Table of Contents

Chapter 1. The Law Concerning Authenticity of Electronic Evidence

This chapter is current through December 2021.

***Federal Rule of Evidence 901(a)*: "To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is."**

1.A. Authenticity Generally

Just because a party has probative evidence does not mean that evidence will be admitted. Pursuant to the Federal Rules of Evidence, in order to admit evidence the proponent must establish that the evidence is authentic, *i.e.*, that it is what it purports to be. This is an important part in the admission process because it ensures that the evidence is genuine.

1.B. The Authenticity Standard

Federal Rule of Evidence 901 governs the authentication of evidence. According to the rule, "[t]o satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is." Traditionally, this could be done, for example, through the testimony of a witness with knowledge, the testimony of an expert, and identification of distinctive characteristics.

1.C. Authentication In The Digital Age

But how does one authenticate new forms of evidence in the digital age? Today, evidence is not limited to written documents or physical objects. Through modern technology, evidence can include things such as geolocation data, social media, and the Internet of Things. Evidence once contained on paper is now more typically solely electronic. Consequently, there are now important considerations attorneys must be prepared to address when seeking to authenticate electronic evidence. By thinking through these considerations ahead of time, attorneys can increase their chances of successfully authenticating electronic evidence.

1.C.1. Source Of The Data

An important consideration for trial attorneys is what is the source of the data they seek to introduce? When determining what the source of data is, attorneys should take the following into consideration:

- Who created the database[1] the evidence is stored in?

- Who created the account where the evidence originated?
- Who created the evidence?
- Is the evidence from a static or dynamic source?[2]
- Who owns the device the evidence is on?

These considerations can be important to determine what types of witnesses or extrinsic evidence may be needed to authenticate electronic evidence.

1.C.2. Access To The Source

Another consideration attorneys should factor in when preparing to authenticate electronic evidence is: who can access the source of the data they seek to introduce? When determining the impact of access to the source of data an attorney seeks to introduce, attorneys should consider the following questions:

- Is the source secure?
- Who has access to password and login information?
- Has the source been hacked[3] or otherwise accessed by someone other than the purported "author" of that data?

As illustrated in later sections, the security of a source of evidence can be critical to whether an attorney can authenticate that evidence. In some cases, a lack of security may be fatal to authentication, even where there is other evidence supporting authentication.

1.C.3. Accuracy Of The Source

Perhaps the most important consideration attorneys should be aware of is the accuracy of the source of the evidence they seek to introduce. Rule 901(b)(9) states that evidence from electronic recordings may be authenticated if accompanied by evidence "describing a process or system used to produce a result and showing that the process or system produces an accurate result." When determining the accuracy of the source of the evidence, attorneys must take the following into account:

1.C.4. Does The Source Record Data Correctly?

One concern with electronic evidence is that often times it is generated without human input (*e.g.*, by a computer or a fitness tracker). Thus, there is concern about the reliability of the processing and output functions of the program that generated or recorded the evidence. This concern is particularly acute because no human witness can confirm the veracity of the evidence.

Courts across jurisdictions agree that a party need only make *"some* showing"[4] of the accuracy of electronic recording methods for authentication. *See also* Section 1.C.4.1 on Geolocation Evidence. But there is no single test applied to confirm the accuracy of electronic evidence under Rule 901. Most jurisdictions use one of two tests—a four-step test or the "silent witness" test—to evaluate whether electronic processes or systems produce accurate results in accordance with Rule 901(b)(9).

1.C.4.1. Geolocation Evidence

1.C.4.1.1. The Four-Step Test

A majority of jurisdictions follow the four-step test to determine whether a party has made a sufficient showing that an electronic recording process or system is accurate. Under this test, witnesses must provide: (1) proof that they have experience with the source; (2) a description of the process or system the source uses; (3) a description of how records are obtained from the source; and (4) an explanation how the recording method has produced accurate results for the particular device or data at issue. Conclusory statements about accuracy are not sufficient to satisfy this test.

For example, in *State v. Brown, 818 S.E.2d 735*, 740 (S.C. 2018), the South Carolina Supreme Court held that GPS records were not authenticated where a probation agent testified that records with respect to probationers were accurate because "we use it in court all the time." There, the state sought to introduce evidence based on a GPS ankle monitor that the defendant was wearing at the time of an alleged robbery. *Id.* at 739. The court noted that although the agent was qualified to lay the foundation for the GPS records, his testimony "provide[ed] no assistance in assessing the accuracy of the GPS records." *Id.* at 740. The court emphasized that, instead, a proponent of such evidence needed to present "[e]vidence describing [the] process or system used to produce the GPS records and show[] that the process or system produces an accurate result." *Id.* at 741 (internal citations omitted).

Conversely, in *State v. Rice, 222 So.3d 32*, 33-34 (La. 2017), the Louisiana Supreme Court found that the defense made a sufficient showing of accuracy for a surveillance video where the witness "explained that he had personally designed and managed the video surveillance system at his home (for security purposes) and knew the video at issue to be what it was asserted to be. He also described the process and system by which the video was created and testified to the accuracy of that system." *Id.*

The Nevada Court of Appeals similarly adopted a more lenient approach with regards to authenticating geolocation evidence in *Scott v. State*. *2020 WL 733972* (Ct. App. Nev. Feb. 11, 2020). In *Scott*, the defendant claimed the district court abused its discretion by admitting screen shots of a cell phone tracking application that generated maps depicting GPS locations of the witness's stolen cell phones. *Id.* at *3. The defendant specifically alleged that the witness did not have the requisite knowledge about GPS data in order to authenticate the exhibits. *Id.* The lower court held that if the witness "uses the cell phone tracking app and he finds it to be accurate and reliable[,] then he can testify about it." *Id.* The Nevada Court of Appeals affirmed, and held that such testimony was sufficient to authenticate the evidence. *Id.* Thus, testimony from an individual who has personal experience using the system that produces GPS records and who can attest to its accuracy and reliability, may be sufficient to establish authenticity.

> Furthermore, in *United States v. Lizarraga-Tirado*, the Ninth Circuit held that had defendant raised an authentication objection to a Google Earth satellite image that included automatically generated coordinates, the proponent of the Google-Earth generated evidence would have needed to establish the evidence's reliability and accuracy. 789 F.3d 1107, 1110 (9th Cir. 2015). The court ruled that this could be demonstrated through "testimony from a Google Earth programmer or a witness who frequently works with and relies on the program," for example. *Id.*
>
> Thus, to demonstrate the authenticity of GPS records, a party typically needs to produce a witness who has "experience with the electronic monitoring system used" and who could "provide testimony describing the monitoring system, the process of generating or obtaining the records, and how this process has produced accurate results for the particular device or data at issue."[5] Practitioners seeking to admit GPS records must therefore consider presenting testimony describing the electronic process at issue, how it generates and obtains records, and demonstrating that the system produces accurate results.

1.C.4.1.2. The "Silent Witness" Test

Some courts apply a stricter test, known as the "silent witness" test, when authenticating electronically recorded photographs or videos.[6] The "silent witness" test applies in situations where it is impossible for a percipient witness to confirm that the

evidence fairly and accurately depicts a scene or object. *See, e.g., Washington v. State, 961 A.2d 1110*, 1115-16 (Md. 2008) (surveillance cameras); *McFall,* 71 N.E.3d at 388 (cell phone videos and photos). The test is founded on the presumption that the evidence "speaks for itself," but courts still must confirm that the recording process produces an accurate result. Under this test, a witness essentially[7] must: (1) confirm the accuracy of the process producing or reproducing the electronic evidence, (2) show that the electronic evidence was not altered in any significant respect, and (3), if relevant, establish the date that the electronic evidence was created. *See, e.g., id.; McFall,* 71 N.E.3d at 388.

Courts consider a range of factors in determining whether a witness has demonstrated that the recording process is accurate, including the type of equipment used, its general reliability, the quality of the recorded product, the process by which the image was focused, and the general reliability of the entire system.

For example, in *Washington v. State*, the court found that the state had failed to establish the accuracy of reproduced surveillance videos because "the videotape recording, made from eight surveillance cameras, was created by some unknown person, who through some unknown process, compiled images from the various cameras to a CD, and then to a videotape." 961 A.2d at 1117. "There was no testimony as to the process used, the manner of operation of the cameras, the reliability or authenticity of the images, or the chain of custody of the pictures." *Id.*

Conversely, in *United States v. Taylor,* 530 F.2d 639, 641-42 (5th Cir. 1976), the Fifth Circuit found that the state had made a sufficient showing of the accuracy of analog surveillance video from a bank robbery where government witnesses "testified as to the manner in which the film was installed in the camera, how the camera was activated, the fact that the film was removed immediately after the robbery, the chain of its possession, and the fact that it was properly developed and contact prints made from it." *Id.*

1.C.4.2. Has The Data Been Altered?

Courts acknowledge that digital evidence is susceptible to alteration in several ways that pose a risk to its authenticity. Because of this, it is important for the proponent to demonstrate that the evidence in question was not altered after it was recorded. Courts rely both on traditional tools for confirming authentication (*i.e.*, certification and testimony) and on digital characteristics, metadata, and other digital forensic analysis to assess whether an alteration has occurred.

"Metadata"[8] from the source of the electronic evidence can be very helpful in showing whether a given data file has been altered. A party may offer testimony about analysis of metadata, for example, from an engaged data forensics expert or an employee of the owner of the data source who is familiar with the system and competent to analyze the date. *See* e.g., Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640, 655 (D. Kan. 2005) (certain electronic evidence could contain "a 'hash mark' . . . that is unique to that particular file. This 'digital fingerprint' akin to a tamper-evident seal . . . would have shown if the electronic spreadsheets were altered. . . ."); *Wi-LAN Inc. v. Sharp Electronics Corp.*, 362 F. Supp. 3d 226, 232 (D. Del. 2019) (evidence not admitted where there were inconsistencies in the metadata concerning when the data was created, but court noted that it might have been able to reach a different decision if the plaintiff had provided the court with "change logs, file comparisons, or other evidence of code revisions that might clear up inconsistencies.") *Chevron Corp. v. Donziger*, 974 F. Supp. 2d 362, 509 (S.D.N.Y. 2014), *aff'd*, 833 F.3d 74 (2d Cir. 2016) (court adjudicated a dispute concerning the true author of a 72-page document. Document's metadata showed that it had been edited for a total of only two minutes before it was last saved. Because it is impossible to write a 72-page document in that time, court was able to conclude that the document was actually created by a different individual). *See Aguilar v. Immigration & Customs Enf't Div. of U.S. Dep't of Homeland Sec.*, 255 F.R.D. 350, 354 (S.D.N.Y. 2008) ("System metadata is relevant . . . if the authenticity of a document is questioned or if establishing 'who received what information when' is important . . . .").

Attorneys should not lose sight of the fact that testimony by a person with knowledge that a piece of evidence is what it is claimed to be also can be effective to establish the authenticity of electronic information. *See United States v. Gagliardi*, 506 F.3d 140, 151 (2d Cir. 2007) (authenticity deemed sufficient where party sought to authenticate certain purported chat room

messages that had been cut and pasted into a Word document through testimony by a person who participated in the "chat" with the defendant to the effect that the document was an accurate record of his conversations with the defendant was enough to authenticate.); *United States v. Tank*, 200 F.3d 627, 630 (9th Cir. 2000) (testimony by a chat room member as to how he created a chat room log and that the log appeared to be an accurate representation of the chatroom's conversations was sufficient to authenticate where the defendant had testified that he used one of the screennames that appeared on the log).

For example, the court in *Novak v. Tucows* declined to authenticate internet archive information pulled from the "Wayback Machine"[9] because of validity concerns, noting that "the authorized owners and managers of the archived websites play no role in ensuring that the material posted in the Wayback Machine accurately reflects what was posted on their official websites at the relevant time." No. 06-CV-1909(JFB)(ARL), 2007 WL 922306, at *5 (E.D.N.Y. March 26, 2007). In light of this, the court found the archive information could not be authenticated without "testimony []or 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" who would have been familiar with the sites' content at the relevant time. *Id.*

Other courts have permitted the admission of archived information from the Wayback Machine when it was authenticated by someone with personal knowledge about the Wayback Machine. *See Specht v. Google Inc.*, 747 F.3d 929 (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."); *United States v. Bansal*, 663 F.3d 634 (3d Cir. 2011) ("To authenticate that the screen-shot was what it purported to be, the government called a witness to testify about how the Wayback Machine website works and how reliable its contents are."); *Open Text S.A. v. Box, Inc.*, No. 13-cv-04910-JD, 2015 U.S. Dist. LEXIS 11312, at *7 (N.D. Cal. Jan. 30, 2015) (refusing to accept a screenshot from the Wayback Machine into evidence without testimony from a representative of the Internet Archive confirming its authenticity).

The Internet Archive, which runs the Wayback Machine, also has a standard affidavit explaining how the Wayback Machine works that it will provide—for a fee—for use in authentication.[10] Such an affidavit has been accepted in place of live testimony to authenticate information pulled from the Wayback Machine. *See Telewizja Polska USA, Inc. v. Echostar Satellite Corp.*, No. 02 C 3293, 2004 WL 2367740, at *6 (N.D. Ill. Oct. 15, 2004) (ruling that affidavit verifying the Internet Archive's retrieval of the archived information was sufficient for authentication).

Attorneys should also consider whether archived information is judicially noticeable and thus does not need to be authenticated under Rule 901. *Compare Erickson v. Neb. Machinery Co.*, 2015 WL 4089849, at *1 n.1 (N.D. Cal. July 6, 2015) ("Courts have taken judicial notice of the contents of web pages available through the Wayback Machine as facts that can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned."), *with My Health v. Gen. Elec. Co.*, 2015 WL 9474293, at *1 (W.D. Wisc. Dec. 28, 2015) ("The weight of authority in this circuit holds that Internet Archive evidence is not amenable to judicial notice.").

1.C.5. When Was The Data Created?

A final consideration in authenticating electronic evidence is when the data was created. Today, metadata can establish when a file was created or identify if it has been altered. This can help pinpoint key events in a timeline. *See Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 547–48 (D. Md. 2007) ("Because metadata shows the date, time and identity of the creator of an electronic record, as well as all changes made to it, metadata is a distinctive characteristic of all electronic evidence that can be used to authenticate it under Rule 901(b)(4).").

When data or evidence was created can also provide circumstantial evidence that supports authenticating the electronic evidence the attorney seeks to admit. To illustrate, circumstantial evidence could correlate whether the creation of the evidence coincides with certain events.

In *United States v. Bloomfield*, 591 F. App'x. 847, 848–49 (11th Cir. 2014), the government offered a YouTube video showing the defendant firing an AR–15 rifle in front of Fowler Firearms. *Id.* at 848. The date that the video was made was critical to establishing the alleged crime. To authenticate the video, a manager at Fowler Firearms testified that the defendant was a member of the gun range and that on January 21, 2011, the defendant purchased, for the only time, two boxes of PMC .223 ammunition. *Id.* at 848-49. The manager further stated that the only firearm Fowler Firearms rented to customers at the time that ammunition was used was the AR–15 rifle. *Id.* at 849. The government also introduced the testimony of an employee who worked at Fowler Firearms for ten years who established that the video showed side deflectors and lights on the gun range, which were installed in late 2010 or early 2011. *Id.* This witness further explained that Fowler Firearms paints its floors and walls at the beginning of each season, and he noted the freshly-painted floor and walls in the video. *Id.* When combined this witness testimony created sufficient circumstantial evidence authenticating the date of the video. *Id.* at 852.

The American College of Trial Lawyers Handbook of Electronic Evidence

---

[1] A database is “a usually large collection of data organized especially for rapid search and retrieval (as by a computer).” *Database*, Merriam-Webster Dictionary, https://www.merriam-webster.com/dictionary/database (last visited June 21, 2021).

[2] A static source is one that has constant or fixed content that cannot be changed by users who access the source. A dynamic source on the other hand is one that displays different content every time it is viewed. For example, a newspaper's website would be an example of a dynamic web page.

[3] To hack means “to gain illegal access to (a computer network, system, etc.).” *Hack*, Merriam-Webster Dictionary, https://www.merriam-webster.com/dictionary/hack (last visited June 21, 2021).

[4] State v. Brown, 818 S.E.2d 735, 741 (S.C. 2018) (emphasis in original).

[5] *Brown*, 818 S.E.2d 735 at 742 (citing *United States v. Washington*, 498 F.3d 225, 231 (4th Cir. 2007)). The court noted that when machines produce information derived from the manipulation of data or mathematical techniques, such as GPS records, then parties must establish the proper foundation for the particular device or data at issue.

[6] The authors have not identified any reported cases in which this test was used to authenticate non-visual electronic evidence.

[7] These factors may vary slightly by jurisdiction.

[8] “Metadata is ‘data about the data.’” *Wiley v. Paulson*, No. 06CV172 (DGT RER), *2007 WL 7059722*, at *1 (E.D.N.Y. Sept. 26, 2007). For example, metadata for emails could potentially reveal “such information as the emails’ complete transmission paths and dates of creation, modification and access.” *Id.*

[9] The Internet Archive's Wayback Machine allows users to view previous versions of websites, including websites that might no longer exist. The previous versions, to the extent available, are time-stamped based on when the Internet Archive's automated systems accessed and recorded the websites. Site owners have the ability to put code on their sites such that the Internet Archive systems will not archive the site. Thus, for that reason and a variety of other reasons such as the fact that some websites’ content is dynamically generated, the Internet Archive's records are not necessarily complete.

[10] Standard Affidavit, Internet Archive, https://archive.org/legal/affidavit.php (last visited June 21, 2021); Information Requests: The Internet Archive's Policy for Responding to Information Requests, Internet Archive, https://archive.org/legal/ (last visited June 21, 2021).
