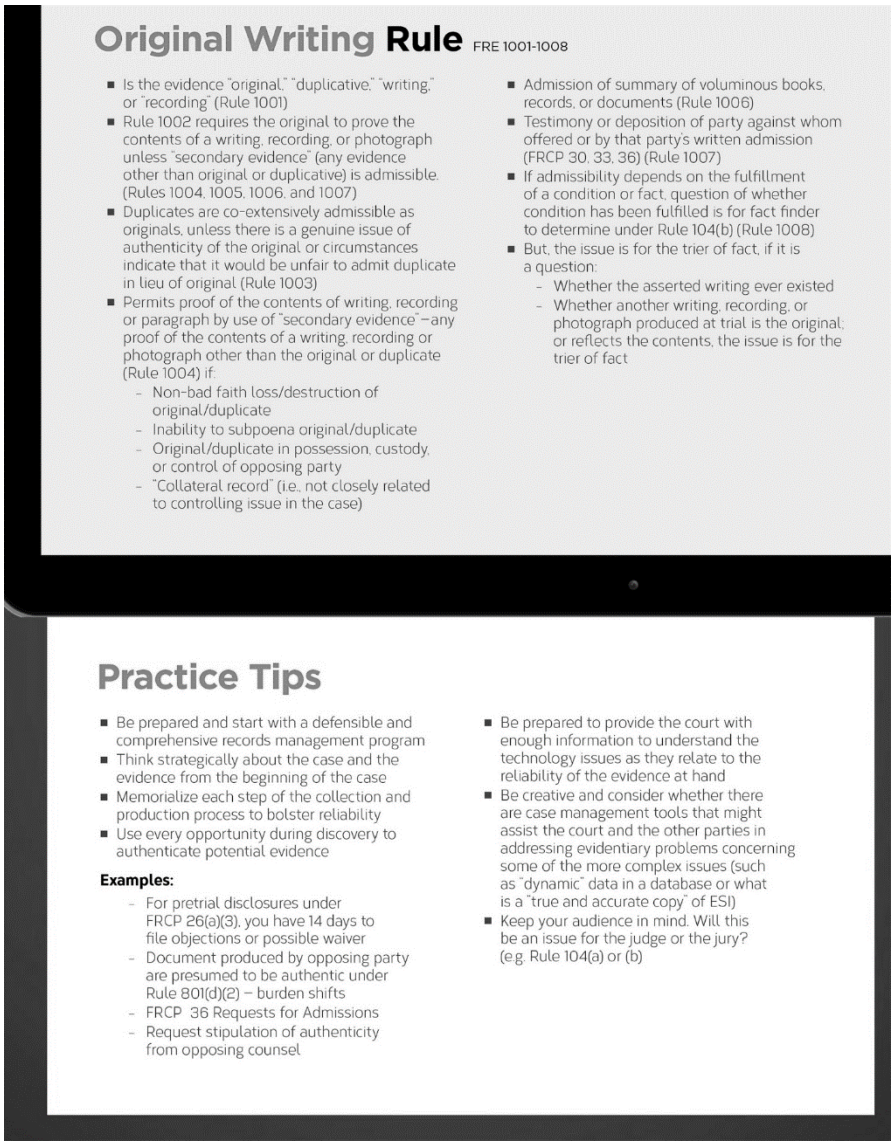
APPENDIX D: CHECKLIST OF POTENTIAL AUTHENTICATION METHODS[262]



262. Full-size PDF available at https://thesedonaconference.org/sites/default/files/Grimm_Brady_Evidence_Admissibility_Chart_2018.pdf.


Potential Authentication Methods
Email, Text Messages, and Instant Messages
Witness with personal knowledge (901(b)(1))
Expert testimony or comparison with authenticated examples (901(b)(3))
Distinctive characteristics including circumstantial evidence (901(b)(4))
System or process capable of proving a reliable and dependable result (901(b)(9))
Trade inscriptions (902(7))
Certified copies of business record (902(11))
Certified records generated by an electronic process or system (902(13))
Certified data copied from an electronic device, storage medium, or file (902(14))
Chat Room Postings, Blogs, Wikis, and Other Social Media Conversations
Witness with personal knowledge (901(b)(1))
Expert testimony or comparison with authenticated examples (901(b)(3))
Distinctive characteristics including circumstantial evidence (901(b)(4))
System or process capable of proving a reliable and dependable result (901(b)(9))
Official publications (902(5))
Newspapers and periodicals (902(6))
Certified records generated by an electronic process or system (902(13))
Certified data copied from an electronic device, storage medium, or file (902(14))
Digitally Stored Data and Internet of Things
Witness with personal knowledge (901(b)(1))
Expert testimony or comparison with authenticated examples (901(b)(3))
Distinctive characteristics including circumstantial evidence (901(b)(4))
System or process capable of proving a reliable and dependable result (901(b)(9))
Certified records generated by an electronic process or system (902(13))
Certified data copied from an electronic device, storage medium, or file (902(14))
VR
Computer Processes, Animations, Virtual Reality, and Simulations
Witness with personal knowledge (901(b)(1))
Expert testimony or comparison with authenticated examples (901(b)(3))
System or process capable of proving a reliable and dependable result (901(b)(9))
Certified records generated by an electronic process or system (902(13))
Digital Photographs
Witness with personal knowledge (901(b)(1))
System or process capable of providing reliable and dependable result (901(b)(9))
Official publications (902(5))
Certified records generated by an electronic process or system (902(13))
Certified data copied from an electronic device, storage medium, or file (902(14))
Social Media Sites (Facebook, LinkedIn, Twitter, Instagram, and Snapchat)
Witness with personal knowledge (901(b)(1))
Expert testimony or comparison with authenticated examples (901(b)(3))
Distinctive characteristics including circumstantial evidence (901(b)(4))
Public records (901(b)(7))
System or process capable of proving a reliable and dependable result (901(b)(9))
Official publications (902(5))
Certified records generated by an electronic process or system (902(13))
Certified data copied from an electronic device, storage medium, or file (902(14))
Know Which Approach Your Jurisdiction Follows
Maryland Approach to Rules 104 and 901:
A higher standard for authentication for social media evidence. In this approach, the burden is on the admitting party to show that the social media evidence was not falsified or created by another user through either:
Testimony of the creator of the website page or the post
Search of the internet history or hard drive of the purported creator's computer
Information obtained directly from social media site
See, Griffin v. State, 19 A. 3d 415, 423 (Md. 2011).
Texas Approach to Rules 104 and 901:
A lower standard for authentication of social media evidence. In this approach, the burden is on the admitting party to show evidence sufficient to support a finding by a reasonable juror that the social media evidence is what its proponent claims it to be through either:
Direct testimony of a witness with personal knowledge
Expert testimony or comparison with authenticated evidence
Circumstantial evidence
See, Tienda v. State, 358 S. W. 3d 633 (Tex. Crim. App. 2012)


Is Evidence Hearsay?
FRE 801 (a-c)
Is it a statement? (written/ spoken assertion, non-verbal/ non-assertive verbal conduct intended to be assertive.)
Is statement made by "Declarant?" (person, not generated by machine.)
Is statement offered for proving truth of assertion? NOTE: Statement is not offered for substantive truth if offered to prove:
Communicative/ comprehension capacity of declarant
Effect on the hearer
Circumstantial evidence of state of mind of declarant
Verbal acts/parts of acts
Utterances of independent legal significance
Is statement excluded from definition of hearsay by 801(d)(1) and (2)?
Prior witness statements – 801(d)(1)
Prior testimonial statement 801(d)(1)(A)
Prior consistent statement 801(d)(1)(B) to rebut allegations of recent fabrication or rehabilitate a witness that has been impeached
Statement of identification 801(d)(1)(C)
Admission by party opponents – 801(d)(2)*
Individual admission 801(d)(2)(A)
Adoptive admission 801(d)(2)(B)
Admission by person with authority 802(d)(2)(C)
Admission by agent/ employees 802(d)(2)(D)
Co-conspirator statements 801(d)(2)(E)
* Documents produced in discovery by opposing party are presumed to be authentic under 801(d)(2). Certification of business records under 902(11) and (12) must meet requirements of 803(6).
If HEARSAY, then it is INADMISSIBLE unless covered by a recognized exception.
Hearsay Exception
Availability of Declarant Irrelevant – 803
Present sense impression 803(1)
Excited utterance 803(2)
State of mind exception 803(3)
Statements for purposes of medical diagnosis or treatment 803(4)
Past recollection recorded 803(5)
Business records 803(6)
Absence of an entry in records kept in the regular course of business 803(7)
Public records or reports 803(8)
Records of vital statistics 803(9)
Absence of public record or entry 803(10)
Records/ documents affecting interest in property 803(14) & (15)
Statements in ancient documents 803(16)
Market reports and commercial publications 803(17)
Learned treatises 803(18)
Character reputation testimony 803(21)
Record of felony convictions 803(22)
Declarant Unavailable – 804
Unavailability – 804(a)(1-5) (privilege, refused to testify, lack of memory, death/illness, beyond subpoena power)
Unavailability Exceptions – 804(b):
Former Testimony 804(b)(1)
Dying Declaration 804(b)(2)
Statement Against Interest 804(b)(3)
Statement of personal or family history 804(b)(4)
Forfeiture by wrongdoing 804(b)(6)
Residual "Catchall" Exception – 807
A hearsay statement is not excluded by Rule 802 even if the statement is not specifically covered by Rule 803 or 804 under the following circumstances:
Statement has equivalent circumstantial guarantees of trustworthiness
Offered as evidence of a material fact
More probative on the point for which it is offered than any other evidence that the proponent can obtain through reasonable efforts
Admitting it will best serve the purposes of these rules and the interest of justice
The statement is admissible only if, before the trial or hearing, the proponent gives reasonable notice of intent to offer the statement and its particulars, and the opposing party has a fair opportunity to meet it.



Original Writing Rule FRE 1001-1008

- Is the evidence "original," "duplicative," "writing," or "recording" (Rule 1001)
- Rule 1002 requires the original to prove the contents of a writing, recording, or photograph unless "secondary evidence" (any evidence other than original or duplicative) is admissible. (Rules 1004, 1005, 1006, and 1007)
- Duplicates are co-extensively admissible as originals, unless there is a genuine issue of authenticity of the original or circumstances indicate that it would be unfair to admit duplicate in lieu of original (Rule 1003)
- Permits proof of the contents of writing, recording or paragraph by use of "secondary evidence"—any proof of the contents of a writing, recording or photograph other than the original or duplicate (Rule 1004) if:
  - Non-bad faith loss/destruction of original/duplicate
  - Inability to subpoena original/duplicate
  - Original/duplicate in possession, custody, or control of opposing party
  - "Collateral record" (i.e., not closely related to controlling issue in the case)
- Admission of summary of voluminous books, records, or documents (Rule 1006)
- Testimony or deposition of party against whom offered or by that party's written admission (FRCP 30, 33, 36) (Rule 1007)
- If admissibility depends on the fulfillment of a condition or fact, question of whether condition has been fulfilled is for fact finder to determine under Rule 104(b) (Rule 1008)
- But, the issue is for the trier of fact, if it is a question:
  - Whether the asserted writing ever existed
  - Whether another writing, recording, or photograph produced at trial is the original; or reflects the contents, the issue is for the trier of fact

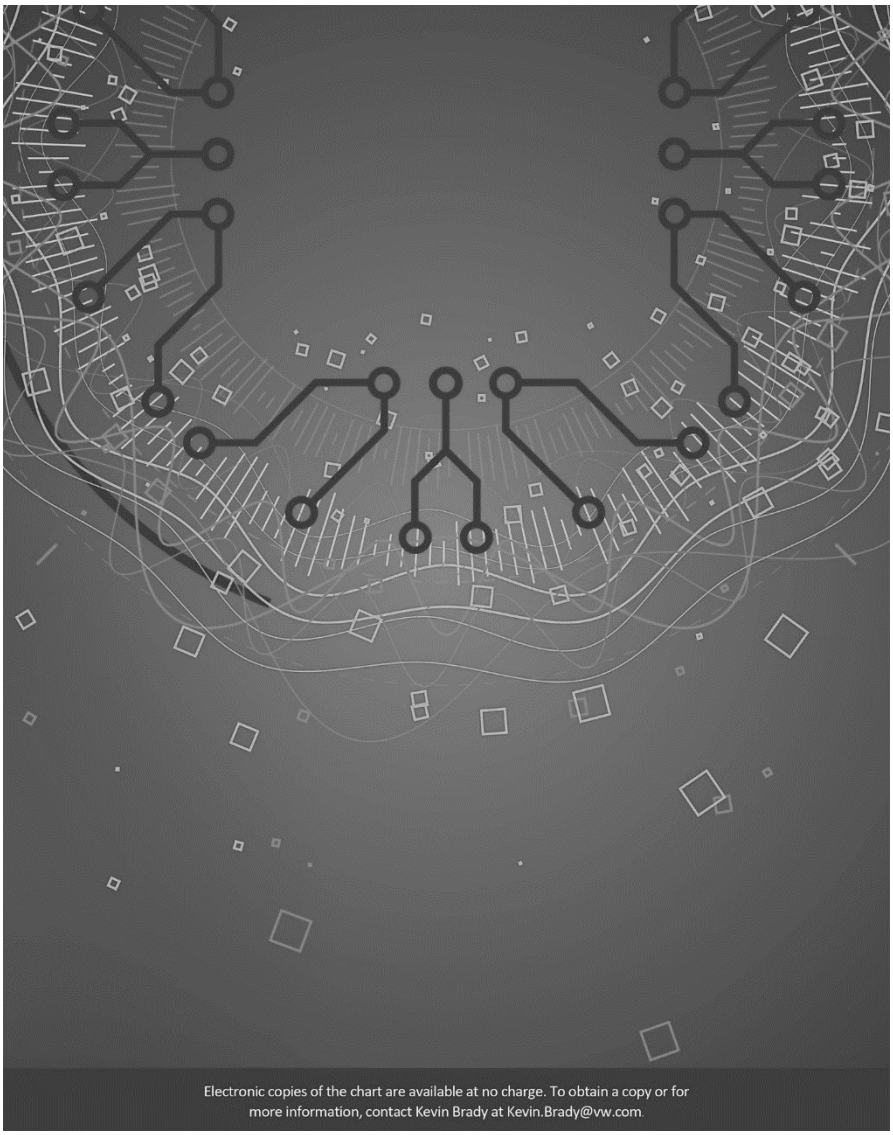
Practice Tips

- Be prepared and start with a defensible and comprehensive records management program
- Think strategically about the case and the evidence from the beginning of the case
- Memorialize each step of the collection and production process to bolster reliability
- Use every opportunity during discovery to authenticate potential evidence

Examples:

- For pretrial disclosures under FRCP 26(a)(3), you have 14 days to file objections or possible waiver
- Document produced by opposing party are presumed to be authentic under Rule 801(d)(2) – burden shifts
- FRCP 36 Requests for Admissions
- Request stipulation of authenticity from opposing counsel

- Be prepared to provide the court with enough information to understand the technology issues as they relate to the reliability of the evidence at hand
- Be creative and consider whether there are case management tools that might assist the court and the other parties in addressing evidentiary problems concerning some of the more complex issues (such as "dynamic" data in a database or what is a "true and accurate copy" of ESI)
- Keep your audience in mind. Will this be an issue for the judge or the jury? (e.g. Rule 104(a) or (b)


Electronic copies of the chart are available at no charge. To obtain a copy or for more information, contact Kevin Brady at Kevin.Brady@vw.com.