HOW TWO NEW RULES FOR SELF-AUTHENTICATION WILL SAVE YOU TIME AND MONEY

BY JOHN M. HARIED

The Standing Committee on Federal Rules recently approved two new self-authentication rules for electronic machine-generated evidence. The goal is to save time and money by creating a pretrial procedure for the parties to eliminate court appearances for unnecessary witnesses when there is not a genuine dispute about authenticity. Barring disapproval by the Supreme Court or Congress, the rules will become effective on Dec. 1, 2017.

THE PROBLEM: UNPRODUCTIVE ROADBLOCKS TO AUTHENTICATION OF ELECTRONIC EVIDENCE

In June 2013, Pfc. Bradley Manning was facing a military court-martial on charges of leaking classified information to WikiLeaks. The court-martial was conducted at Fort Meade, Md., under the Military Rules of Evidence, which follow the Federal Rules of Evidence.

The prosecution argued that WikiLeaks had posted on its website a solicitation for the types of classified information that Manning was charged with providing. As evidence, the prosecutor sought to introduce Exhibit 109, a screen capture of WikiLeaks' "Most Wanted Leaks of 2009." The prosecution obtained Exhibit 109 from Archive.org, located in San Francisco, which operates the Wayback Machine (archive.org/web/). The Wayback Machine is an internet archiving system that uses software programs known as web crawlers to surf the internet and automatically capture and store images from webpages.

Manning objected to Exhibit 109 as hearsay. In ruling on authentication during trial, the judge found that Exhibit 109 was not a business record that could be self-authenticated under F.R.E. 902(11). However, the trial judge ruled Exhibit 109 was relevant and admissible if the prosecution brought the custodian of records from San Francisco to Maryland to provide live testimony to authenticate it on other Rule 901 grounds. As the witness was about to depart San Francisco for Maryland, the defendant stipulated to the authenticity of Exhibit 109.

The Manning case illustrates several issues common to authentication of electronic machine-generated information. First, in today's electronic information world, authentication witnesses often live far from the courthouse, so presenting live testimony is expensive. The records of Archive.org, Google, Facebook, Microsoft, and other custodians of pervasive electronic records may be evidence in any courthouse in the nation. Second, many categories of machine-generated information are not business records because the custodian did not create the record's content or rely upon the content's accuracy to conduct its business. Third, while the party against whom the evidence is offered often does not genuinely dispute the authenticity of the item, he can force the exhibit's proponent to undertake great trouble and expense because the evidence rules — until now — did not provide a mechanism to resolve the authentication issues before trial. Because machine-generated electronic information is a growing source of important evidence, litigants need a mechanism to avoid unnecessary authentication disputes that waste their money and the court's time.

THE SOLUTION: NEW RULES 902(13) AND 902(14)

Effective Dec. 1, 2017, new Rules 902(13) and 902(14) will provide a mechanism for parties to identify and address authentication issues for evidence generated by an electronic process or system. These new rules combine the conceptual frameworks of Rule 901(b)(9) — authentication by evidence describing a process or system that produces an accurate result — and Rules 902(11) and (12) — self-authentication of business records:

Rule 902. Evidence That Is Self-Authenticating

The following items of evidence are self-authenticating; they require no extrinsic evidence of authenticity in order to be admitted:

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

ILLUSTRATIVE USE CASES

The following hypotheticals illustrate how Rules 902(13) and 902(14) can be used to address authentication of electronic evidence, eliminate unnecessary witnesses, and save money.

COMMITTEE NOTE 902(13)

The amendment sets forth a procedure by which parties can authenticate certain electronic evidence other than through the testimony of a foundation witness. As with the provisions on business records in Rules 902(11) and (12), the Committee has found that the expense and inconvenience of producing a witness to authenticate an item of electronic evidence is often unnecessary. It is often the case that a party goes to the expense of producing an authentication witness and then the adversary either stipulates authenticity before the witness is called or fails to challenge the authentication testimony once it is presented. The amendment provides a procedure under which the parties can determine in advance of trial whether a real challenge to authenticity will be made, and can then plan accordingly.

Nothing in the amendment is intended to limit a party from establishing authenticity of electronic evidence on any ground provided in these Rules, including through judicial notice where appropriate.

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.

The reference to the "certification requirements of Rule 902(11) or (12)" is only to the procedural requirements for a valid certification. There is no intent to require, or permit, a certification under this rule to prove the requirements of Rule 803(6). Rule 902(13) is solely limited to authentication and any attempt to satisfy a hearsay exception must be made independently.

A certification under this Rule can establish only that the proffered item has satisfied the admissibility requirements for authenticity. The opponent remains free to object to admissibility of the proffered item on other grounds – including hearsay, relevance, or in criminal cases the right to confrontation. For example, assume that a plaintiff in a defamation case offers what purports to be a printout of a web page on which a defamatory statement was made. Plaintiff offers a certification under this Rule in which a qualified person describes the process by which the web page was retrieved. Even if that certification sufficiently establishes that the web page is authentic, defendant remains free to object that the statement on the web page was not placed there by defendant. Similarly, a certification authenticating a computer output, such as a spreadsheet, does not preclude an objection that the information produced is unreliable – the authentication establishes only that the output came from the computer.

A challenge to the authenticity of electronic evidence may require technical information about the system or process at issue, including possibly retaining a forensic technical expert; such factors will affect whether the opponent has a fair opportunity to challenge the evidence given the notice provided.

The reference to Rule 902(12) is intended to cover certifications that are made in a foreign country.

Example One: Proving that a USB device was connected to (i.e., plugged into) a computer. In a civil case litigated in Chicago, a disputed issue is whether Susan Hall used her personal computer to access files stored on a particular USB thumb drive. Her computer uses the Windows operating system, which automatically records information about every USB device connected to her computer in a database known as the "Windows registry." The Windows registry database is maintained on the computer by the Windows operating system to facilitate the computer's operations. The registry logs the computer's operations and users' actions, for example, when a user accessed particular files or applications such as internet browsers. A forensic technician, located near Hall's home in Boston, has provided a printout from the Windows registry that indicates that a USB thumb drive, identified by manufacturer, model, and serial number, was last connected to Ms. Hall's computer at a specific date and time.

Without Rule 902(13), the proponent of the evidence would need to present testimony from the forensic technician who obtained the printout in order to establish the authenticity of the evidence. During testimony, the forensic technician typically would be asked to testify about his or her background and qualifications, the process used to conduct the digital forensic examinations, the process by which the Windows operating system maintains information in the Windows registry, including information about USB devices connected to the computer, and the steps taken to examine the Windows registry and to produce the printout identifying the USB device.

With Rule 902(13), the proponent of the evidence could obtain a written certification from the forensic technician, stating that the Windows operating system regularly records information in the Windows registry about USB devices connected to a computer, that the process by which such information is recorded produces an accurate result, and that the printout accurately reflected information stored in the Windows registry of Hall's computer. The proponent would be required to provide reasonable written notice of its intent to offer the printout as an exhibit and to make the written certification and proposed exhibit available for inspection. If the adversary did not dispute the accuracy or reliability of the process that produced the exhibit, the proponent would not need to call the forensic technician as a witness to establish the authenticity of the exhibit.[1] The court would make the threshold Rule 104(a) authenticity finding and admit the exhibit, absent other proper objections.

Example Two: Proving that a server was used to connect to a particular web page. A malicious

COMMITTEE NOTE 902(14)

The amendment sets forth a procedure by which parties can authenticate data copied from an electronic device, storage medium, or an electronic file, other than through the testimony of a foundation witness. As with the provisions on business records in Rules 902(11) and (12), the Committee has found that the expense and inconvenience of producing an authenticating witness for this evidence is often unnecessary. It is often the case that a party goes to the expense of producing an authentication witness, and then the adversary either stipulates authenticity before the witness is called or fails to challenge the authentication testimony once it is presented. The amendment provides a procedure in which the parties can determine in advance of trial whether a real challenge to authenticity will be made, and can then plan accordingly.

Today, data copied from electronic devices, storage media, and electronic files are ordinarily authenticated by "hash value." A hash value is a number that is often represented as a sequence of characters and is produced by an algorithm based upon the digital contents of a drive, medium, or file. 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. The 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.

Nothing in the amendment is intended to limit a party from establishing authenticity of electronic evidence on any ground provided in these Rules, including through judicial notice where appropriate.

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 reference to the "certification requirements of Rule 902(11) or (12)" is only to the procedural requirements for a valid certification. There is no intent to require, or permit, a certification under this rule to prove the requirements of Rule 803(6). Rule 902(14) is solely limited to authentication and any attempt to satisfy a hearsay exception must be made independently.

A certification under this Rule can only establish that the proffered item is authentic. The opponent remains free to object to admissibility of the proffered item on other grounds – including hearsay, relevance, or in criminal cases the right to confrontation. For example, in a criminal case in which data copied from a hard drive is proffered, the defendant can still challenge hearsay found in the hard drive, and can still challenge whether the information on the hard drive was placed there by the defendant.

A challenge to the authenticity of electronic evidence may require technical information about the system or process at issue, including possibly retaining a forensic technical expert; such factors will affect whether the opponent has a fair opportunity to challenge the evidence given the notice provided.

The reference to Rule 902(12) is intended to cover certifications that are made in a foreign country.

hacker executed a denial-of-service attack against Acme's website. Acme's web server maintained an Internet Information Services (IIS) log that automatically records information about every internet connection routed to the web server to view a web page, including the IP address, web page, user agent string, and what was requested from the website. The IIS logs reflected repeated access to Acme's website from an IP address known to be used by the hacker. The proponent wants to introduce the IIS log to prove that the hacker's IP address was an instrument of the attack.

Without Rule 902(13), the proponent would have to call a website expert to testify about the server's operating system, his search of the IIS log, how the IIS log works, and that the exhibit is an accurate record of the IIS log.

With Rule 902(13), the proponent would obtain a website expert's certification of the facts establishing authenticity of the ISS log and provide the certification and exhibit to the opposing party with reasonable notice that it intends to offer the exhibit at trial. If the opposing party does not timely dispute the reliability of the process that produced the ISS log, then the proponent would not need to call the website expert to establish authenticity.

Example Three: Proving that a person was or was not near the scene of an event. Robert Jackson is a defendant in a civil action alleging that he was the driver in a hit-and-run collision with a U.S. Postal Service mail carrier in Atlanta at 2:15 p.m. on March 6, 2016. Mr. Jackson owns an iPhone, which has software that records machine-generated dates, times, and GPS coordinates of each picture he takes with his iPhone. Mr. Jackson's iPhone contains two pictures of his home in an Atlanta suburb at about 1 p.m. on March 6. He wants to introduce into evidence the photos recovered forensically from his iPhone, together with the metadata, including the date, time, and GPS coordinates, to corroborate his alibi that he was at home several miles from the scene at the time of the collision.

> "...[O]ther categories of machine-generated electronic information contain both nonhearsay information and hearsay statements. Rule 902(13) is limited; it only serves as a mechanism to authenticate the machine-generated information, not the hearsay statement.

Without Rule 902(13), the proponent would have to call the forensic technician to testify about Jackson's iPhone's operating system, his search of the phone, how the metadata was created and stored with each photograph, and that the exhibit is an accurate record of the photographs.

With Rule 902(13), the proponent would obtain the forensic technician's certification of the facts establishing authenticity of the exhibits and provide the certification and exhibits to the opposing party with reasonable notice that it intends to offer the exhibits at trial. If the opposing party does not timely dispute the reliability of the process that produced the iPhone's photos and their metadata, then the proponent would not have to call the technician to establish authenticity.

Example Four: Proving association and activity between alleged co-conspirators. Ian Nicholas is charged with conspiracy to rob the First National Bank in San Diego on Jan. 30, 2016. Two armed robbers drove away in a silver Ford Taurus. The alleged co-conspirator was Dain Miller. Dain was arrested on an outstanding warrant on Feb. 1, 2016, and in his pocket was his Samsung Galaxy phone. The phone's software automatically maintained a log of text messages that includes the text content, date, time, and number of the other phone involved. Pursuant to a warrant, forensic technicians examined Dain's phone and located four text messages to Ian's phone from January 29: "Meet my house @9"; "Is Taurus the Bull out of shop?"; "Sheri says you have some blow"; and "see u tomorrow." At Ian's trial the government wants to offer the four text messages to prove the conspiracy.

Without Rule 902(13), the proponent would have to call the forensic technician to testify about Dain's phone's operating system, his search of the phone's text message log, how the log was created, and that the exhibit is an accurate record of the phone's log.

With Rule 902(13), the proponent would obtain the forensic technician's certification of the facts establishing authenticity of the exhibit and provide the certification and exhibit to the opposing party with reasonable notice that it intends to offer the exhibit at trial. If the opposing party does not timely dispute the reliability of the process that produced the phone's log, then the court would make authenticity finding and admit the exhibit.

A hearsay objection would be retained. As discussed below, under Rule 902(13), the adversary — here, defendant Ian — would retain his hearsay objections to the text messages found on Dain's phone.

Example Five: Using Rule 902(14) to authenticate a copy. In the armed robbery scenario, Example 4 above, forensic technician Smith made a forensic copy of Dain's Samsung Galaxy phone in the field in San Diego. Smith verified that the forensic copy was identical to the original phone's text logs using an industry standard methodology (e.g., hash value or other means). Smith then sent the copy to forensic technician Jones, who performed his examination at his lab in Atlanta. Jones used the copy to conduct his entire forensic examination so that he would not inadvertently alter the data on the phone. Jones found the text messages. The government wants to offer the copy into evidence as part of the basis for Jones' testimony about the text messages he found.

Without Rule 902(14), the government would have to call two witnesses. First, forensic technician Smith would need to testify about making the forensic copy of information from Dain's phone, and about the methodology that he used to verify that the copy was an exact copy of information inside the phone. Second, the government would have to call forensic technician Jones to testify about his examination.

With Rule 902(14), the government would obtain Smith's certification of the facts establishing how he copied the phone's information and then verified the copy was true and accurate. Before trial the government would provide the certification and exhibit to the opposing party — here, defendant Ian — with reasonable notice that it intends to offer the exhibit at trial. If Ian's attorney does not timely dispute the reliability of the process that produced the Samsung Galaxy's text message logs, then the government would only call forensic technician Jones. Depending upon its trial strategy, the government might also seek to authenticate the text message logs under Rule 902(13).

POTENTIAL ISSUES WITH THE APPLICATION OF RULE 902(13)

Electronic evidence comes from many sources, thereby implicating different rules of evidence. In criminal cases, electronic evidence — like SMS text messages or photos — can come directly from the memory of personal cell phones and computers seized during an arrest or pursuant to a search warrant. Usually the business records rules — Rules 803(6) and 902(11) — do not apply to information found on personal devices. Conversely, the business records rules often apply to electronic evidence in the records of commercial service providers obtained by subpoena or other legal process. Internet service providers (ISPs) offer a wide array of services, including internet access, mailboxes, and data hosting. The ranks of ISPs include AT&T, DISH Network, Time Warner, Comcast, Century Link, Verizon, and many others. ISPs' business records include machine-generated information like the date and time stamps, accounts used, and routing histories. However, other information maintained by ISPs does not qualify as a business record because the ISP does not rely upon the truthfulness or accuracy of the information to conduct its business. In civil cases, electronic evidence can come from those sources or from the parties' own computer systems. Below are some possible issues.

Hearsay contained within machine-generated electronic information

Machine-generated information is not hearsay because it is not a "statement" of a "person" under Rule 801(a).[2] In Example 1 above, the Windows registry for Susan Hall's home computer contained only machine-generated data about the computer's operations and users' actions, such as when a thumb drive was connected to the computer, when a user opened an internet browser, or when the computer was connected to a particular wireless network. That information is not hearsay. Similarly, in Example 3 the record of the date, time, and GPS coordinates for pictures taken on Robert Jackson's iPhone contained no hearsay.

However, other categories of machine-generated electronic information contain both nonhearsay information and hearsay statements. Rule 902(13) is limited; it only serves as a mechanism to authenticate the machine-generated information, not the hearsay statement. For example, in these text messages found in the memory of individual B's cell phone there is a hearsay statement implicating Dan Defendant:

> Individual A, Friday at 9:50 am: "Who shot the bank guard?"
> Individual B, Friday at 9:52 am: "Not me. Last week Tammy told me she saw Dan shoot him."

At the trial of Dan Defendant, the prosecution could authenticate only some portions of the text messages found on Individual B's phone by a certification from a forensic technician pursuant to Rule 902(13) — such as which phones were used and the date and times of the text messages. But the text messages would not be admitted as evidence on that basis because Dan Defendant would retain his hearsay objection to the statement by Tammy that she saw Defendant shoot the bank guard. The Committee Note to Rule 902(13) notes that the adversary retains other objections, like hearsay.

The result would be the same if the prosecution subpoenaed the very same text messages from the ISP's records. The prosecution could authenticate portions of the messages with the ISP's certification under either Rule 902(11) or 902(13) — like the date and time stamps and accounts used — but under either rule Defendant would still retain his hearsay objection. And, as discussed below, neither Rule 902(11) or Rule 902(13) alone would provide the prosecution a basis to authenticate the text message's content.

The interplay between hearsay, business records, and Rules 803(6), 902(11), and 902(13)

As seen, many instances will arise where the rules governing the admissibility and authentication of electronic evidence intersect and overlap. Some common examples are Facebook posts, instant message chats, emails, and text messages where the evidence of the communication comes from the records of a commercial service provider like Facebook, Instagram, Google, Microsoft, or Verizon. Some facets of the record of a Facebook post, an email, or a text message are machine-generated, such as the date and time stamp and the source and destination account. Other

facets, like the transmitted message's content, may be admissible or inadmissible hearsay statements.

Recently, the Third Circuit addressed these issues and the resulting business records authentication requirements under Rules 803(6) and 902(11). In *United States v. Browne*,[3] the criminal charges included enticement of minors to engage in sexual activity, and the disputed evidence was a series of Facebook chats between the defendant and three victims. The government argued that the Facebook chats in their entirety were Rule 803(6) business records that could be self-authenticated under Rule 902(11). The court disagreed, holding that Facebook chats contained a mixture of Facebook's business records and nonbusiness record information. The business record elements were limited to "certain aspects of the communications exchanged over that platform, that is, confirmation that the depicted communications took place between certain Facebook accounts, on particular dates, or at particular times."[4] The court held that the content of the communications between the defendant and victims were not business records because Facebook did not verify or rely upon the substance of the chats in the course of its business. The chats were merely sent via the Facebook platform.[5]

New Rule 902(13) adds an alternative mechanism of authenticating Facebook chats like those in *Browne*, but it does not change the outcome. Facebook chats — and other electronic evidence — may be authentic because they are the product of a system or process that produces an accurate result. But portions of the record may be inadmissible because the adversary has other valid evidentiary objections, such as hearsay. In the Facebook chat example, a Rule 902(13) certification could establish that the Facebook system accurately records the substance of the chats exchanged, but the certification would not preclude a hearsay or other appropriate objection to the chats' content.

It bears noting that for some types of electronic evidence, the proponent cannot simply rely upon a Rule 902(13) certification to fully establish the authentication required by Rule 901(a). He may need to further authenticate the evidence by linking it to a particular individual to establish authorship. In *Browne* the court faced this issue because the defendant claimed the evidence was insufficient to link him to the Facebook account in the name "Billy Button." The court recited the direct and circumstantial evidence linking the defendant to the account: He told the police it was his account; the victims testified to meeting the defendant in person, identified him, and described their chat communications; and a cell phone the defendant used to contact the victims was found at the defendant's home. The court held that it is "no less proper to consider a wide range of evidence for the authentication of social media records than it is for more traditional documentary evidence."[6]

Confrontation Clause limitations on self-authentication in criminal cases

In criminal cases, there are constitutional limitations on what evidence can be self-authenticated. The Advisory Committee on Evidence Rules carefully considered the Confrontation Clause issues during adoption of Rules 902(13) and 902(14). Relying upon the precedent for Rule 902(11) certificates, the Advisory Committee concluded that Rule 902(13) would not violate the Confrontation Clause because the certificate only authenticates the electronic record.[7]

For example, in *United States v. Yeley-Davis*,[8] the Tenth Circuit Court of Appeals held that a Rule 902(11) certificate authenticating phone records as business records was properly admitted over the defendant's confrontation objection:

> Justice Scalia expressly described the difference between an affidavit created to provide evidence against a defendant and an affidavit created to authenticate an admissible record . . . . In addition, Justice Scalia rejected the dissent's concern that the majority's holding would disrupt the long-accepted practice of authenticating documents under Rule 902(11) and would call into question the holding in *Ellis* [a case which had rejected a Confrontation Clause challenge to the use of Rule 902(11)]. See *Melendez-Diaz*, 129 S.Ct. at 2532 n. 1 ("Contrary to the dissent's suggestion . . . we do not hold, and it is not the case, that anyone whose testimony may be relevant in establishing the . . . authenticity of the sample . . . must appear in person as part of the prosecution's case.").[9]

Other circuits applying the *Melendez-Diaz* carve-out have held that authentication certificates do not violate the Confrontation Clause.[10]

Electronic information resulting from a process or system that produces an accurate result is not hearsay because it is not *testimonial* under *Melendez-Diaz*; the machine is not a "person" and machine-generated information is not a "statement" under Rule 801(a).[11] Similarly, the fact that machine-generated information was prepared in anticipation of litigation is not a bar to its admissibility because, unlike the lab chemist's affidavit in *Melendez-Diaz*, machine-generated information is not testimonial. However, any additional information in the form of witness testimony that interprets or explains the result may indeed be testimonial. Thus, a properly constructed certificate does not violate the Confrontation Clause. Obviously, certificates deserve careful drafting by lawyers and scrutiny by trial judges.

Limitations on what self-authentication certificates can accomplish

Whether in criminal or civil cases, Rule 902(13) certifications should be limited to authenticating the accuracy of the machine-generated *result*. They should not become a Trojan Horse for providing the fact-finder with additional information in the form of a witness's interpretation or explanation of the result.

To illustrate, consider a criminal case where the prosecution obtains a Rule 902(13) certification for a Drug Enforcement Administration lab report of a gas chromatograph test that reports a positive result for heroin and an affidavit of a lab chemist stating that, in his opinion, the sample contained heroin. The defendant makes several objections to the prosecution's evidence: The gas chromatograph report is not authentic and is hearsay, the lab chemist's opinion is hearsay, both reports violate the Confrontation Clause and are inadmissible because they were prepared in anticipation of litigation, and the Rule 902(13)

certification itself is inadmissible hearsay that violates the Confrontation Clause. We will consider each in turn.

The gas chromatograph's machine-generated report of the result, authenticated by an appropriate Rule 902(13) certification, is admissible. It is not testimonial — and not hearsay — because it is not a "statement" of a "person." For the same reason, the fact that the report was prepared in anticipation of litigation is not a bar to its admissibility.

The lab chemist's affidavit is hearsay and its admission would violate the Confrontation Clause. The court held in *Melendez-Diaz* that extra-judicial statements contained in testimonial materials, such as affidavits, depositions, prior testimony or confessions, require live testimony from the witness.

The Rule 902(13) certificate can be considered by the court for the limited purpose of the Rule 104(a) threshold determination of admissibility and made part of the record. Trial lawyers understand that when devising the right mixture of exhibits and witness testimony several strategies come into play. On the one hand, the report of the result, even coupled with the authenticity certificate, may fail to provide sufficient context and explanation of the result to be persuasive and memorable for the jury. Thus, a trial attorney might eliminate one or more purely authentication witnesses by utilizing Rule 902(13), but still call a competent witness to provide explanation and context for the result. On the other hand, if the result is either self-explanatory, not central to the case, not seriously disputed by the opposing party, or stipulated to, then the trial lawyer may conclude that the report of the result standing alone is sufficient. Thus, different trial strategies will lead lawyers to use Rule 902(13) in various ways.

> It bears noting that for some types of electronic evidence, the proponent cannot simply rely upon a Rule 902(13) certification to fully establish the authentication required by Rule 901(a). He may need to further authenticate the evidence by linking it to a particular individual to establish authorship.

Addressing allegations of tampering with electronic evidence

The speculative possibility that electronic evidence could be falsified or tampered with clearly is not a sufficient basis for an objection to authenticity.[12]

But when there are credible grounds to suspect tampering, Rule 902(13) can provide a mechanism to address them. For example, in a civil personal-injury case, plaintiff Moreno claims she suffered serious injuries to her legs from the defendant's conduct. The defendant wants to use a photograph of Moreno dancing with friends to disprove the claimed injuries; the photo's date stamp is just a few weeks after Moreno's injuries. The photo was recovered from the cell phone of Moreno's ex-husband. Moreno denies being at the photo's location on that date, and she asserts her ex-husband used Photoshop software to put her image into the photo. How does Rule 902(13) help address this issue?

The defendant may elect to utilize Rule 902(13) to authenticate the photo, in whole or in part. Because Rule 902(13) incorporates the "reasonable written notice" provisions of Rule 902(11), before the trial the defendant must give Moreno written notice of his intent to use the photo and of the basis for authenticating the photo. Under Rule 902(13), Moreno has the right to challenge the prosecution's basis for authentication. From the defendant's written notice, the court and Moreno will have a better understanding of which authentication factors are not disputed and which are disputed. It may be that Moreno does not dispute the manner in which the electronic file of the photo was collected from the phone, then the defendant can eliminate that authentication witness by using a certificate. If tampering via Photoshop is Moreno's real challenge to authenticity, then the pretrial self-authentication process will help focus the parties' dispute. Alternatively, if the defendant did not invoke Rule 902(13) before trial, then the defendant would need to call all of its authentication witnesses at trial and Moreno would make her tampering challenge at trial.

RULE 902(14)

Rule 902(14) provides litigants a mechanism to eliminate what is usually perfunctory and uncontested testimony about copying data. Data is often copied from an original storage medium — for example, the hard-drive of a computer or cell phone — in order to conduct a forensic examination without altering the contents or metadata of the original device. To preserve the original, almost all forensic examinations are conducted on copies. ▸

The software tools for verifying that the copy matches the original include several industry-standard programs. New software and methodologies are coming into the market. Rule 902(14) is designed to adapt to technology as it evolves.

Rule 902(14) is simple and straightforward. By providing a mechanism for the parties to address any authentication issues before trial, it should enable the parties to eliminate unnecessary authentication witnesses and save time and money.

CONCLUSION

New Rules 902(13) and 902(14) provide litigants with a pretrial procedure to assess whether they have a genuine dispute about the authenticity of records of results generated by an electronic process or system that produces an accurate result. Many types of computer-generated information are routinely relied upon in daily life because they are trustworthy. But the witnesses who can authenticate electronic evidence are spread across the globe, and getting them to the courthouse is one of the expensive complications that make going to trial unaffordable for many litigants. When there is not a genuine dispute about the authenticity of such information, these new rules provide litigants with the tools to eliminate uncontested authentication witness, focus on the real issues in contention, and save time and money.

[1] There are many other examples of the same types of machine-generated information built into computer operating systems, for example, internet browser histories and wifi network access logs.

[2] *See, e.g., United States v. Lizarraga-Tirado*, 789 F.3d 1107, 1109–10 (9th Cir. 2015) (finding Google Earth satellite images and stamped coordinates not statements of people); *United States v. Lamons*, 532 F.3d 1251, 1261–65 (11th Cir. 2008) (determining Sprint billing and call report data not statements of people); *United States v. Blackburn*, 992 F.2d 666, 670 (7th Cir. 1993) (determining lensometer scan of eyeglasses to determine prescription not a statement of a person).

[3] No. 14-1798, 2016 WL 4473226 (3d Cir. Aug. 25, 2016).

[4] *Id*. at *5.

[5] *Id*.

[6] *Id*. at *7.

[7] This analysis is taken from the Report of the Advisory Committee on Evidence Rules, which is available at www.uscourts.gov/file/19778/download.

[8] 632 F.3d 673 (10th Cir. 2011).

[9] *Id*. at 680–81.

[10] *See, e.g., United States v. Albino-Loe*, 747 F.3d 1206, 1211 (9th Cir. 2014) (finding no confrontation violation where the "certifications at issue here did not accomplish anything other than authenticating the A–File documents to which they were attached. In particular, they did not explicitly state anything about Albino–Loe's alienage."); *United States v. Brinson*, 772 F.3d 1314, 1323 (10th Cir. 2014) ("The prosecution presented the certificate in part to authenticate the debit card records under Federal Rule of Evidence 902(11). This rule permits a party to establish the authenticity of documents as domestic business records through a declaration from the records' custodian. . . . Mr. Brinson relies on *Melendez–Diaz v. Massachusetts* . . . There, the Supreme Court held that affidavits showing the results of a forensic analysis are testimonial statements. . . . *Melendez–Diaz* does not apply. Our certificate does not contain any "analysis" that would constitute out-of-court testimony. Without that analysis, the certificate is simply a non-testimonial statement of authenticity."). *See also Yeley–Davis*, 632 F.3d at 681 ("The Court's ruling in *Melendez–Diaz* does not change our holding that Rule 902(11) certifications of authenticity are not testimonial.")).

[11] *See, e.g., United States v. Moon*, 512 F.3d 359 (7th Cir. 2008) (determining that readings from an infrared spectrometer and a gas chromatograph did not violate *Crawford* because "data are not 'statements' in any useful sense. Nor is a machine a 'witness against' anyone.")

[12] *Lorraine v. Markel American Ins. Co.*, 241 F.R.D. 534 (D. Md. 2007) (collecting cases and analyzing authentication of electronic evidence). *See also* Hon. Paul W. Grimm, Michael V. Ziccardi, and Alexander W. Major, *Back to the Future:* Lorraine v. Markel American Insurance Co. *and New Findings on the Admissibility of Electronically Stored Information*, 42 Akron L.R. 357 (2009).

JOHN M. HARIED is Criminal eDiscovery Coordinator for the Executive Office for U.S. Attorneys, U.S. Department of Justice, and an Assistant United States Attorney for the District of Colorado in Denver. Views expressed in this article do not necessarily represent the views of the Department of Justice or the United States.