67 DOJ J. Fed. L. & Prac. 81

Department of Justice Journal of Federal Law and Practice
February, 2019

Michael L. Levy [a1]
Assistant United States Attorney
Eastern District of Pennsylvania

John M. Haried [a2]
Criminal eDiscovery Coordinator
United States Department of Justice

PRACTICAL CONSIDERATIONS WHEN USING NEW EVIDENCE RULE 902(13) TO SELF-AUTHENTICATE ELECTRONICALLY GENERATED EVIDENCE IN CRIMINAL CASES

This article addresses some of the legal issues and strategic decisions that criminal prosecutors face when using new Federal Evidence Rule 902(13) certifications to self-authenticate the results of an electronic system or process that produces an accurate result. The article builds upon an earlier article published in the January 2018 issue of the Department of Justice Journal of Federal Law and Practice (formerly United States Attorneys' Bulletin), *Two New Self-Authentication Rules That Make It Easier to Admit Electronic Evidence*, [1] and a particularly helpful Baylor Law Review article, *Authenticating Digital Evidence*. [2]

Although Federal Rule of Evidence 902(13) [3] and 902(14), [4] were ***82** intended to work in the same manner as the Rule 902(11) business records certification in practice, [5] Rule 902(13) has the potential to present a number of strategic issues for prosecutors. These issues include the contents of the certification, the possible Confrontation Clause questions raised by offering the certificate to the jury, and the potential need for a witness to explain machine-generated records, even with a certification.

Rule 902(13) is meant to work in tandem with Rule 901(b)(9). Under Rule 901(b)(9), a party may authenticate evidence by offering "evidence describing a process or system and showing that it produces an accurate result." [6] On its own, Rule 901(b)(9) requires a live witness to offer such evidence. [7] Rule 902(13) creates the opportunity to prove authenticity by using a certification to make the showing. [8] In this regard, the drafters intended the rule to work in the same way that Rule 902(11) works with Rule 803(6), the business records exception to the hearsay rule. [9] The Advisory Committee Notes for the adoption of Rule 902(13) contain the following paragraph:

> A proponent establishing authenticity under this Rule must present a certification containing information that would be sufficient to establish authenticity were that information provided by a witness at trial. If the certification provides information that would be insufficient to authenticate the record if the certifying person testified, then authenticity is not established under this Rule. The Rule specifically allows the authenticity foundation that satisfies Rule 901(b)(9) to be established by a certification rather than the testimony of a live witness. [10]

While the facts asserted in a typical Rule 902(11) business-records certification are generally perfunctory and are rarely, if ever, challenged, the assertion that a process produces a reliable result could be accepted on its face, or it could face challenges to its factual assertions and sufficiency.

***83** Consider an example that no one would challenge--a copy made by a photocopy machine. While this may seem an odd example, a photocopy machine is an example of a system or process that produces an accurate result. That proposition is so widely accepted that the drafters of the Federal Rules of Evidence wrote it into the rules. Rule 1003 makes a copy admissible as an original because photocopying was an accepted process, when they wrote the Rules in 1972. [11] Prosecutors likely will have similar ready acceptance of log files of a provider, such as Google, Yahoo!, or Facebook when the logs show the date and time of access to an account and the connecting Internet Protocol (IP) address. A simple statement in a certification from Google will probably go unchallenged. Machine-generated records from less familiar systems and processes, however, may require a more factually detailed certification.

The January 2018 article outlined four examples of Rule 902(13) certifications: (1) showing that a particular USB device was connected to a computer; (2) proving that a server was used to connect to a particular web page; (3) proving that a person was not near the scene of an event; and (4) proving association and activity between alleged co-conspirators. [12] A review of each example is instructive.

Example 1: USB drive. Whenever a person plugs a USB device (thumb drive, external hard drive, or mouse) into a computer using the Windows operating system (OS), the OS will record the vendor and brand of the device and its serial number. [13] Without Rule 902(13), the lawyer would need to call a forensic examiner, qualify the examiner as an expert, and have the examiner testify about the ***84** Windows OS and the fact that it always records the device information. Rule 902(13) allows the lawyer to offer a certification of the examiner. The question becomes: what will that certification say? If there really is not a dispute over the issue, the certification will likely read something like this: *The Windows OS records vendor, brand, and serial number of every USB device plugged into the computer. This is a regular feature of Windows and the Windows system records this information accurately.*

What happens if the defense contests this issue, or you have a cantankerous technophobe for a judge? In that case, a more detailed certification may be required. As outlined in the Advisory Committee Notes: "If the certification provides information that would be insufficient to authenticate the record if the certifying person testified, then authenticity is not established under this Rule." [14] The more familiar the technology is to the judge (and jury), the more likely a simple certification will suffice. With unfamiliar technology, it is certainly conceivable that some judges will not be satisfied with anything less than a live witness explaining the process. Of course, the advantage of the procedural elements of Rule 902(13) is that if the opposing party objects to the certification and the court agrees, the attorney will know in advance of trial what to do to authenticate the evidence.

Example 2: Web server log. To qualify a web server log without Rule 902(13), the lawyer would need to call a witness who was involved with running the website to explain how the web server software records the date, time, and IP address of everyone accessing the site. With Rule 902(13), a certification from the witness explaining that the web server records this information will be sufficient. [15] While the certification may suffice for a judge to authenticate the web server log, the attorney may still want a live witness for trial. The live witness will educate the jury and make the log persuasive.

Example 3: Proving a person was or was not near a scene. In this example, the attorney wants to offer the metadata from pictures taken with an iPhone to show that the GPS coordinates for the image, along with the date and time stamp, establish that the person was somewhere other than the scene. Without Rule 902(13), the proponent of the evidence would need to call someone familiar with the operation ***85** of an iPhone camera to testify that the Apple iOS embeds the information into every photograph, using data from the phone's processor, which keeps track of time, and from the phone's GPS chip, which keeps track of location. That person would have to testify about how the iOS operates and that the data it records is accurate. Using Rule 902(13), this process may be simplified by using a certification. [16]

If the evidence at issue is seriously contested in the trial, the opponent of the evidence may not relent when the proponent offers the certification. In that case, a certification with only the barebones language that "the system produces an accurate result" may

not suffice and the court may require a more detailed certification. This may depend, however, on the judge's familiarity with the technology. The judge may readily understand the idea that a smart phone "tags" photos with data regarding date, time, and location. In that case, the judge may overrule the objection promptly. If, however, the attorney is offering a Fitbit's calculation of velocity at the time of a collision, a simple conclusory affidavit might not persuade the judge.

Example 4: Text messages to show association. Here, the government wishes to offer text messages between co-conspirators to show association and to admit statements in furtherance of the conspiracy. The messages have been recovered from the phone of one of the defendants. Without Rule 902(13), the government will have to call a forensic witness to explain that the phone's operating system keeps of log of the text messages, that the log includes the date, time, content, and recipient of each message, and that the operating system produces an accurate result. With Rule 902(13), a certification from the forensic witness may suffice. [17] Of course, as with the examples above, there may be instances where the attorney or the judge is not satisfied with a simple certification and may want more detail or a live witness. [18]

I. Who should be the affiant?

Rule 902(13) does not have a requirement regarding the identity of the signer of the certificate. Anyone "qualified" to make the required ***86** assertions can sign the certificate. [19] In examples one (USB device), three (GPS information in photograph), and four (text message logs), the examiner who performed the forensic examination is an obvious choice as the affiant of the certification. Yet, anyone with the necessary expertise can be the affiant. This is also true for example two (webserver logs). For example, to show that a defendant made an unauthorized access to the victim's online pharmacy records, the pharmacy's IT employee who runs the webserver is an obvious candidate. There are other options however. One example would be an FBI agent who was a network engineer and ran his employer's website before joining the FBI. He could also provide a certification.

This is similar to what is customarily done with business records--even before the adoption of Rule 902(11). Rule 803(6)(D) always required "the testimony of the custodian *or another qualified witness*." [20] Courts have long held that the other "qualified witness" only needs to understand the record keeping system to authenticate the evidence. [21]

II. Can--and should--the certification go before the jury?

As noted in the Baylor Law Review article, *Authenticating Digital Evidence*, authentication challenges come in three flavors. [22] In the first, the opponent may not seek to challenge authenticity. [23] In the second, the opponent may argue against authenticity, but offer no evidence. [24] In the third, the opponent wants to offer evidence to challenge the authenticity of the proponent's evidence. [25]

The response to any of the three scenarios starts with Rule 901(a). It states that "[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 ***87** claims it is." [26] The standard in Rule 901(a) is a prima facie showing. [27]

Rule 104(a) [28] governs how the judge should address the first two examples. Because there are no disputed issues of fact on the authentication questions in the first two examples, the judge will decide the authenticity question. [29] If the certification is sufficient, the court will rule that the evidence is properly authenticated for presentation to the jury. The court then turns to other evidentiary questions, such as relevance or hearsay.

When the opponent offers evidence to challenge the authenticity of the proponent's evidence, Rule 104(b) controls. [30] In this instance, the judge makes the preliminary determination whether the proponent offered sufficient evidence under Rule 901(a)

to allow the issue of authenticity to go to the jury. [31] If so, the judge admits the evidence subject to the jury's determination. [32] The judge should give an instruction to the jury that if they find it is more likely that the evidence is authentic, they may consider it for whatever worth they give it. The instruction should continue that if they conclude that it is ***88** more likely than not that the evidence is not authentic, they should disregard it. [33]

Thus, in contested cases, the question arises: if the proponent can use the certification to have the judge make the preliminary ruling, should she also present it to the jury? Offering a certificate may raise questions under the Confrontation Clause. [34]

In *Melendez-Diaz v. Massachusetts,* the United States Supreme Court stated that business records certificates did not violate the Confrontation Clause. [35] The majority opinion noted:

> The dissent identifies a single class of evidence, which, though prepared for use at trial, was traditionally admissible: a clerk's certificate authenticating an official record--or a copy thereof--for use as evidence. But a clerk's authority in that regard was narrowly circumscribed. He was permitted "to certify to the correctness of a copy of a record kept in his office," but had "no authority to furnish, as evidence for the trial of a lawsuit, his interpretation of what the record contains or shows, or to certify to its substance or effect." The dissent suggests that the fact that this exception was "narrowly circumscribed" makes no difference. To the contrary, it makes all the difference in the world. It shows that even the line of cases establishing the one narrow exception the dissent has been able to identify simultaneously vindicates the general rule applicable to the present case. A clerk could by affidavit *authenticate* or provide a copy of an otherwise admissible record, but could not do what the analysts did here: *create* a record for the sole purpose of providing evidence against a defendant. [36]

Based on the quoted language (known as "the *Melendez-Diaz* carve-out"), some courts have held that offering the certificate of the records' custodian to the jury is not a violation of the Confrontation ***89** Clause. [37] The recognition by the Supreme Court in *Melendez-Diaz* that a clerk's certificate can authenticate a copy should resolve the issue of presenting a Rule 902(14) certification (accurate copy) to a jury.

A Rule 902(13) certificate presents some issues that prosecutors should understand and consider. First, the machine output being certified would not present a Confrontation Clause problem. A machine is not a witness and its results are not a statement within the meaning of the Sixth Amendment and Federal Rule of Evidence 801(a). In contrast, an affiant's statement in a certification that interprets or explains the machine's result, or which explains how the affiant collected the underlying evidence or ran the test, likely is subject to the Confrontation Clause. As the Seventh Circuit put it in *United States v. Moon*:

> A physician may order a blood test for a patient and infer from the levels of sugar and insulin that the patient has diabetes. The physician's diagnosis is testimonial, but the lab's raw results are not, because data are not "statements" in any useful sense. Nor is a machine a "witness against" anyone. If the readings are "statements" by a "witness against" the defendants, then the machine must be the declarant. Yet how could one cross-examine a gas chromatograph? Producing spectrographs, ovens, and centrifuges in court would serve no one's interests. That is one reason why Rule 703 provides that the expert's source materials need not be introduced or even admissible in evidence. The vital questions-was the lab work done properly? what do the readings mean?-can be put to the expert on the stand. ***90** The background data need not be presented to the jury. [38]

Thus, the focus of attention when drafting Rule 902(13) certifications should be on the distinction between facts that authenticate the machine's results and facts that go further and attempt to interpret or explain the results.

The decisions in *Melendez-Diaz v. Massachusetts* [39] and *Bullcoming v. New Mexico* [40] help illustrate the distinction between factual assertions that authenticate a machine's results and other factual assertions that attempt to interpret or explain the results. In *Melendez-Diaz*, the prosecution offered certificates of analysis from the forensic examiner. [41] The certificates reported the weight of the seized bags and the results of the chemical tests on the contents of the bags. [42] No witness testified about the analysis and the prosecution offered no machine-generated results. [43] The analyst's statement in the certification that the seized evidence contained cocaine was clearly hearsay. Because it described acts performed by the affiant, it violated the Confrontation Clause. [44]

In *Bullcoming*, the prosecution offered a certificate of one analyst and the live testimony of another analyst. The analyst who performed the gas chromatography test completed the certificate. The analyst, who was familiar with the lab procedures, but who had no personal knowledge of the particular test in evidence, was the witness in court. [45] The certificate included the factual assertions that the breath sample was received with the seals intact and that the analyst had followed the procedures in performing the test set forth in the ***91** certificate, along with the raw data of the machine readout. [46] The analyst's statements in the certificate violated the Confrontation Clause, because they went beyond authenticating the machine-generated result and attempted to explain facts about the chain-of-custody and lab procedures. [47]

In *Melendez-Diaz* and in *Bullcoming*, the certificates contained assertions that interpreted, explained, or added context to machine-generated facts. The problematic assertions were the statements of the witnesses about their activities and interpretations of machine-generated information. Indeed, in her concurring opinion in *Bullcoming*, Justice Sonia M. Sotomayor wrote, "[t]hus, we do not decide whether, as the New Mexico Supreme Court suggests, ... a State could introduce (assuming an adequate chain of custody foundation) raw data generated by a machine in conjunction with the testimony of an expert witness." [48]

The authentication certificate is the statement of a person, so prosecutors should consider whether the factual assertions in a certificate fall within or outside of the *Melendez-Diaz* carve-out. When the certification simply tracks the language of the rule (the "process or system that produces an accurate result"), [49] there should not be a Confrontation Clause problem when offering the certificate to the jury.

The check on whether the system or process produces a reliable result was not done for the purposes of litigation. The check was done when the system was created, or at some later testing, to ensure that the system functioned properly. When Microsoft created the Windows OS, it verified that the logging function accurately tracked the thumb drives inserted into the computer. [50] When Cellebrite created its ***92** machines, it checked to be sure that it accurately copied the contents of a cell phone. When a law enforcement agency buys and installs a Cellebrite machine, it likely tests it to be sure that it accurately copies what is on a cell phone. Thus, the Rule 902(13) certification is similar to the business records certification. It is a statement about a pre-existing test of the reliability of the system or process that generated the result. [51] Such a certification is analogous to the clerk's certificate referenced in *Melendez-Diaz*.

As the certifications become more detailed, however, there is a serious risk of a Confrontation Clause error if a prosecutor tries to offer the certificate into evidence before the jury. It is not the amount of detail showing authenticity that is the problem. Rather, the risk is that a prosecutor drafts an out-of-court statement that goes beyond authentication and attempts to interpret or explain the machine-generated record. Recall the language from *Melendez-Diaz*:

> But a clerk's authority in that regard was narrowly circumscribed. He was permitted "to certify to the correctness of a copy of a record kept in his office," but *had "no authority to furnish, as evidence for the trial of a lawsuit, his interpretation of what the record contains or shows, or to certify to its substance or effect*." [52]

Prosecutors may want to consider having a live witness testify and be subject to cross-examination to avoid Confrontation Clause issues. In addition, if the certification is detailed, a live witness may be more ***93** convincing to a jury than a piece of paper. As discussed above, the witness does not have to be employed by the institution that generated the machine record.

III. Which witness should explain the significance of the machine generated record?

Again, a witness from the organization whose equipment generated the record is an obvious choice. There are, however, logistical constraints. Companies may resist sending witnesses to trials in various locations for only a few minutes of testimony. Google and Facebook, for example, do not want to send witnesses to courtrooms around the country every week to give five minutes worth of testimony. Moreover, the government does not want to pay the costs of transporting and housing these witnesses. An agent who has a background in this field may be a useful alternative. Consider first whether you need a witness at all. Some machine-generated records do not need explanation. The average juror likely understands a monthly bank statement and a telephone call detail record without the help of a witness. Web access logs, or cell site location information with GPS latitude and longitude coordinates, however, will likely be confusing to most jurors. In those instances, an agent may be a good option as a witness. Be aware that you are calling this agent as an expert under Rule 702. This witness, as outlined by Rule 702, holds "specialized knowledge [that] will help the trier of fact understand the evidence or to determine a fact in issue." [53]

Expert witnesses do not have to testify in the form of an opinion. Rule 702 states that they may testify "in the form of an opinion *or otherwise*." [54] As the Advisory Committee Notes state:

> Most of the literature assumes that experts testify only in the form of opinions. The assumption is logically unfounded. The rule accordingly recognizes that an expert on the stand may give a dissertation or exposition of scientific or other principles relevant to the case, leaving the trier of fact to apply them to the ***94** facts. [55]

Accordingly, the agent, as an expert, can explain the machine process to the jury, and explain the records. Do not forget, however, to give the required expert notice. Federal Rule of Criminal Procedure 16(a)(1)(G) provides, in part:

> [T]he government must give to the defendant a written summary of any testimony that the government intends to use under Rules 702, 703, or 705 of the Federal Rules of Evidence during its case-in-chief at trial .... The summary provided under this subparagraph must describe the witness's opinions, the bases and reasons for those opinions, and the witness's qualifications. [56]

IV. What is the value of Rule 902(13) if a live witness may still be needed?

Recall that authentication is a two-step process. First, the judge must determine that the proponent has made a prima facie showing of the authenticity of the evidence. [57] Second, it is always up to the jury whether to accept evidence as authentic. Therefore, even without thinking about it, we typically authenticate the evidence for the jury as well. Frequently, we will prove authenticity to the jury (even if it is not contested) to make the evidence more persuasive. One can use internal contents of documents, such as e-mails or text messages, as provided in Rule 901(b)(4). [58] For example, the prosecutor may argue that the contents make it clear that only the defendant could have sent or received these electronic messages. Prosecutors may compare evidence with other evidence, the authenticity of which is not in question, for example, referencing film from a surveillance camera. [59]

Using a Rule 902(13) certification may serve to overcome the first ***95** hurdle--the judge's determination of a prima facie showing of authenticity--without having to call a witness. In that case, the evidence will be authenticated and, assuming it is relevant and not unduly prejudicial, it will be admissible. The Rule 902(13) certification eliminated one witness whose attendance at trial may be expensive or difficult to procure.

Now, at trial, you can call an agent or other qualified witness to delve into the evidence using other means of authentication, such as distinctive characteristics (Rule 901(b)(4)) to show the jury why the evidence is both authentic and persuasive. Using a Rule 902(13) certification means there is no need to waste time dragging a perfunctory authentication witness to the courthouse to convince the judge first, before you can present the evidence to the jury.

For example, consider the extraction of data from a cell phone. A certification by a qualified person under Rule 902(13) stating that a Cellebrite machine uses a process or system that produces an accurate result of a phone's contents might be sufficient to authenticate the evidence for the judge. Now, at trial, the agent, who knows the case well, can go through the contents of the phone, showing the jury that only the defendant could have sent or received the pictures, e-mails, and text messages found in the phone. This will give the jury confidence that the cell phone contents are authentic and persuasive.

There are two additional benefits to using Rule 902(13). First, if you file a pretrial motion in limine to authenticate the evidence, attaching the Rule 902(13) certificate, you can begin to educate the judge--before trial--about the nature of your case and your proof. Second, as noted above, by obtaining a pretrial determination, you know whether you need an authenticating witness or not.

***96 V. Conclusion**

Rule 902(13) has the potential to make life easier for prosecutors by giving them the chance to authenticate and admit a host of machine-generated records more easily. At a minimum, Rule 902(13) can help prosecutors know well before trial which witnesses will be needed for trial. If you are considering offering the certification as evidence for the jury to see, you must consider the potential Confrontation Clause pitfalls and plan ahead to address them.

Footnotes

a1 **Michael L. Levy** is an Assistant United States Attorney in the Eastern District of Pennsylvania. From 2001 until 2017 (when he entered phased retirement), he was the Chief of Computer Crimes in that district. He has also served as the First Assistant United States Attorney and was twice the interim United States Attorney**.**

a2 **John M. Haried** is an Assistant United States Attorney in the District of Colorado. He is also the Criminal eDiscovery Coordinator for the Executive Office for United States Attorneys (EOUSA) in Washington, D.C., and a member of EOUSA's Electronic Litigation Working Group and the Department of Justice's Electronic Discovery Working Group. He is also a member of the Joint Electronic Technology Working Group (JETWG), which is a collaboration between the Department of Justice, the Office of Defender Services, Federal Defender Organizations, the Administrative Office of U.S. Courts, private attorneys who accept Criminal Justice Act (CJA) appointments, and liaisons from the United States Judiciary.

1 John M. Haried, *Two New Self-Authentication Rules That Make It Easier to Admit Electronic Evidence*, 66 U.S. ATT'YS BULL., no. 1, 2018, at 127.

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

3 FED. R. EVID. 902(13) ("A record generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent must also meet the notice requirements of Rule 902(11).").

4 FED. R. EVID. 902(14) (data copied from an electronic storage medium). We do not believe that Rule 902(14) will present similar problems. Rule 902(14) requires a digital certification of the accuracy of the copy-usually a hash value--and there should be few issues with it.

5 FED. R. EVID. 902(11) (the business records certification).

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

7 *Id.*

8 *See* FED. R. EVID. 902(13).

9 FED. R. EVID. 803(6).

10 FED. R. EVID. 902(13) advisory committee's note to 2017 amendment.

11 FED. R. EVID. 1003 advisory committee's note to 1972 amendment ("When the only concern is with getting the words or other contents before the court with accuracy and precision, then a counterpart serves equally as well as the original, if the counterpart is the product of a method which insures accuracy and genuineness. By definition ... a 'duplicate' possesses this character.").

12 Haried, *supra* note 1, at 128-30.

13 *See, e.g.*, *How to Analyze USB Device History in Windows*, MAGNET FORENSICS, https://www.magnetforensics.com/computer-forensics/how-to-analyze-usb-device-history-in-windows/ (last visited Nov. 20, 2018); *USB Device Registry Entries*, MICROSOFT, https://docs.microsoft.com/en-us/windows-hardware/drivers/usbcon/usb-device-specific-registry-settings (last visited Nov. 20, 2018); *USB History Viewing*, FORENSICS WIKI, https://www.forensicswiki.org/wiki/USB_History_Viewing (last visited Nov. 20, 2018).

14 FED. R. EVID. 902(13) advisory committee's note to 2017 amendment.

15 *See* FED. R. EVID. 902(13).

16 *See id.*

17 *See id.*

18 This article only discusses authenticating text messages. Attorneys will still need to address other evidentiary issues such as relevance or hearsay. Rule 902(13) does not offer assistance on those questions.

19 *See* FED. R. EVID. 902(13) (requiring "certification of a qualified person").

20 FED. R. EVID. 803(6)(D).

21 *See, e.g.,* United States v. Ray, 930 F.2d 1368, 1369-70 (9th Cir. 1990); United States v. Franco, 874 F.2d 1136, 1139-40 (7th Cir. 1989); United States v. Hathaway, 798 F.2d 902, 905-07 (6th Cir. 1986).

22 *See* Grimm, *supra* note 2, at 5-11.

23 *See id.*

24 *See id.*

25 *See id.*

26 FED. R. EVID. 901(a); see also *In re* Japanese Elec. Prod. Antitrust Litig., 723 F.2d 238, 285 (3d Cir. 1983), rev'd on other grounds, 475 U.S. 574 (1986) ("All that is required is a foundation from which the fact-finder could legitimately infer that the evidence is what its proponent claims it to be.").

27 *See, e.g.,* United States v. Fluker, 698 F.3d 988, 999 (7th Cir. 2012); United States v. Vidacak, 553 F.3d 344, 349 (4th Cir. 2009); United States v. American Honda Motor Co., 921 F.2d 15, 16 n.2 (1st Cir. 1990); United States v. Blackwood, 878 F.2d 1200, 1202

(9th Cir. 1989); United States v. Caldwell, 776 F.2d 989, 1002 (11th Cir. 1985); United States v. Jardina, 747 F.2d 945, 951 (5th Cir. 1984); United States v. Helberg, 565 F.2d 993, 997 (8th Cir. 1977); United States v. Albergo, 539 F.2d 860, 864 (2d Cir. 1976).

28 FED. R. EVID. 104(a) ("The court must decide any preliminary question about whether a witness is qualified, a privilege exists, or evidence is admissible. In so deciding, the court is not bound by evidence rules, except those on privilege.").

29 *See id.* Of course, the jury has the right to accept or reject any evidence offered.

30 FED R. EVID. 104(b) ("When the relevance of evidence depends on whether a fact exists, proof must be introduced sufficient to support a finding that the fact does exist. The court may admit the proposed evidence on the condition that the proof be introduced later.").

31 *Id.*

32 *See id.*

33 *See* Grimm, *supra* note 2, at 5-11 (outlining a more complete discussion of the analysis).

34 *See, e.g.,* Melendez-Diaz v. Massachusetts, 557 U.S. 305 (2009).

35 *Id.*

36 *Melendez-Diaz*, 557 U.S. at 322-23 (internal citations omitted; footnote omitted; emphasis in original).

37 *See, e.g.,* United States v. Yeley-Davis, 632 F.3d 673, 680 (10th Cir. 2011) (holding certification presented "merely to authenticate the cell phone records--and not to establish or prove some fact at trial ... [was] not testimonial"); United States v. Morgan, 505 F.3d 332, 338-39 (8th Cir. 2007) (holding "business records are not testimonial in nature and their admission at trial is not a violation of the Confrontation Clause"); United States v. Ellis, 460 F.3d 920, 927 (7th Cir. 2006) (holding that certification by custodian of records at a local hospital attesting that records are kept in the ordinary course of business are not testimonial); United States v. Weiland, 420 F.3d 1062, 1076-77 (9th Cir. 2005) (holding admission of records of prior convictions without subjecting Secretary of State records custodian to cross-examination did not violate the Confrontation Clause).

38 United States v. Moon, 512 F.3d 359, 362 (7th Cir. 2008); see also United States v. Washington, 498 F.3d 225, 230 (4th Cir. 2007) ("[T]he raw data generated by the diagnostic machines are the 'statements' *of the machines* themselves, not their operators. But 'statements' made by machines are not out-of-court statements made by declarants that are subject to the Confrontation Clause." (emphasis in original)).

39 557 U.S. 305 (2009).

40 564 U.S. 647 (2011).

41 *Melendez-Diaz*, 557 U.S. at 308.

42 *Id.*

43 *See id.*

44 *Id.* at 321-22.

45 *Bullcoming*, 564 U.S. at 657.

46 *Id.* at 653.

47 *Id.* at 673-74 (Sotomayor, J., concurring).

48 *Id.* at 674 (Sotomayor, J., concurring) (internal citation omitted).

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

50 *See How to Analyze USB Device History in Windows*, MAGNET FORENSICS, https://www.magnetforensics.com/computer-forensics/how-to-analyze-usb-device-history-in-windows/ (last visited Dec. 5, 2018); *USB Device Registry Entries*, MICROSOFT, https://docs.microsoft.com/enus/windowshardware/drivers/usbcon/usbdevice-specific-registry-settings (last visited Dec. 5, 2018); *USB History Viewing*, FORENSICS WIKI, https://www.forensicswiki.org/wiki/USB_History_Viewing (last visited Dec. 5, 2018).

51 *See* Williams v. Illinois, 567 U.S. 50, 58 (2012). The plurality opinion in *Williams* also supports this view:
The Cellmark report is very different from the sort of extrajudicial statements, such as affidavits, depositions, prior testimony, and confessions, that the Confrontation Clause was originally understood to reach. The report was produced before any suspect was identified. The report was sought not for the purpose of obtaining evidence to be used against petitioner, who was not even under suspicion at the time, but for the purpose of finding a rapist who was on the loose. And the profile that Cellmark provided was not inherently inculpatory.
Id.

52 Melendez-Diaz v. Massachusetts, 557 U.S. 305, 322 (2009) (citations omitted, emphasis added).

53 FED. R. EVID. 702(a).

54 FED. R. EVID. 702 (emphasis added).

55 FED. R. EVID. 702 advisory committee's note to 1972 proposed rules.

56 FED. R. CRIM. P. 16(a)(1)(G).

57 *See* FED. R. EVID. 901(a); FED. R. EVID. 104; see cases, *supra* note 26.

58 FED. R. EVID. 901(b). The following are examples only--not a complete list--of evidence that satisfies the requirement: "... (4) Distinctive Characteristics and the Like. The appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances." FED. R. EVID. 901(b)(4).

59 *See* Timothy M. O'Shea, *Whole Device Authentication*, 67 DOJ. J. FED. L. & PRAC., 97, 97-113 (2019) (providing several examples of these types of authentication).

67 DOJJFLP 81

End of Document