# BEST PRACTICES FOR AUTHENTICATING DIGITAL EVIDENCE

HON. PAUL W. GRIMM
*United States District Judge for the District of Maryland*
*former member of the Judicial Conference Advisory Committee on Civil Rules*

GREGORY P. JOSEPH, ESQ.
*Partner, Joseph Hage Aaronson, New York City*
*former member of the Judicial Conference Advisory Committee on Evidence Rules*

DANIEL J. CAPRA
*Reed Professor of Law, Fordham Law School*
*Reporter to the Judicial Conference Advisory Committee on Evidence Rules*

WEST ACADEMIC PUBLISHING

444 Cedar Street, Suite 700
St. Paul, MN 55101
1-877-888-1330

Printed in the United States of America

**ISBN:** 978-1-68328-471-0

# TABLE OF CONTENTS

# BEST PRACTICES FOR AUTHENTICATING DIGITAL EVIDENCE

## I. Introduction

Digital evidence is now offered commonly at trial. Examples include emails, spreadsheets, evidence from websites, digitally-enhanced photographs, PowerPoint presentations, texts, tweets, Facebook posts, and computerized versions of disputed events. Does the fact that an item is electronic raise any special challenges in authenticating that item?

In Federal Courts, authenticity is governed by Rule 901(a), which requires that to establish that an item is authentic, a proponent must produce admissible evidence "sufficient to support a finding that the item is what the proponent claims it is."[1] Rule 901(b) provides many examples of evidence that satisfies the standard of proof for establishing authenticity, including testimony of a witness with knowledge,[2] circumstantial evidence,[3] and evidence describing a process or system that shows that it produces an accurate result.[4] The standards and examples provided by Rule 901(a) and (b) are flexible enough to adapt to all forms of electronic evidence.

That does not mean that authenticating digital evidence is automatic. There are a large number of cases dealing with authentication of digital evidence over the last 15 years; and such evidence can present challenges in establishing that it has not been altered and that it comes from a certain source. The Judicial Conference Advisory Committee on Evidence Rules, surveying this case law, determined that the Bench and Bar would be well-served by a Best Practices Handbook that would provide guidance on factors that should be taken into account for authenticating each of the major new forms of digital evidence that are being offered in the courts. The idea for such a Handbook grew out of a symposium sponsored by the Advisory Committee on the challenges of electronic evidence. After that Symposium, the Reporter to the Advisory Committee began to work with two noted authorities on electronic evidence—Hon. Paul Grimm and Gregory P. Joseph, Esq. The result is this Best Practices Handbook; it is the work of the authors alone.

This Handbook begins with an analysis by Judge Grimm of the basic rules on authenticating evidence, with a focus on digital evidence and the interplay between Evidence Rules 104(a) (providing that the judge is to decide admissibility factors by a preponderance of the evidence) and Rule 104(b) (providing that for questions of conditional relevance—such as authenticity—the standard of proof for admissibility is enough evidence sufficient to support a finding).

Following Judge Grimm's introduction, Part Two of the Handbook sets forth some guidelines on authentication of the kinds of electronic evidence

---

[1] Evidence proffered to support authenticity of a challenged item must itself be admissible. See, e.g., United States v. Bonds, 608 F.3d 495 (9th Cir. 2010) (records could not be authenticated where the only basis for authentication was a hearsay statement not admissible under any exception).

[2] Fed.R.Evid. 901(b)(1).

[3] Fed.R.Evid. 901(b)(4).

[4] Fed.R.Evid. 901(b)(9).

that are most frequently offered in litigation today: 1) emails; 2) texts; 3) chatroom conversations; 4) web postings; and 5) social media postings.[5] In Part Three, we consider whether and when the proponent might argue that the court can take judicial notice of the authenticity of certain digital evidence. Finally, Part Four provides an extensive discussion of two amendments to the Federal Rules of Evidence—Rules 902(13) and (14)—scheduled to go into effect on December 1, 2017, that will ease the burden of authenticating electronic evidence.

At the outset it is important to emphasize that the standard for establishing authenticity of digital evidence is the same mild standard as for traditional forms of evidence. None of the checklists set forth below are going to be required to be met *in toto* before digital evidence is found authentic. They are just relevant factors, and usually satisfying one or two of any of the listed factors will be enough to convince the court that a juror could find the digital evidence to be authentic. But the factors will need to be applied case-by-case.

## II. An Introduction to the Principles of Authentication for Electronic Evidence: The Relationship Between Rule 104(a) and 104(b)

This Handbook is designed to provide answers to the fundamental evidentiary questions of how to authenticate digital evidence. But before turning to the authentication rules themselves, there are two preliminary rules that must be discussed and understood, because without them, authentication decisions are apt to be erroneous. These rules are Fed.R.Evid. 104(a) (which states the general rule governing preliminary questions about the admissibility of evidence) and Fed.R.Evid. 104(b) (the so-called "conditional relevance" rule[6]). Understanding these two rules is essential to making correct decisions about the authentication of digital evidence.

We start with Rule 104(a). Its text is deceptively straightforward: "[t]he 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." (emphasis added). Most decisions about admissibility of evidence, whether digital or otherwise, are made by the judge alone. They include decisions about whether evidence is relevant, constitutes hearsay (or fits within one of the many hearsay exceptions), or is excessively prejudicial when compared to its probative value, whether experts are qualified and the extent of opinion testimony that will be allowed, and most questions regarding application of the original writing rule. When the judge makes a ruling under Rule 104(a) he or she is the sole decision maker as to whether the evidence may be heard by the jury. If admitted, of course, the jury is free to give the evidence whatever weight (if any) they think it deserves. This is familiar turf to trial judges, but with

[5] This Best Practices Handbook covers the relatively new forms of electronic communications. Parties have been authenticating more traditional forms of electronic evidence for many years—examples include telephone conversations, audiotapes, and video recordings. See, e.g., United States v. Taylor, 530 F.2d 639 (5th Cir. 1976). (video evidence from a bank security camera was properly authenticated where testimony revealed the camera was present on the day in question and was facing the events of an armed robbery, and was functioning properly). This pamphlet does not cover such traditional forms of electronic communication. For more on authentication of such information, see Saltzburg, Martin & Capra, Federal Rules of Evidence Manual § 901 (11th ed. 2015), which provides relevant case law and commentary.

[6] Fed.R.Evid. 104(b) (1972) Advisory Note.

digital evidence, there is a greater likelihood that the judge alone may not be the final decision maker regarding admissibility. The jury also may have a part to play in the admissibility decision, and this is where Rule 104(b) comes in.

Rule 104(b) qualifies Rule 104(a). It provides "[w]hen 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." Read in isolation, Rule 104(b) seems too abstract to be helpful. But, in the case of disputes over the authenticity of digital evidence, it can be an important qualifier to the general rule of 104(a) that the trial judge decides questions about the admissibility of evidence. An illustration will help bring things into focus. Imagine the following variations of a common theme. In an employment discrimination case the plaintiff, a woman, alleges that her supervisor, a man, intentionally discriminated against her in deciding to promote a lesser qualified man to a position that the plaintiff sought. As evidence of intentional discrimination, the plaintiff wants to introduce an email that she asserts her supervisor sent to her that says: "Jane, stop bugging me about the sales supervisor position. Your track record compared to the men in our sales group is terrible, and confirms what I always have suspected. Women just don't have the stuff it takes to get out there and sell our products. You should be glad you still have your sales job, and quit trying to be something you can never do well. Bob." The email is from the company email account (Bob@company.com), addressed to the plaintiff (Jane@company.com), apparently signed by the supervisor (Bob), discusses a subject matter about which the supervisor has knowledge, and is dated on a day and time the supervisor was known to be at the office. Plaintiff contends that the email is "smoking gun" evidence of intentional gender discrimination.

Imagine further the following scenarios when the plaintiff offers the email into evidence at trial. One: the defense attorney objects to the introduction of the email, the judge asks for the basis of the objection, and the defense attorney says "inadequate foundation". Two: the defense attorney objects, the judge asks for the basis of the objection, and the defense attorney says "Judge, this is an email, there is no evidence that the supervisor was the one who actually wrote it. It was found on a company computer, anyone in the company had access to that computer, including the plaintiff herself, whose office was right next to his, and my client is often away from his desk during the day, and he does not log out of his computer. Plaintiff hasn't shown that someone else didn't send that email pretending to be my client, and everyone knows how easy it is to fake an email." Three: the defense attorney objects, the judge asks for the basis of the objection, and the defense attorney says "Judge, my client will testify that on the day and time stated on the email he was at a sales meeting with the other supervisors and the president of the company. Five other people saw him there at that day and time and will testify that they did. During those meetings, no one is allowed to use their smart phone or to send or receive emails, on pain of being fired if the president sees them looking at their phones. The location of the meeting was on a different floor from where my client and the plaintiff work. He will testify that he did not send the email, and that when he leaves his office he does not log out, his computer stays on, and anyone can access it without a password and use his office email account. He also will testify that when he came back from the meeting, the plaintiff looked at him in a strange way, and said "I wouldn't look so smug if I were you. You might not be that way for very long."

With these scenarios in mind, what is the interplay between Rule 104(a) and 104(b) in determining whether the email may be admitted at trial and considered by the jury? In the first scenario, no explanation was given by the defense attorney for excluding the email other than the conclusory statement that the plaintiff had not laid a sufficient foundation. Here, the trial judge alone decides, under Rule 104(a), whether an adequate foundation has been established. If the foundation was deficient, the judge will require the plaintiff's lawyer to make a fuller showing, and allow or exclude the email accordingly. Rule 104(b) is not implicated.

In the second scenario, the defense attorney has made a conclusory legal argument that provides no facts showing that the supervisor did not author the email, but rather speculates that it *could have* been written by someone else. The argument invites the trial judge to require the plaintiff's lawyer to "prove a negative"—that no one but the supervisor was the author. But this is not the burden that the plaintiff must meet under Rule 104(a) to establish the admissibility of the email. Rather, all that plaintiff must do is to meet the obligation imposed by Rule 901(a), which is to "produce evidence sufficient to support a finding that the item is what the proponent claims it is." Certainty is not required. All that is needed is evidence sufficient to convince a reasonable juror that, more likely than not, the email is what the plaintiff claims it is—an email her supervisor drafted. And, under the hypothetical facts of the second scenario, the defense counsel is wrong in saying the plaintiff has offered no evidence that the email came from the supervisor. She has shown that the email came from the supervisor's email address, on the company email server, on a day when the supervisor was at the office, discussing a topic about which the supervisor had knowledge, and is signed with his name. Certainly this would be an example of authentication under Rule 901(b)(4), where the "appearance, contents, substance . . . or other distinctive characteristics of the item, taken together with all the circumstances" tend to show that the supervisor authored the email.

The second scenario also raises only Rule 104(a) issues for the trial judge alone to determine admissibility. The facts, under which admissibility must be judged, are undisputed. If the trial judge concludes (as she should under these facts) that a reasonable juror *could* find from the foundation presented that it is more likely than not that the supervisor wrote the email, it is admissible. Defense counsel's speculation about what "could" have happened is reserved for argument to the jury about how much weight (if any) to give to the email. Absent from scenario two is evidence that the supervisor in fact did not author the email, to contradict the undisputed facts introduced by the plaintiff regarding the distinctive characteristics of the email that associate it with the supervisor.

Scenario three does introduce facts contradicting the evidence the plaintiff introduced about the distinctive characteristics of the email tying it to the supervisor. The defense attorney has proffered that he will introduce evidence (the supervisor, the five witnesses who corroborate that he was with them at the time the email was sent, the policy prohibiting use of cell phones during meetings with the company president, the meeting's location on a different floor of the building). Now the trial judge is presented with competing evidence that the supervisor did, and did not, author the email. If the plaintiff's evidence is accepted over that of the defendant, then it is more likely than not that the supervisor is the author, and the email is relevant to show his discriminatory intent. But, if the defendant's version of the facts is accepted over those offered by the plaintiff, then the supervisor did not author the email, and it is irrelevant to prove his state of mind. The relevance of the

email turns on whether the plaintiff's version or the defendant's version is accepted, and this falls squarely within the scope of Rule 104(b). The relevance of the email depends on the existence of a disputed fact—authorship of the email. Who decides between the competing versions? If the case is tried before a jury, it is the jury, not the judge, who must resolve the dispute.[7] The judge's role under Rule 104(a) is to evaluate whether a reasonable jury *could* find (more likely than not) either that the supervisor did, or did not, author the email. If either version is plausible, then the judge conditionally admits the email, but at the time it is introduced instructs the jury that if they find that the plaintiff has shown that the supervisor more likely than not authored the email, they may consider it as evidence and give it the weight that they feel it is entitled to. Contrastingly, if they find that the defendant has persuaded them that, more likely than not, he did not author the email, they must disregard it entirely, and give it no weight in their deliberations. The final decision about whether the email has been admitted (and can be considered by the jury) or excluded (and disregarded by the jury) must await the jury's deliberation on the merits of the case. The judge makes a preliminary assessment of whether the evidence is one-sided or two, and if the latter, submits it to the jury for their decision. The issue of conditional relevance generated by disputed facts regarding the authenticity (and hence, relevance) of evidence is especially prevalent with digital evidence.

It is important for judges to distinguish between which of the scenarios listed above is presented to them when ruling on admissibility of digital evidence. For scenario one situations, the judge alone decides whether the proponent has laid a proper foundation to authenticate the digital evidence. Most often, the judge will consider whether one or more of the illustrations of how to authenticate found at Fed.R.Evid. 901(b)[8] or 902[9] has been shown.

---

[7] Fed.R.Evid. 104(b) (1972) Advisory Note ("If preliminary questions of conditional relevancy were determined solely by the judge, as provided in subdivision (a), the functioning of the jury as a trier of fact would be greatly restricted and in some cases virtually destroyed. These are appropriate questions for juries. Accepted treatment, as provided in the rule, is consistent with that given fact questions generally. The judge makes a preliminary determination whether the foundation evidence is sufficient to support a finding of fulfillment of the condition. If so, the item is admitted. If after all the evidence on the issue is in, pro and con, the jury could reasonably conclude that fulfillment of the condition is not established, the issue is for them. If the evidence is not such as to allow a finding, the judge withdraws the matter from their consideration.").

[8] For digital evidence, the most useful authentication rules within Rule 901(b) are: 901(b)(1) (a witness with personal knowledge that the evidence is what it purports to be); 901(b)(3) (comparison of the evidence with an authenticated specimen by an expert witness or the finder of fact); 901(b)(4) (the appearance, contents, substance, internal patterns or other distinctive characteristics of the item, taken together with all the circumstances); 901(b)(5) (for audio recordings, an opinion identifying a person's voice, whether heard firsthand or through electronic transmission or recording, based on having heard that voice in the past); and 901(b)(9) (evidence describing a process or system of showing that it produces an accurate result).

[9] Fed.R.Evid. 902 provides examples of self-authentication, where no extrinsic evidence or testimony is needed to authenticate. The following self-authentication rules may be helpful for digital evidence; 902(5) (A book, pamphlet, or other publication purporting to be issued by a public authority. Most public authorities have web sites and post publications relating to their fields of jurisdiction.); 902(6) (Printed material purporting to be a newspaper or periodical. Most newspapers and periodicals have "on line editions", and this rule potentially is available to self-authenticate.); 902(11) and (12) (certified copy of domestic and foreign records of regularly conducted activities); proposed Rule 902(13) (certified copy of machine-generated information); and proposed Rule 902(14) (certified copy

For scenario two situations, the judge alone makes the decision whether to admit or exclude. In doing so, he must be careful not to let unparticularized and conclusory argument by the party objecting to the introduction of the digital evidence about what "might" or "could have happened" lead him to impose on the proponent of the evidence a burden of proof greater than that ordinarily required by Rule 104(a)—a showing that the evidence more likely than not is what it purports to be. It is a mistake for a judge to require the party introducing digital evidence to prove that no one other than the purported maker could have created the evidence if the introducing party has shown that, more likely than not, it was created by a particular person, unless there is evidence (not argument) that some other person could have done so.[10] Finally, for scenario three situations, where the judge is faced with competing facts plausibly showing that the digital evidence was, and was not, created by the person claimed by the proponent, then she should allow the evidence to be admitted "conditionally" under Rule 104(b), and instruct the jury that if they find that the evidence that the person claimed to have created the evidence did not do so is more believable than the evidence that he did, they must disregard it and give it no weight in their deliberations.

Careful attention to the interplay between Rule 104(a) and 104(b), as well as consideration of the abundant authentication tools identified in Rules 901(b) and 902, will go a long way towards removing the mystery about authenticating digital evidence, even when the technology at play is unfamiliar to the judge. In the end, technical expertise is not needed. Rather, an awareness of the fundamental evidence rules governing admissibility and authentication of any evidence, whether digital or not, is all that is needed. And this Handbook aims to provide illustrations to make the effort even easier.

## III. Relevant Factors for Authenticating Digital Evidence

What follows are general guidelines and lists of relevant factors for authenticating the basic forms of digital evidence that have developed over the last 20 years. The lists of relevant factors do not purport to be exclusive. There is no attempt to weigh the factors, or to take a cumulative approach, as the importance of any factor will be case-dependent. And there is no intent to imply that all of the factors listed must be met before the proffered digital evidence can be found authentic.

In evaluating all the factors below, it is important to remember that the threshold for the court's determination of authenticity under Rule 901 is not high: "the court need not find that the evidence is necessarily what the proponent claims, but only that there is sufficient evidence that the jury ultimately might do so." [11] The possibility of alteration "does not and cannot be the basis for excluding ESI as unauthenticated as a matter of course, any more that it can be the rationale for excluding paper documents."[12]

---

of computer generated or stored information). Authentication under Rules 902(13) and (14) is discussed in a separate section, infra.

[10] Grimm, et al, *Authentication of Social Media Evidence*, 36 American Journal of Trial Advocacy 433, 459 (2013) ("A trial judge should admit the evidence if there is plausible evidence of authenticity produced by the proponent of the evidence and only speculation or conjecture—not facts—by the opponent of the evidence about how, or by whom, it 'might' have been created.").

[11] United States v. Safavian, 435 F. Supp. 2d 36, 38 (D.D.C. 2006).

[12] *Id.* at 40.

Generally speaking, it will be a rare case in which an item of digital evidence *cannot* be authenticated. The question is whether the proponent is willing and able to expend the resources necessary to do so.[13] The factors set forth below are intended to direct litigants to ways in which resources can be usefully spent on authenticating digital evidence—and on ways to avoid such costs in certain situations.

## *A. Emails*

The authentication questions for email most commonly focus on whether the email was sent or received by the person whom the party claims sent or received it. There are a number of factors that will assist the proponent in establishing authenticity for either or both of these purposes. Among them are:

### 1. A Witness with Personal Knowledge May Testify to Authenticity[14]

Possibilities include:

- The author of the email in question testifies to its authenticity.[15]
- A witness testifies that s/he saw the email in question being authored/received by the by the person who the proponent claims authored/received it.[16]

### 2. Business Records

The custodian of records of a regularly conducted activity testifies to a foundation, or certifies, in accordance with Fed.R.Evid. 902(11) or (12), that an email satisfies the criteria of Fed.R.Evid. 803(6). It should be noted, however, that emails—even of a business, do not automatically qualify as business records.[17]

---

[13] *See* Jeffrey Bellin and Andrew Guthrie Ferguson, *Judicial Notice in the Information Age,* 108 Nw. U. L.Rev. 1137, 1157 (2014) ("Although much is made of [the authentication] hurdle in the Information Age, it is * * * an easy one to surmount. Success generally depends not on legal or factual arguments, but rather the amount of time and resources a litigant devotes to the problem.")

[14] See Fed.R.Evid. 901(b)(1).

[15] See, e.g., Anderson v. United States, 2014 U.S. Dist. LEXIS 166799, at *13 (N.D. Ga. Dec, 2, 2014) (defendant-witness acknowledged that the documents in question contained emails he sent to an undercover agent, the emails were sent from his email address, and the document contained the entirety of his email exchange with the undercover agent; this was a sufficient showing of authenticity). See also Citizens Bank & Trust v. LPS Nat'l Flood, LLC, 2014 U.S. Dist. LEXIS 134933, at *12 (N.D. Ala. Sept. 25, 2014) (witness's personal knowledge of email contents and her affidavit authenticating emails as the ones she sent sufficient for admissibility).

[16] United States v. Fluker, 698 F.3d 988 (7th Cir. 2012) (the court, in outlining the variety of ways in which an email could be authenticated, stated that testimony from a witness who purports to have seen the declarant create the email in question was sufficient for authenticity under Rule 901(b)(1)).

[17] See, e.g., United States v. Cone, 714 F.3d 197, 220 (4th Cir. 2013):

> While properly authenticated e-mails may be admitted into evidence under the business records exception, it would be insufficient to survive a hearsay challenge simply to say that since a business keeps and receives e-mails, then ergo all those e-mails are business records falling within the ambit of Rule 803(6)(B). "An e-mail created within a business entity does not, for that reason alone, satisfy the business records exception of the hearsay rule." Morisseau v. DLA Piper, 532 F. Supp. 2d 595, 621 n. 163 (S.D.N.Y. 2008).

### 3. Jury Comparison with Other Authenticated Emails[18]

The authenticity of an email can be determined by the trier of fact by comparing the email in question with emails already authenticated and in evidence.[19]

### 4. Production in Discovery

If a document request is sufficiently descriptive, production in response to that request may serve in itself to authenticate the email, as the act of production may be a concession that the document is what the party asked for—and thus is what the party says it is. The act of production can constitute a statement of a party-opponent and consequently admissible evidence of authenticity. See Fed.R.Evid. 801(d)(2).[20] Authentication has also been found when an adversary produces in discovery a third party's email received by the producing party in the ordinary course of business, and the email is offered against the adversary.[21]

### 5. Circumstantial Evidence[22]

Applying Rule 901(b)(4)—covering authentication on the basis of "appearance, contents, substance, internal patterns, or other distinctive characteristics of the item"—requires consideration of the "totality of circumstantial evidence."[23] While any one factor *may* be insufficient to determine admissibility, when weighed together, authenticity may be established. "This rule is one of the most frequently used to authenticate e-mail and other electronic records."[24]

Set forth below are factors that can, alone or in conjunction (depending on the case), establish authenticity. Different circumstantial factors may be relevant depend on whether the authenticity dispute is over whether a person sent or received the email.

---

It is probably fair to state that emails and social media postings will often be prepared too casually and irregularly to be admissible as business records. But this is not inevitably so, and again if the electronic communication does fit the admissibility requirements it is just as admissible as a hardcopy record.

[18] Fed.R.Evid. 901(b)(3).

[19] United States v. Safavian, 435 F. Supp. 2d 36, 40 (D.D.C. 2006) ("Those emails that are not clearly identifiable on their own can be authenticated under Rule 901(b)(3), which states that evidence may be authenticated by the trier of fact with 'specimens which have been authenticated'—in this case those emails that have been independently authenticated.").

[20] See, e.g., AT Engine Controls Ltd. v. Goodrich Pump & Engine Control Sys., Inc., 2014 U.S. Dist. LEXIS 174535 (D. Conn. Dec. 18, 2014) (collecting cases holding that production of emails in discovery constitutes a concession of authenticity); Nola Fine Art, Inc. v. Ducks Unlimited, Inc., 2015 U.S. Dist. LEXIS 17450 (E.D. La. Feb. 12, 2015) ("[Defendant] produced the email to plaintiffs in discovery and therefore cannot seriously dispute the email's authenticity").

[21] Broadspring, Inc. v. Congoo, LLC, 2014 U.S. Dist. LEXIS 177838 (S.D.N.Y. Dec. 29, 2014) (third party emails sent to a party in the ordinary course of business and produced by the party in litigation are sufficiently authenticated by the act of production when offered by an opponent, but hearsay and other admissibility objections as to the third parties' statements must separately be satisfied).

[22] Fed.R.Evid. 901(b)(4).

[23] United States v. Henry, 164 F.3d 1304, 1305 (10th Cir. 1999).

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

### a. Authenticating Authorship Circumstantially

***The inclusion of some or all of the following in an email can be sufficient to authenticate the email as having been sent by a particular person:***

- the purported author's known email address;[25]
- the author's electronic signature;
- the author's name;[26]
- the author's nickname; [27]
- the author's screen name;
- the author's initials;
- the author's moniker;[28]
- the author's customary use of emoji or emoticons;
- the author's use of the same email address elsewhere;
- a writing style similar or identical to the purported author's manner of writing;
- reference to facts only the purported author or a small subset of individuals including the purported author would know;[29]
- reference to facts uniquely tied to the author—*e.g.*, contact information for relatives or loved ones; photos of the author or items of importance to the author (e.g., car, pet); the author's personal information, such as a cell phone number, social security number, etc.[30]

[25] See. e.g., United States v. Siddiqui, 235 F.3d 1318, 1322 (11th Cir. 2000) (an email identified as originating from the defendant's email address and that automatically included the defendant's address when the reply function was selected was considered sufficiently authenticated).

[26] See, e.g., United States v. Fluker, 698 F.3d 988, 999–1000 (7th Cir. 2012) (emails sent from a "More Than Enough, LLC" (MTE) email address were sufficiently authenticated when the purported author was an MTE board member and "[i]t would be reasonable for one to assume that an MTE Board member would possess an email address bearing the MTE acronym."); *Safavian*, 435 F. Supp. 2d at 40 (email messages held properly authenticated when containing distinctive characteristics, including email addresses and name of the person connected to the address).

[27] United States v. Brinson, 772 F.3d 1314 (10th Cir. 2014) (use of fake name commonly used by defendant).

[28] See United States v. Simpson, 152 F.3d 1241 (10th Cir. 1998) (chatroom log where user "Stavron" identified himself as the defendant and shared his email address was used to authenticate subsequent emails from that email address).

[29] See United States v. Siddiqui, 235 F.3d 1318, 1322 (11th Cir. 2000) (messages that referred to facts only the defendant was familiar with were ruled admissible).

[30] Commonwealth v. Amaral, 78 Mass. App. Ct. 671, 674–675, 941 N.E.2d 1143, 1147 (2011) ("In other e-mails, Jeremy provided his telephone number and photograph. When the trooper called that number, the defendant immediately answered his telephone, and the photograph was a picture of the defendant. These actions served to confirm that the author of the e-mails and the defendant were one and the same") (citing Mass. G. Evid. § 901(b)(6)).

***Factors outside the content of the email itself can establish authenticity of authorship circumstantially. For example:***

- a witness testifies that the author told him to expect an email prior to its arrival;[31]
- the purported author acts in accordance with, and in response to, an email exchange with the witness;
- the author orally repeats the contents soon after the email is sent;
- the author discusses the contents of the email with a third party;
- the author leaves a voicemail with substantially the same content.

***Forensic information may be used to support a circumstantial showing that the email was sent by the purported author. Forensic sources include:***

- an email's hash values;[32]
- testimony from a forensic witness that an email issued from a particular device at a particular time.[33]

### b. Authenticating Receipt Circumstantially

***The following factors can be probative in authenticating an email as having been received by a particular person:***

- a reply to the email was received by the sender from the email address of the purported recipient;
- the subsequent conduct of the recipient reflects his or her knowledge of the contents of the sent email;
- subsequent communications from the recipient reflects his or her knowledge of the contents of the sent email;
- the email was received and accessed on a device in the possession and control of the alleged recipient.

---

[31] State v. Ruiz, 2014 Mich. App. LEXIS 855 (Mich. Ct. App. May 15, 2014) (interpreting MRE 901) (witness testified to knowing the defendant authored an email because the defendant told him to expect an email relating to arson—the contents of the email subsequently received).

[32] A hash value is "[a] unique numerical identifier that can be assigned to a file, a group of files, or a portion of a file, based on a standard mathematical algorithm applied to the characteristics of the data set. The most commonly used algorithms, known as MD5 and SHA, will generate numerical values so distinctive that the chance that any two data sets will have the same hash value, no matter how similar they appear, is less than one in one billion. 'Hashing' is used to guarantee the authenticity of an original data set and can be used as a digital equivalent of the Bates stamp used in paper document production." Federal Judicial Center, Managing Discovery of Electronic Information: A Pocket Guide for Judges, Federal Judicial Center, 2007 at 24. See also Lorraine v. Markel American Ins. Co, 241 F.R.D. 534, 547 (D. Md. 2007) (noting that "[h]ash values can be inserted into original electronic documents when they are created to provide them with distinctive characteristics that will permit their authentication under Rule 901(b)(4).").

[33] *Lorraine,* 241 F.R.D. 534 at 547–48 (because an electronic message's metadata (including an email's metadata) can reveal when, where, and by whom the message was authored, the court found it could be used to successfully authenticate a document under 901(b)(4)).

Finally, while it is true that an email may be sent by anyone who, with a password, gains access to another's email account, similar questions (of possible hacking) could be raised with traditional documents. Therefore, there is no need for separate rules of authenticity for emails. And importantly, the mere fact that hacking, etc., is possible is not enough to exclude an email or any other form of digital evidence. If the mere possibility of electronic alteration were enough to exclude the evidence, then no digital evidence could ever be authenticated.[34]

### *B. Text Messages*

Text messages are not different in kind from email and so the rules and guidelines on authentication are similar. Here are some of the relevant factors for authenticating text messages:[35]

#### 1. A Witness with Personal Knowledge May Testify to Authenticity

Possibilities include:

- The author of the text in question testifies to its authenticity.
- A witness testifies that s/he saw the text in question being authored/received by the person who the proponent claims authored/received it.[36]

#### 2. Jury Comparison with Other Authenticated Texts

#### 3. Production in Discovery

#### 4. Establishing That an Electronic System of Recordation Records Accurately

This process of illustration, authorized by Fed.R.Evid. 901(b)(9), can be useful if the objection to authenticity is that the original text has been altered in some way. For example, in *United States v. Kilpatrick*, 2012 U.S. Dist. LEXIS 110166 (E.D. Mich. Aug. 7, 2012), the government sought to authenticate text messages sent from two SkyTel pages, each belonging to one of the defendants respectively. A SkyTel records-custodian verified that the text messages the government offered had not been and could not be edited in any way because when the messages are sent from the devices belonging to the defendants, they are automatically saved on SkyTel's server with no capacity for editing. The court ruled that this showing was sufficient,

[34] See, e.g., Interest of F.P., 878 A.2d 91 (Pa. Super. 2005) (just as an email can be faked, a "signature can be forged; a letter can be typed on another's typewriter; distinct letterhead stationary can be copied or stolen. We believe that e-mail messages and similar forms of electronic communication can be properly authenticated within the existing framework of Pa. R.E. 901 and Pennsylvania case law.").

[35] The case law cited under the various factors discussed in the section on emails should be equally useful as supportive citations for the similar (or identical) factors supporting authentication of texts.

[36] United States v. Barnes, 803 F.3d 209 (5th Cir. 2015) (government laid a proper foundation to authenticate Facebook and text messages as having been sent by the defendant; the defendant was a quadriplegic, but the witness who received the messages testified she had seen the defendant use Facebook, she recognized his Facebook account, and the Facebook messages matched the defendant's manner of communicating: "[a]lthough she was not certain that Hall [the defendant] authored the messages, conclusive proof of authenticity is not required for admission of disputed evidence").

under Fed.R.Evid. 901(b)(9), to establish authenticity over a claim that the messages had been altered.

It should be noted that the showing as to the process or system in *Kilpatrick* will be able to be made by a certificate of the foundation witness—substituting for live testimony—under an amendment to the Evidence Rules that is scheduled to take effect on December 1, 2017.[37]

### 5. Circumstantial Evidence

#### a. Authenticating Authorship Circumstantially

***The inclusion of some or all of the following in a text can be sufficient to authenticate the text as having been sent by a particular person:***

- the purported author's ownership of the phone or other device from which the text was sent;[38]
- the author's possession of the phone;
- the author's known phone number;
- the author's name;
- the author's nickname;[39]
- the author's initials;
- the author's moniker;
- the author's name as stored on the recipient's phone;
- the author's customary use of emoji or emoticons;
- the author's use of the same phone number on other occasions;
- a writing style similar or identical to the purported author's manner of writing;
- reference to facts only the purported author or a small subset of individuals including the purported author would know;
- reference to facts uniquely tied to the author—*e.g.*, contact information for relatives or loved ones; photos of author or items of importance to author (e.g., car, pet); author's personal information, such as contact information, social security number, etc.; receipt of messages addressed to the author by name or reference.[40]

---

[37] The proposed amendments would add two new subdivisions to Rule 902, which provides for various forms of self-authentication. See Section IV, infra, for a full discussion of the use to which these new proposals can be put.

[38] United States v. Mebrtatu, 543 F. App'x 137, 140–141 (3d Cir. 2013) (phone was in the purported sender's possession; phone contains texts sent to and signed with the purported author's first name, including texts from her boyfriend professing love and other texts whose content links them to her; texts sufficiently authenticated as hers).

[39] United States v. Kilpatrick, 2012 U.S. Dist. LEXIS 110166, at *11 (E.D. Mich. Aug. 7, 2012)(the court outlined a number of distinctive characteristics that established the authenticity of the pager and cellphone text messages at issue; among these factors were the defendants' use of their names (Kilpatrick) and nicknames ("Zeke" or "Zizwe") to sign the messages they sent).

[40] United States v. Benford, 2015 U.S. Dist. LEXIS 17046, at *16–*17 (W.D. Okla. Feb. 12, 2015) (in establishing that text messages from a device were authored by the defendant, the prosecution pointed to evidence that contact information for the defendant's brother and girlfriend were saved on the phone and that incoming messages addressed the defendant by name); United States v. Ellis, 2013 U.S. Dist. LEXIS 73031, at *3–*4 (E.D. Mich. May

***Factors outside the content of the text itself can establish authenticity of authorship circumstantially. For example:***

- a witness testifies that the author told him to expect a text message prior to its arrival;
- the purported author acts in accordance with a text exchange;
- the purported author orally repeats the contents soon after the text message is sent or discusses the contents with a third party.

#### b. Authenticating Receipt Circumstantially

***The following factors can be probative in authenticating a text as having been received by a particular person:***

- a reply to the text message was received by the sender from the purported recipient's phone number;
- the subsequent conduct of the recipient reflects his or her knowledge of the sent message's contents;
- subsequent communications from the recipient reflect his or her knowledge of the contents of the sent text message;
- the text message was received and accessed on a device in the possession and control of the alleged recipient.

### *C. Chatroom and Other Social Media Conversations*

By definition, chatroom postings and other social media communications are made by third parties, not the owner of the site. Further, chatroom participants usually use screen names (pseudonyms) rather than their real names. Thus the authenticity challenge is to provide enough information for a juror to believe that the chatroom entry or other social media communication is made by a particular person.

Simply to show that a posting appears on a particular user's webpage is insufficient to authenticate the post as one written by the account holder. Third party posts, too, must be authenticated by more than the names of the purported authors reflected on the posts. Evidence sufficient to attribute a social media or chat room posting to a particular individual may include, for example:

- testimony from a witness who identifies the social media account as that of the alleged author, on the basis that the witness on other occasions communicated with the account holder;
- testimony from a participant in the conversation based on firsthand knowledge that the transcript fairly and accurately captures the conversation;[41]

23, 2013) (the defendant's possession of a cellphone that received messages addressed to him by name or moniker was, among other circumstantial evidence (such as his possession of the device), sufficient to establish that he was the author of outgoing text messages from the same phone).

[41] See, e.g., United States v. Lebowitz, 676 F.3d 1000 (11th Cir. 2012) (internet chat authenticated by credible testimony of one participant); United States v. Lundy, 676 F.3d 444 (5th Cir. 2012) (testimony by one party to chat that the chats are as he recorded them is enough to meet the low threshold for authentication); United States v. Barlow, 568 F.3d 215, 220 (5th Cir. 2009) ("English, as the other participant in the year-long 'relationship,'

- evidence that the purported author used the same screen name on other occasions;
- evidence that the purported author acted in accordance with the posting (*e.g.*, when a meeting with that person was arranged in a chat room conversation, he or she attended);
- evidence that the purported author identified himself or herself as the individual using the screen name;
- an admission that the computer account containing the chat is that of the purported author;[42]
- use in the conversation of the customary signature, nickname, or emoticon associated with the purported author;
- disclosure in the conversation of particularized information that is either unique to the purported author or known only to a small group including the purported author;
- evidence that the purported author had in his or her possession information given to the person using the screen name;
- evidence from the hard drive of the purported author's computer reflecting that a user of the computer used the screen name in question;
- evidence that the chat appears on the computer or other device of the account owner and purported author;
- evidence that the purported author elsewhere discussed the same subject matter.

### *Authentication as Business Records?*

Note that an attempt to authenticate social media messaging as business records will, of necessity, be limited to the timestamps, metadata, etc. maintained by the owner. The content of the messages themselves will not qualify as business records and accordingly cannot be authenticated as business records under Rule 902(11). For example, in *United States v. Browne,* 2016 U.S. App. LEXIS 15668 (3rd Cir.), the government contended that Browne engaged in incriminating conversations over Facebook Messenger. The government sought to authenticate the records with a certificate of a records custodian of Facebook. The custodian certified that the records "were made and kept by the automated systems of Facebook in the course of regularly conducted activity as a regular practice of Facebook." The court held correctly that this showing was insufficient to authenticate the messages as having come from the defendant—whether the defendant made the communications involved another level of hearsay, and the custodian had no personal knowledge of the authorship of the messages. Thus, the certificate could authenticate only the fact of that the message was sent at a certain time from one address to another.

---

had direct knowledge of the chats. Her testimony could sufficiently authenticate the chat log presented at trial").

[42] United States v. Manley, 787 F.3d 937, 942 (8th Cir. 2014) ("the government presented testimony of a law enforcement officer who helped to execute the search warrant, and the officer testified that the defendant admitted adopting the username 'mem659' for his computer account. The username for his computer account was the same one used in some of the chats.").

The *Browne* court held, however, that any in admitting the records with an inadequate authentication was harmless, because there was sufficient extrinsic evidence to authenticate Browne as the author of the messages: the people that he communicated with testified at trial consistently with the communications; Browne "made significant concessions that served to link him to the Facebook conversations"; the content of the conversation indicated facts about the sender that linked to Browne; and the government "supported the accuracy of the chat logs by obtaining them directly from Facebook and introducing a certificate attesting to their maintenance by the company's automated systems."

### *D. Internet, Websites, etc.*

Websites present authenticity issues because they are dynamic. If the issue is what is on the website at the time the evidence is being proffered, then there are no authenticity issues because the court and the parties can simply access the site and see what the website says.[43] But proving up historic information on the website raises the issue of whether the information was actually posted as the proponent says it was.[44]

#### 1. Rule 901 Authentication Standards as Applied to Dynamic Website Information

In applying Rule 901 authentication standards to website evidence, there are three questions that must be answered:

- What was actually on the website?
- Does the exhibit or testimony accurately reflect it?
- If so, is it attributable to the owner of the site?

A sufficient showing of authenticity of dynamic website information is usually found if a witness testifies—or certifies in compliance with a statute or rule—that:

- the witness typed in the Internet address reflected on the exhibit on the date and at the time stated;
- the witness logged onto the website and reviewed its contents; and
- the exhibit fairly and accurately reflects what the witness perceived.[45]

---

[43] Jeffrey Bellin & Andrew Guthrie Ferguson, *Trial by Google: Judicial Notice in the Information Age*, 108 Nw. U.L.Rev. 1137, 1157 (2014) ("It is hard to imagine many good faith disputes about whether proffered evidence really is a page from Google Maps or WebMD. Malfeasance would be foolish. The opposing party can simply go to the website to verify its authenticity, and if fraud is detected, the consequences for the offering party are dire."). See also Wells Fargo Bank, N.A. v. Wrights Mill Holdings, LLC, 2015 U.S. Dist. LEXIS 115610, at*21–22 (S.D.N.Y. Aug. 31, 2015) (confirming that authenticity of existing website information could be determined by conducting a "basic Internet search.").

[44] See, e.g., Adobe Sys. v. Christenson, 2011 U.S. Dist. LEXIS 16977, at *29 (D. Nev. Feb. 7, 2011) ("[a]lthough Defendants can probably determine, with little difficulty, whether a current Google search for the search terms 'software surplus' provides links on the first page [of a website], this would not prove that such a search would have resulted in such a link at a prior point in time.").

[45] See, e.g., Estate of Konell v. Allied Prop. & Cas. Ins. Co., 2014 U.S. Dist. LEXIS 10183 (D. Or. Jan. 28, 2014) ("To authenticate a printout of a web page, the proponent must offer evidence that: (1) the printout accurately reflects the computer image of the web page as of a specified date; (2) the website where the posting appears is owned or controlled by a particular person or entity; and (3) the authorship of the web posting is reasonably

The exhibit should bear the Internet address and the date and time the webpage was accessed and the contents downloaded.[46]

***When evaluating the proffer, the court may consider the following factors as circumstantial indications that the information was posted by the owner of the site, under Rule 901(b)(4):***

- distinctive website design, logos, photos, or other images associated with the website or its owner;[47]
- the contents of the webpage are of a type ordinarily posted on that website or websites of similar people or entities;
- the owner of the website has elsewhere published the same contents, in whole or in part;
- the contents of the webpage have been republished elsewhere and attributed to the website; and
- the length of time the contents were posted on the website.

***Other possible means of authenticating website postings are as follows:***

- testimony of a witness who created or is in charge of maintaining the website. That witness may testify on the basis of personal knowledge that the printout of a webpage came from the site.[48]
- a printout obtained from the Internet Archive's "wayback machine." The Internet Archive documents and stores all websites and the "wayback machine" can retrieve website information from any particular time.[49] Some courts require a witness from the Internet archive to testify to establish that the "wayback machine" employs a process that produces accurate results under Rule 901(b)(9).[50] Other courts, as discussed infra, take judicial notice of the reliability of the "wayback machine."

---

attributable to that person or entity"); Buzz Off Insect Shield, LLC v. S.C. Johnson & Son, Inc., 2009 U.S. Dist. LEXIS 17530 (M.D.N.C. Mar. 6, 2009) ("[defendant] could authenticate its printouts of various websites by calling witnesses who could testify that they viewed and printed the information, or supervised others in doing so, and that the printouts were accurate representations of what was displayed on the listed website on the listed day and time"); Rivera v. Inc. Village of Farmingdale, 29 F. Supp. 3d 121 (E.D.N.Y. 2013) (internet postings offered to show community bias in Fair Housing Act case; testimony that witness "personally downloaded all of the postings and confirmed the identities of the key posters . . . [suffices to show] a 'reasonable likelihood' that they were actually posted on the internet by members of an online community comprised of the Village's own residents").

[46] See, e.g., Foreword Magazine, Inc. v. OverDrive Inc., 2011 U.S. Dist. LEXIS 125373, at *8–*11 (W.D. Mich. Oct. 31, 2011) (admitting screenshots from websites, accompanied only by the sworn affidavit of an attorney, given "other indicia of reliability (such as the Internet domain address and the date of printout)").

[47] See, e.g., Metcalf v. Blue Cross Blue Shield of Mich., 2013 U.S. Dist. LEXIS 109641 (D. Or. Aug. 5, 2013). (authenticity of website information of an organization's purported website was established by logos or headers matching those of the organization).

[48] St. Luke's Cataract & Laser Inst., P.A. v. Sanderson, 2006 U.S. Dist. LEXIS 28873 (M.D. Fla. May 12, 2006) (web master's testimony can authenticate a printout).

[49] Another example of a website that allows users to access archival copies of webpages is www.viewcached.com, which allows users to employ one interface to search three different archival services—the Wayback Machine, Google Cache, and Coral Cache.

[50] See, e.g., Telewizja Polska USA, Inc. v. Echostar Satellite Corp., No. 02 C 3293, 2004 WL 2367740, at 6* (N.D. Ill. Oct. 15, 2004) (approving the use of the Internet Archive's

The opponent of the evidence is free to challenge authenticity of dynamic website data by adducing facts showing that the exhibit does not accurately reflect the contents of a website, or that those contents are not attributable to the ostensible owner of the site. There may be legitimate questions concerning the ownership of the site or attribution of statements contained on the site to the ostensible owner.

### 2. Self-Authenticating Website Data

Under Fed.R.Evid. 902, three types of webpage exhibits are self-authenticating—meaning that a presentation of the item itself is sufficient to withstand an authenticity objection from the opponent.

#### a. Government Websites

Under Rule 902(5) data on governmental websites are self-authenticating.[51] As discussed below, courts regularly take judicial notice of these websites.

#### b. Newspaper and Periodical Websites

Under Rule 902(6) (*Newspapers and Periodicals*), "[p]rinted material purporting to be a newspaper or periodical" is self-authenticating. This includes online newspaper and periodicals, because Rule 101(b)(6) provides that any reference in the Rules to printed material also includes comparable information in electronic form. Thus all newspaper and periodical material is self-authenticating whether or not it ever appeared in hard copy.[52]

#### c. Websites Certified as Business Records

Rules 902(11) and (12) render self-authenticating business (organizational) records that are certified as satisfying Rule 803(6) by "the custodian or another qualified person." Exhibits extracted from websites that are maintained by, for, and in the ordinary course of, a business or other regularly conducted activity can satisfy this rule.[53]

---

"wayback machine" to authenticate websites as they appeared on various dates relevant to the litigation). Compare Open Text S.A. v. Box, Inc., 2015 U.S. Dist. LEXIS 11312 (N.D. Cal. Jan. 30, 2015) (court was unwilling to accept a screenshot from the Wayback Machine into evidence without testimony from a representative of the Internet Archive confirming its authenticity).

Under a proposed amendment to the Federal Rules of Evidence, the reliability of the wayback machine process could be established by a certificate of the Internet Archive official, rather than in-court testimony). See Proposed Rule 902(13) (allowing proof of authenticity of electronic information produced by a process leading to an accurate result to be established by the certificate of a knowledgeable witness). That proposed amendment is scheduled to become effective on December 1, 2017.

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

[52] See, e.g., White v. City of Birmingham, 2015 U.S. Dist. LEXIS 39187 (N.D. Ala. Mar. 27, 2015) (noting sua sponte that news articles from Huntsville Times website (AL.com) "could be found self-authenticating at trial").

[53] See, e.g., United States v. Hassan, 742 F.3d 104, 132–134 (4th Cir. 2014) (Facebook posts, including YouTube videos were self-authenticating under Rule 902(11) where accompanied by certificates from Facebook and Google custodians "verifying that the Facebook pages and YouTube videos had been maintained as business records in the course of regularly conducted business activities"); Randazza v. Cox, 2014 U.S. Dist. LEXIS 49762 (D. Nev. April 10, 2014) (videos posted to YouTube "are self-authenticating as a certified

### 3. Authenticating the Date of Information Posted on a Website

In some cases, a party may need to show not only that a posting was made on a website, but also the date on which the information was generated—this can be a distinct question from establishing what the website looked like at a particular time, which can be shown by the methods discussed above. Assume, for example, that a video is posted on YouTube on January 1, 2016. If the proponent wants to prove that it was posted on that day, this can be done by a person with knowledge, circumstantial evidence, etc. It is a different question if the proponent needs to show that the information itself was *generated* on a certain day. That will not be shown by proving it was posted on a certain date. For example, in *Sublime v. Sublime Remembered*, 2013 U.S. Dist. LEXIS 103813 (C.D. Cal. July 22, 2013), the plaintiffs brought suit against the defendant for violating a court order prohibiting defendant from performing songs belonging to the plaintiffs. As evidence, the plaintiffs sought to admit a YouTube video of the defendant performing the prohibited music. The court ruled that the video was not properly authenticated without evidence that it was recorded *after* the court order was issued. The mere fact that it was *posted* after the court order was issued was not enough to establish that the video was what the proponent said it was—performance of the music after the court order was entered.

Establishing that a video (or any other kind of information posted on a website) was *prepared* on—or before or after—a certain date thus presents a separate question of authenticity. But it is a question that can be addressed through the same factors discussed above: for example, by a person with personal knowledge, a forensic expert, and/or circumstantial evidence. Illustrative is *United States v. Bloomfield*, 591 Fed.Appx. 847, 848–49 (11th Cir. 2014), in which the defendant was convicted of felon-firearm possession. The government offered a YouTube video which showed the defendant discharging an AR–15 rifle in front of Fowler Firearms. The date that the video was made was obviously critical. If it was made before the defendant was a convicted felon, then it depicted no crime. The government was not required, necessarily, to prove that the video was taken on a specific day, but it was required to establish that the video was taken after the defendant was convicted of a felony. And the date that the video was posted on YouTube was not the relevant date. The court found the date was properly authenticated in the following passage:

- Fowler Firearms's manager testified that Broomfield was a Fowler Firearms member, that on January 21, 2011, Broomfield purchased two boxes of PMC .223 ammunition, and that he had not purchased that ammunition at any other time. Dezendorf stated that the only firearm Fowler Firearms rented to customers at the time that used PMC .223 ammunition was the AR–15 rifle.
- An employee who had worked at Fowler Firearms for ten years testified that he could discern the approximate date the video was taken. He explained that the video showed side deflectors and lights on the gun range, which Fowler Firearms had installed in late 2010 or early 2011. He also testified that Fowler Firearms paints its floors and walls at the beginning of the season, and the freshly-painted floor and walls seen in the video indicated that the footage was filmed close to the start of 2011.

domestic record of a regular conducted activity if their proponent satisfies the requirements of the business-records hearsay exception.").

- A witness who operated a maintenance business that provided repair and maintenance to Fowler Firearms testified that he installed the lighted baffles shown in the video, in late September or early October of 2010.

All this was more than enough to indicate that the video was taken around the beginning of 2011—post-dating the defendant's felony status—and so depicted the crime of felon-firearm possession.

### *E. Social Media Postings*

"Social media" is defined as "forms of electronic communications (as websites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content."[54] Parties have increasingly sought to use social media evidence to their advantage at trial. A common example would be a picture or entry posted on a person's Facebook page, that could be relevant to contradict that person's testimony at trial. If the entry is challenged for authenticity, the proponent must present a prima facie case that the evidence is what the party says it is—e.g., that it is in fact a posting on the person's Facebook page. If the goal is to prove that the page or a post is that of a particular person, authenticity standards are not automatically satisfied by the fact that the post or the page is in that person's name, or that the person is pictured on the post.[55] That is because someone can create a Facebook or other social media page in someone else's name. Moreover, one person may also gain access to another's account.

What more must be done to establish authenticity of a social media page? Most courts have found that it is enough for the proponent to show that the pages and accounts can be tracked through internet protocol addresses associated with the person who purportedly made the post.[56]

---

[54] Definition of Social Media, Merriam-Webster, http://www.merriam-webster.com/dictionary/social%20media# (last visited January 16, 2016).

[55] See, e.g., United States v. Vayner, 769 F.3d 125, 132 (2d Cir. 2014), where the court held that a page on the Russian version of Facebook was not sufficiently authenticated simply by the fact that it bore the name and picture of the purported "owner" Zhyltsou:

> It is uncontroverted that information about Zhyltsou appeared on the VK page: his name, photograph, and some details about his life consistent with Timku's testimony about him. But there was no evidence that Zhyltsou himself had created the page or was responsible for its contents. Had the government sought to introduce, for instance, a flyer found on the street that contained Zhyltsou's Skype address and was purportedly written or authorized by him, the district court surely would have required some evidence that the flyer did, in fact, emanate from Zhyltsou. Otherwise, how could the statements in the flyer be attributed to him?

Essentially the court in *Vayner* held that a Facebook page is not self-authenticating. Compare United States v. Encarnacion-LaFontaine, 2016 WL 611925 (2d Cir. Feb. 16, 2016) (threatening Facebook posts were properly authenticated where "the Government introduced evidence that (1) the Facebook accounts used to send the messages were accessed from IP addresses connected to computers near Encarnacion's apartment; (2) patterns of access to the accounts show that they were controlled by the same person; (3) in addition to the Goris threats, the accounts were used to send messages to other individuals connected to Encarnacion; (4) Encarnacion had a motive to make the threats, and (5) a limited number of people, including Encarnacion, had information that was contained in the messages.").

[56] United States v. Hassan, 742 F.3d 104, 133 (4th Cir. 2014) (the trial court did not abuse its discretion in admitting Facebook pages purportedly maintained by two of the defendants; the trial court properly determined that the prosecution had satisfied its burden under Rule 901(a) "by tracking the Facebook pages and Facebook accounts to Hassan's and Yaghi's email addresses via internet protocol addresses"); United States v. Brinson, 772 F.3d 1314 (10th Cir. 2014) (Facebook account linked to the defendant's email).

***Other factors that can be relied upon to support authentication of social media postings include the following:***[57]

- testimony from the purported creator of the social network profile and related postings;
- testimony from persons who saw the purported creator establish or post to the page;
- testimony of a witness that she often communicated with the alleged creator of the page through that account;
- expert testimony concerning the results of a search of the social media account holder's computer hard drive;[58]
- testimony about the contextual clues and distinctive aspects in the messages themselves tending to reveal the identity of the purported author;
- testimony regarding the account holder's exclusive access to the originating computer and social media account;
- information from the social media network that links the page or post to the purported author;
- testimony directly from the social networking website that connects the establishment of the profile to the person who allegedly created it and also connects the posting sought to be introduced to the person who initiated it;
- expert testimony regarding how social network accounts are accessed and what methods are used to prevent unauthorized access;
- production pursuant to a document request;
- whether the purported author knows the password to the account, and how many others know it as well;
- that the page or post contains some of the factors previously discussed as circumstantial evidence of authenticity of texts, emails, etc., including:
  - — nonpublic details of the purported author's life;
  - — other items known uniquely to the purported author or a small group including him or her;
  - — references or links to, or contact information about, loved ones, relatives, co-workers, others close to the purported author;
  - — photos and videos likely to be accessed by the purported author;

[57] See generally Honorable Paul W. Grimm, *Authentication of Social Media Evidence*, 36 AM. J. TRIAL ADVOC. 433 (2013); Richard Raysman and Peter Brown, Authentication of Social Media Evidence, New York Law Journal, November 11, 2011, p. 3.

[58] Honorable Paul W. Grimm, Authentication of Social Media Evidence, 36 AM. J. TRIAL ADVOC. 433, 468 (2013) ("A computer forensic expert can frequently authenticate the maker of social media content. Obviously, you will need to retain the proper expert and ensure that he or she has enough time and information to make the identification. Advance planning is essential, and be mindful of the potentially substantial cost.").

— biographical information, nicknames, not generally accessible;

— the structure or style of comments that are in the style of the purported author;

— that the purported author acts in accordance with the contents of the page or post.

Finally, a social media post meeting the foundational requirements of a business record under Fed.R.Evid. 803(6) may be self-authenticating under 902(11). While this may not be enough to authenticate the *identity* of the person posting,[59] it will be enough to establish that the records were not altered in any way after they were posted.[60]

## IV. Judicial Notice of Digital Evidence

This Best Practices Handbook has discussed the many ways that new forms of digital evidence might be authenticated. Almost all of these methods require expenditure of resources. Courts and parties have begun to realize that some of this new digital evidence has reached the point of being an undisputed means of proving a fact. In these circumstances, judicial notice may be used to alleviate the expenditure of resources toward authentication.

Under Fed.R.Evid. 201(b) a court may judicially notice a fact if it is not subject to reasonable dispute. An example of a court taking judicial notice of a fact obtained through an electronic process is found in *United States v. Brooks,* 715 F.3d 1069, 1078 (8th Cir. 2013). The defendant in a bank robbery prosecution challenged the admissibility of GPS data that was obtained from a GPS tracker that the teller placed in the envelope of stolen money. The trial court took judicial notice of the accuracy and reliability of GPS technology. The court of appeals found no error:

> We cannot conclude that the district court abused its discretion in taking judicial notice of the accuracy and reliability of GPS technology. Commercial GPS units are widely available, and most modern cell phones have GPS tracking capabilities. Courts routinely rely on GPS technology to supervise individuals on probation or supervised release, and, in assessing the Fourth Amendment constraints associated with GPS tracking, courts generally have assumed the technology's accuracy.

---

[59] See United States v. Browne, 2016 U.S. App. LEXIS 15668 (3rd Cir.), where the court found that a Rule 902(11) certification by a Facebook custodian concerning Facebook posts was not sufficient authentication that the post was made by a certain individual:

> Facebook does not purport to verify or rely on the substantive contents of the communications in the course of its business. At most, the records custodian employed by the social media platform can attest to the accuracy of only 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. This is no more sufficient to confirm the accuracy or reliability of the contents of the Facebook chats than a postal receipt would be to attest to the accuracy or reliability of the contents of the enclosed mailed letter.

[60] See, e.g., United States v. Hassan, 742 F.3d 104, 134 (4th Cir. 2014):

> The government presented the certifications of records custodians of Facebook and Google, verifying that the Facebook pages and YouTube videos had been maintained as business records in the course of regularly conducted business activities. According to those certifications, Facebook and Google create and retain such pages and videos when (or soon after) their users post them through use of the Facebook or Google servers.

Another common example of judicial notice of digital information is that courts take judicial notice of distances, locations, and the physical contours of an area by reference to Google Maps.[61]

What follows are some examples of judicial notice of digital information.

### 1. Government Websites

Judicial notice may be taken of postings on government websites,[62] including:

- Federal, state, and local court websites.[63]
- Federal, state, and local agency, department and other entities' websites.[64]
- Foreign government websites.[65]
- International organization websites.[66]

### 2. Non-Government Websites

Generally, courts are reluctant to take judicial notice of non-governmental websites because the Internet "is an open source" permitting anyone to "purchas[e] an internet address and create a website" and so the information recorded is subject to dispute.[67] A few websites, however, as discussed above, have become a part of daily life—their accuracy is both objectively verifiable and actually verified millions of times a day. Other websites are the online versions of sources that courts have taken judicial notice of for years, and the courts find little reason to distinguish a reputable web equivalent from a reputable hard copy edition.

---

[61] See, e.g., United States v. Burroughs, 810 F.3d 833, 835, n.1 (D.C.Cir. 2016) ("We grant the government's motion to take judicial notice of a Google Map. It is a 'source whose accuracy cannot be reasonably questioned,' at least for the purpose of identifying the area where Burroughs was arrested and the general layout of the block."); McCormack v. Hiedeman, 694 F.3d 1004, 1008 (9th Cir. 2012) (relying on Google Maps to determine the distance between two cities; the court held that Google Maps was a website whose accuracy could not reasonably be questioned under Fed.R.Evid. 201(b)(2).). See also Cline v. City of Mansfield, 745 F. Supp. 2d 773, 800 n.23 (N.D. Ohio 2010) (the court took judicial notice that the sun set at 7:47 pm on a particular date according to www.timeanddate.com).

[62] See, e.g., United States v. Head, 2013 U.S. Dist. LEXIS 151805, at *7 n.2 (E.D. Cal. Oct. 22, 2013) ("The court may take judicial notice of information posted on government websites as it can be 'accurately and readily determined from sources whose accuracy cannot reasonably be questioned.' "); Puerto Rico v. Shell Oil Co. (In re MTBE Prods. Liab. Litig.), 2013 U.S. Dist. LEXIS 181837, at *16 (S.D.N.Y. 2013) ("Courts routinely take judicial notice of data on government websites because it is presumed authentic and reliable").

[63] See, e.g., Feingold v. Graff, 516 Fed. App'x 223, 226 (3d Cir. 2013).

[64] See, e.g., United States v. Iverson, 818 F.3d 1015, 1022 (9th Cir. 2016) (noting that "courts have considered the FDIC website so reliable that they have taken judicial notice of information on it"; citing cases); Lawrence v. Fed. Home Loan Mortg. Corp., 2015 U.S. Dist. LEXIS 40012 (W.D. Tex. Mar. 30, 2015) (federal government's agreement with national bank as posted on government website); Flores v. City of Baldwin Park, 2015 U.S. Dist. LEXIS 22149 (C.D. Cal. Feb. 23, 2015) (municipal police department website).

[65] See, e.g., United States v. Broxmeyer, 699 F.3d 265, 296 (2d Cir. 2012) (websites of governments of Vietnam and Brazil).

[66] See, e.g., Kirtsaeng v. John Wiley & Sons, Inc., 133 S. Ct. 1351, 1367 (2013) (World Bank website).

[67] United States v. Kane, 2013 U.S. Dist. LEXIS 154248 (D. Nev. Oct. 28, 2013).

***Examples of Information Found Authentic on Non-Governmental Websites Through Judicial Notice:***

- Internet maps (*e.g.*, Google Maps, MapQuest).
- Calendar information.[68]
- Newspaper and periodical articles.[69]
- Online versions of textbooks, dictionaries, rules, charters.[70]

Most non-Governmental websites, even if familiar, are of debatable authenticity and therefore not appropriately the object of judicial notice. Wikipedia is a prime example. Courts have declined requests to take judicial notice of the contents of Wikipedia entries,[71] except for the fact that the contents appear on the site as of a certain date of access.[72]

### 3. Wayback Machine

Archived versions of websites as displayed on the "wayback machine" (www.archive.org) are frequently the subject of judicial notice,[73] but this is not always the case.[74] Note that it is only the contents of the archived pages that may warrant judicial notice—the dates assigned to archived pages may not apply to images linked to them, and more generally, links on archived pages may direct to the live web if the object of the old link is no longer available.

---

[68] See, e.g., Tyler v. United States, 2012 U.S. Dist. LEXIS 184007, at *9–*10 n.6 (N.D. Ga. Dec. 6, 2012); Local 282, Int'l Bhd. of Teamsters v. Pile Found. Constr. Co., 2011 U.S. Dist. LEXIS 86644, at *17–*18 n.5 (E.D.N.Y. Aug. 5, 2011).

[69] See, e.g., Ford v. Artiga, 2013 U.S. Dist. LEXIS 106805, at *19 n.5 (E.D. Cal. July 30, 2013); HB v. Monroe Woodbury Cent. Sch. Dist., 2012 U.S. Dist. LEXIS 141252 (S.D.N.Y. Sept. 27, 2012).

[70] See, e.g., United States v. Mosley, 672 F.3d 586, 591 (8th Cir. 2012) (PHYSICIANS' DESK REFERENCE); Shuler v. Garrett, 2014 U.S. App. LEXIS 2772, at *7 (6th Cir. Feb. 14, 2014) (OXFORD ENGLISH DICTIONARY); Dealer Computer Servs. v. Monarch Ford, 2013 U.S. Dist. LEXIS 11237, at *11 & n.3 (E.D. Cal. Jan. 25, 2013) (American Arbitration Association rules); Morgan Stanley Smith Barney LLC v. Monaco, 2014 U.S. Dist. LEXIS 149419 (D. Colo. Aug. 26, 2014) (FINRA rules); Famous Music Corp. v. 716 Elmwood, Inc., 2007 U.S. Dist. LEXIS 96789, at *12–*13 n.7 (W.D.N.Y. Dec. 28, 2007) (Articles of Association of ASCAP).

[71] See, e.g., Blanks v. Cate, 2013 U.S. Dist. LEXIS 11233, at *8 n.4 (E.D. Cal Jan. 28, 2013) (refusing to take judicial notice of a Wikipedia entry "as such information is not sufficiently reliable"); Stein v. Bennett, 2013 U.S. Dist. LEXIS 126667, at *20–21 n.10 (M.D. Ala. Sept. 5, 2013) ("Wikipedia is not a source that warrants judicial notice"); Gonzales v. Unum Life Ins. Co. of Am., 861 F. Supp. 2d 1099, 1104 n.4 (S.D. Cal. 2012) ("The Court declines Plaintiff's request to take judicial notice of the Wikipedia definition of Parkinson's Disease because the internet is not typically a reliable source of information").

[72] See, e.g., McCrary v. Elations Co., LLC, 2014 U.S. Dist. LEXIS 8443, at *4–5 n.3 (C.D. Cal. Jan. 13, 2014) ("While the court may take judicial notice of the fact that the internet, Wikipedia, and journal articles are available to the public, it may not take judicial notice of the truth of the matters asserted therein").

[73] See, e.g., Under a Foot Plant Co. v. Exterior Design, Inc., 2015 U.S. Dist. LEXIS 38190 (D. Md. Mar. 25, 2015) ("District courts have routinely taken judicial notice of content from The Internet Archive").

[74] See, e.g., Open Text S.A. v. Box, Inc., 2015 U.S. Dist. LEXIS 11312 (N.D. Cal. Jan. 30, 2015) (proffered Wayback Machine printouts not authenticated absent certification from representative of InternetArchive.org).

## V. Authenticating Electronic Evidence by Way of Certification—New Amendments to the Federal Rules of Evidence, Scheduled to Go into Effect on December 1, 2017

The Rules Committee of the Judicial Conference has unanimously approved a proposal from the Advisory Committee on Evidence to add two new subdivisions to Rule 902, the rule on self-authentication. The first provision would allow self-authentication of machine-generated information, upon a submission of a certification prepared by a qualified person. The second proposal would provide a similar certification procedure for a copy of data taken from an electronic device, medium or file. These proposals are analogous to Rules 902(11) and (12) of the Federal Rules of Evidence, which permit a foundation witness to establish the authenticity of business records by way of certification. Barring any unforeseen developments, these new rules would go into effect on December 1, 2017.

The proposals have a common goal of making authentication easier for certain kinds of electronic evidence that are, under current law, likely to be authenticated under Rule 901 but only by calling a witness to testify to authenticity. The Advisory Committee concluded that the types of electronic evidence covered by the two proposed rules are rarely the subject of a legitimate authenticity dispute, but it has often been the case that the proponent is nonetheless forced to produce an authentication witness, incurring expense and inconvenience—and often, at the last minute, opposing counsel ends up stipulating to authenticity in any event.

The self-authentication proposals, by following the approach taken in Rule 902(11) and (12) regarding business records, essentially leave the burden of going forward on authenticity questions to the opponent of the evidence. Under those rules a business record is authenticated by a certificate, but the opponent is given "a fair opportunity" to challenge both the certificate and the underlying record. The proposals for new Rules 902(13) and 902(14) would have the same effect of shifting to the opponent the burden of going forward (not the burden of proof) on authenticity disputes regarding the described electronic evidence.

These new amendments do not change the *standards* for authentication of electronic evidence. Rather, they change the *manner* in which the proponent's submission on authenticity can be made. Instead of calling a witness, the proponent can provide a certificate prepared by the witness of the submission that he would have made if required to testify. Of course, if that submission would be insufficient if he *had* testified, these new amendments will be of no use. An insufficient showing of authenticity does not somehow become better by way of a certificate in lieu of testimony.

### *Applications of Rules 902(13) and (14)*

In order to assist the Bench and the Bar in evaluating how these new self-authentication rules can be used, the Reporter to the Advisory Committee, with the assistance of John Haried, an attorney from the Justice Department, prepared the following illustrative examples:

**Examples of how Rule 902(13) can be used:**

**1. Proving that a USB device was connected to (i.e., plugged into) a computer:** In a hypothetical civil or criminal case in Chicago, a disputed issue is whether Devera Hall used her computer to access files stored on a USB thumb drive owned by a co-worker. Ms. Hall's 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 in order to facilitate the computer's operations. A forensic technician, located in Dallas, Texas, 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):** Without Rule 902(13), the proponent of the evidence would need to call the forensic technician who obtained the printout as a witness, in order to establish the authenticity of the evidence. During his or her testimony, the forensic technician would typically be asked to testify about his or her background and qualifications; the process by which digital forensic examinations are conducted in general; the steps taken by the forensic technician during the examination of Ms. Hall's computer in particular; 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 by the forensic examiner to examine the Windows registry and to produce the printout identifying the USB device.

**Impact of Rule 902(13):** 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 Ms. 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 opposing party 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. (There are many other examples of the same types of machine-generated information on computers, for example, internet browser histories and wifi access logs.)

**2. Proving that a server was used to connect to a particular webpage:** Hypothetically, a malicious hacker executed a denial-of-service attack against Acme's website. Acme's 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, webpage, 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 mechanics of 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 the website expert'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 registry key, then the proponent would not need to call the website expert to establish authenticity.

**3. Proving that a person was or was not near the scene of an event:** Hypothetically, Robert Jackson is a defendant in a civil (or criminal) 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, 2015. 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 together with the metadata, including the date, time, and GPS coordinates, recovered forensically from his iPhone to corroborate his alibi that he was at home several miles from the scene at the time of the collision.

**Without Rule 902(13):** The proponent would have to call the forensic technician to testify about Mr. 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 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 iPhone's logs, then the proponent would not have to call the technician to establish authenticity.

**4. Proving association and activity between alleged co-conspirators:** Hypothetically, Ian Nichols is charged with conspiracy to commit the robbery of First National Bank that occurred in San Diego on January 30, 2015. Two robbers drove away in a silver Ford Taurus. The alleged co-conspirator was Dain Miller. Dain was arrested on an outstanding warrant on February 1, 2015, and in his pocket was his Samsung Galaxy phone. The Samsung phone's software automatically maintains 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 ya tomorrow." In the separate trial of Ian, 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 logs are created; and that the exhibit is an accurate record of the iPhone's logs.

**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 iPhone's logs, then the court would make the Rule 104 threshold authenticity finding and admit the exhibits, absent other proper objection.

**Hearsay Objection Retained:** Under Rule 902(13), the opponent—here, criminal defendant Ian—would retain his hearsay objections to the text messages found on Dain's phone. For example, the judge would evaluate the text "Sheri says you have some blow" under F.R.E. 801(d)(2)(E) to determine whether it was a coconspirator's statement during and in furtherance of a conspiracy, and under F.R.E. 805, to assess the hearsay within hearsay. The court might exclude the text "Sheri says you have some blow" under either rule or both.

**Example of how Rule 902(14) can be used:**

In the armed robbery hypothetical, above, forensic technician Smith made a forensic copy of Dain's Samsung Galaxy phone in the field. 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 gave the copy to forensic technician Jones, who performed his examination at his lab. 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 of Jones's 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 Jones to testify about his examination.

**With Rule 902(14):** The proponent 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 proponent would only call Jones.

---

The Committee Note approved by the Committee emphasizes that the goal of the amendment is narrow one: to allow authentication of electronic information that would otherwise be established by a witness, instead to be established through a certification by that same witness. The Note makes clear that these are authentication-only rules and that the opponent retains all objections to the item other than authenticity—most importantly that the item is hearsay or that admitting the item would violate a criminal defendant's right to confrontation.

***What follows is the text of the new rules and the Committee Notes:***

**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).

**COMMITTEE NOTE**

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 webpage 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 webpage was retrieved. Even if that certification sufficiently establishes that the webpage is authentic, defendant remains free to object that the statement on the webpage 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 effect 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.

* * *

**(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).

**Committee Note**

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 effect 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.

## APPENDIX

### Federal Rules of Evidence Most Commonly Used to Establish Authenticity of Digital Evidence

**Rule 901. Authenticating or Identifying Evidence**

**(a) In General.** 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.

**(b) Examples.** The following are examples only—not a complete list—of evidence that satisfies the requirement:

**(1)** ***Testimony of a Witness with Knowledge.*** Testimony that an item is what it is claimed to be.

* * *

**(3)** ***Comparison by an Expert Witness or the Trier of Fact.*** A comparison with an authenticated specimen by an expert witness or the trier of fact.

**(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.

* * *

**(9)** ***Evidence About a Process or System.*** Evidence describing a process or system and showing that it produces an accurate result.

**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:

* * *

**(5)** ***Official Publications.*** A book, pamphlet, or other publication purporting to be issued by a public authority.

**(6)** ***Newspapers and Periodicals.*** Printed material purporting to be a newspaper or periodical.

* * *

**(11)** ***Certified Domestic Records of a Regularly Conducted Activity.*** The original or a copy of a domestic record that meets the requirements of Rule 803(6)(A)–(C), as shown by a certification of the custodian or another qualified person that complies with a federal statute or a rule prescribed by the Supreme Court. Before the trial or hearing, the proponent must give an adverse party reasonable written notice of the intent to offer the record—and must make the record and certification available for inspection—so that the party has a fair opportunity to challenge them.

**(12)** ***Certified Foreign Records of a Regularly Conducted Activity.*** In a civil case, the original or a copy of a foreign record that meets the requirements of Rule 902(11), modified as follows: the certification, rather than complying with a federal statute or Supreme Court rule, must be signed in a manner that, if falsely made, would subject the maker to a criminal penalty in the country where the certification is signed. The proponent must also meet the notice requirements of Rule 902(11).

***Proposed Additions to Rule 902, Projected Effective Date December 1, 2017:***

**(13)** ***Certified Records Generated by an Electronic Process or System.*** A record generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent must also meet the notice requirements of Rule 902(11).

**(14)** ***Certified Data Copied from an Electronic Device, Storage Medium, or File.*** Data copied from an electronic device, storage medium, or file, if authenticated by a process of digital identification, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent also must meet the notice requirements of Rule 902(11).

**Rule 201. Judicial Notice of Adjudicative Facts**

**(a) Scope.** This rule governs judicial notice of an adjudicative fact only, not a legislative fact.

**(b) Kinds of Facts That May Be Judicially Noticed.** The court may judicially notice a fact that is not subject to reasonable dispute because it:

**(1)** is generally known within the trial court's territorial jurisdiction; or

**(2)** can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned.

**(c) Taking Notice.** The court:

**(1)** may take judicial notice on its own; or

**(2)** must take judicial notice if a party requests it and the court is supplied with the necessary information.

**(d) Timing.** The court may take judicial notice at any stage of the proceeding.

* * *