Digital Evidence

2015

Jeffrey B. Welty

UNC
SCHOOL OF
GOVERNMENT

Chapter 5: The Admissibility of Electronic Evidence

Even evidence that has been lawfully seized cannot be admitted in court if it cannot satisfy the evidence rules. This chapter considers how the rules of evidence apply to electronic evidence. It focuses on issues that are of particular significance for digital evidence: authentication, the original writing rule (also known as the best evidence rule), and hearsay. Of course, issues of privilege, relevance, and the like may arise with electronic evidence as they may with any form of evidence. Because those issues are not unique to electronic evidence, they are not addressed in this publication.

Like other chapters of this book, this chapter draws heavily on cases decided in other jurisdictions. Fortunately, the rules of evidence are similar across jurisdictions, even sharing a common numbering system based on the federal rules.

I. Authentication

Authentication is widely regarded as the evidentiary consideration that is most different for electronic evidence than it is for traditional evidence.[1] This section reviews important general principles regarding authentication and then applies the principles to several common types of electronic evidence.

A. Authentication Generally

Simply put, authentication is the process of establishing that the piece of evidence in question is what it purports to be, such as an email from the defendant, or a website created by a witness. As explained in the Advisory Committee's Note to Rule 901 of the North Carolina Rules of Evidence, it is a "special aspect of relevancy." To illustrate that point with an example, if a self-incriminating email wasn't actually written by the defendant, it does not tend to establish the defendant's guilt and so should not be admitted at the defendant's trial.

Under N.C. R. Evid. 901(a), "[t]he requirement of authentication . . . is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims."[2] This is a low hurdle that courts often

1. *See, e.g.*, G. Michael Fenner, *The Admissibility of Web-Based Evidence*, 47 Creighton L. Rev. 63, 64 (2013) ("By and large, the novel question regarding the admissibility of web-based evidence . . . is going to be authentication. . . . Once the evidence is authenticated . . . most of the rest of the evidentiary problems are the common problems lawyers face all the time.").

2. Section 8C-901(a) of the North Carolina General Statutes (hereinafter G.S.).

describe as a prima facie showing.[3] Doubts about authentication generally go to the weight, not the admissibility, of the evidence.[4]

Furthermore, there are many ways to authenticate evidence. N.C. R. Evid. 901 gives several examples of how authentication can be accomplished, such as testimony of a witness who knows what the evidence is under Rule 901(b)(1) and authentication by the distinctive characteristics of the evidence under Rule 901(b)(4). But the Rule itself states that these examples are "[b]y way of illustration only, and not by way of limitation."[5] The following sections of this publication apply these general principles to several common types of digital evidence.

B. Authentication of Electronic Communications

The central concern with authenticating electronic communications is whether the proponent of the evidence has established who authored the communication in question. Sufficient evidence of authorship can be provided in several ways.

---

3. State v. Mercer, 89 N.C. App. 714, 716 (1988) (noting approvingly that "federal courts have held that a *prima facie* showing, by direct or circumstantial evidence, such that a reasonable juror could find in favor of authenticity, is enough"); United States v. Vidacak, 553 F.3d 344, 349 (4th Cir. 2009) (explaining that "[t]he burden to authenticate under [Federal] Rule [of Evidence] 901 is not high—only a *prima facie* showing is required," and stating that all that is needed is evidence "from which the jury could reasonably find that the evidence is authentic"); United States v. Gadson, 763 F.3d 1189, 1203 (9th Cir. 2014) (endorsing the *prima facie* showing standard); United States v. Turner, 718 F.3d 226, 232 (3d Cir. 2013) (stating that the burden of authentication is "slight" and that the court "does not require conclusive proof of a document's authenticity, but merely a prima facie showing of some competent evidence to support authentication," with the ultimate determination of authenticity to be made by the jury); United States v. Fluker, 698 F.3d 988, 999 (7th Cir. 2012) ("Only a prima facie showing of genuineness is required; the task of deciding the evidence's true authenticity and probative value is left to the jury."). *See generally* Fenner, *supra* note 1, at 87–88 (noting that the proponent of evidence need only "make a prima facie showing that the evidence . . . is what he or she claims it is" and that "[t]his is not a particularly high barrier to surmount"); United States v. Hassan, 742 F.3d 104, 133 (4th Cir. 2014) (endorsing the prima facie showing standard in a case involving Facebook and YouTube evidence).

4. Thomas v. Dixson, 88 N.C. App. 337, 344 (1988) ("Authentication does not, however, require strict, mathematical accuracy, and a lack of accuracy will generally go to the weight and not the admissibility of the exhibit.").

5. G.S. 8C-901(b).

1. Rule 901(b)(1): Testimony of a Witness with Knowledge

Occasionally, the proponent is able to call the author of the evidence or someone who saw the author create the evidence. For example, the State might be able to call a witness who saw the defendant compose and send a Tweet about shooting a victim, or a witness to whom the defendant subsequently admitted to sending a threatening email.[6] The leading North Carolina case in this area is *State v. Gray*,[7] where a group of people planned a robbery and communicated about the crime via text message. An officer uncovered, and took pictures of, texts between two of the co-conspirators while searching a phone that belonged to one of them. The State sought to introduce the text messages at the trial of a third co-conspirator. One of the co-conspirators testified at trial that she sent the text messages in question and that the pictures accurately reflected the text messages that she sent. The trial court admitted the messages and the court of appeals affirmed, citing N.C. R. Evid. 901(b)(1). Since the co-conspirator sent the messages herself, she was able to testify about their authorship.

The *Gray* court considered and rejected the defendant's argument that the messages were not adequately authenticated because the State did not call an employee of the telecommunications service provider to explain how the company processes and delivers text messages. Although the court did not explain its reasoning on this point in detail, it is reasonable to assume that the court views modern telecommunications processes as presumptively reliable.

There are a few cases that suggest that Rule 901(b)(1) allows the "personal knowledge" of a recipient of a communication to authenticate the communication as coming from a particular author.[8] That suggestion is probably

---

6. Moore v. State, 763 S.E.2d 670, 674 (Ga. 2014) (ruling that evidence from the defendant's Facebook page was adequately authenticated in part because the defendant "admitted to [his girlfriend] that the Facebook page belonged to him"); Bobo v. State, 285 S.W.3d 270, 275 (Ark. Ct. App. 2008) (ruling that emails sent by the defendant were adequately authenticated in part because the defendant "admitted that she sent emails to [the victim]," even though she disputed the content of the emails).

7. ___ N.C. App. ___, 758 S.E.2d 699, *review allowed*, ___ N.C. ___, 766 S.E.2d 635 (2014).

8. *See, e.g.*, Shea v. State, 167 S.W.3d 98, 105 (Tex. App. 2005) (ruling that emails were properly authenticated under Texas Rule of Evidence 901(b)(1) where a witness testified only "that she was familiar with [the author's] e-mail address and that she had received the six e-mails in question from [the author]"); State v. Koch, 334 P.3d 280, 290 (Idaho 2014) (stating that because a witness testified that she "recognized [the defendant's] number and had previously been in frequent communication with him" at that number, text messages sent from that

mistaken. The recipient of an electronic communication typically does not have first-hand knowledge of who wrote it. Normally, the recipient is making an inference about the identity of the author based on the account from which the communication is sent, the content of the communication, and the like. In other words, the recipient is relying on the characteristics of the communication to identify the author. Such an inference may be entirely reasonable and sufficient to authenticate the communication, as discussed below in connection with Rule 901(b)(4), but it does not constitute personal knowledge under Rule 901(b)(1).

Case Summaries Regarding Rule 901(b)(1)

State v. Gray, ___ N.C. App. ___, 758 S.E.2d 699 (discussed in text, above), *review allowed*, ___ N.C. ___, 766 S.E.2d 635 (2014).

Donati v. State, 84 A.3d 156, 171 (Md. Ct. Spec. App. 2014) (under Maryland Evidence Rule 901(b)(1), "the proponent could admit the e-mail through the testimony of the author of the e-mail or a person who saw the author compose and send the e-mail").

United States v. Fluker, 698 F.3d 988, 999 (7th Cir. 2012) (noting that authentication under Federal Rule of Evidence 901(b)(1) was impossible because neither "[the author] nor anyone who saw [the author] author the emails testified that the emails were actually sent by [the author]").

State v. Webster, 955 A.2d 240 (Me. 2008) (ruling that a transcript of online chats between the defendant and an undercover officer was properly authenticated by the personal knowledge of the undercover officer).

2. Rule 901(b)(4): Distinctive Characteristics

Most often, electronic communications will be authenticated by their distinctive characteristics. That is, the proponent of the evidence will show that it was authored by a specific person by establishing that the communication came from that person's email or social media account; referred to matters known only to that person or of particular interest to that person; contained nicknames, terms, or sayings typically used by that person; and the like.

---

number were properly authenticated under Idaho Rule of Evidence 901(b)(1); the court also ruled that the messages were authenticated under Rule 901(b)(4) of the state rules).

These methods are similar to those used to authenticate traditional means of communication, such as letters.[9]

As to what kind, and what quantity, of such circumstantial evidence is enough to authenticate a communication, the cases nationally "arrive at widely disparate outcomes" and are as "clear as mud."[10] Although the lack of agreement in the case law makes it very difficult to announce general rules, a rough summary of the state of the law follows.

First, the fact that an electronic communication concludes with the name of the purported author (such as "Respectfully yours, Janet Adams") or comes from an account that contains the name of the purported author (such as janetadams@gmail.com) is not alone sufficient to establish the authorship of the communication.[11]

Second, the fact that a communication comes from an account linked to a specific person (such as an account that a witness testifies Janet Adams has used for years or an account linked to Janet Adams through subscriber information obtained from a service provider) is at least important evidence of the authorship of the communication. Depending on the strength of the connection between the purported author and the account, such evidence may in some cases be sufficient to authenticate authorship.[12]

---

9. *See, e.g.*, State v. Young, 186 N.C. App. 343, 354 (2007) (holding that letters were properly authenticated as having been written by the defendant where the defendant told the recipient that he would write to him, the letters used nicknames normally used by the defendant and the recipient, and the letters reflected "intimate knowledge of the crime").

10. Paul W. Grimm et al., *Authentication of Social Media Evidence*, 36 Am. J. Trial Advoc. 433, 441 (2013).

11. Commonwealth v. Purdy, 945 N.E.2d 372, 381 (Mass. 2011) (stating that "[e]vidence that the defendant's name is written as the author of an e-mail or that the electronic communication originates from an e-mail or a social networking Web site such as Facebook or MySpace that bears the defendant's name is not sufficient alone to authenticate the electronic communication as having been authored or sent by the defendant," arguing that "[t]here must be some 'confirming circumstances' sufficient for a reasonable jury to find by a preponderance of the evidence that the defendant authored the e-mails," and finding sufficient confirming circumstances to authenticate a series of e-mails); 2 Kenneth S. Broun et al., McCormick on Evidence § 221, at 57 (6th ed. 2006) (noting in connection with traditional writings that "the purported signature or recital of authorship on the face of a writing will *not* be accepted, without more, as sufficient proof of authenticity to secure the admission of the writing in evidence"); *Id.* § 227, at 73 n.2 ("For purposes of authentication, self-identification of an e-mail is insufficient, just as are the traditional signature and telephonic self-identification.").

12. *Compare* Hollie v. State, 679 S.E.2d 47, 50 (Ga. Ct. App. 2009) ("Though the e-mail transmission in question appears to have come from P.M.'s [the victim's] e-mail address, this alone does not prove its genuineness."), *aff'd*, 696 S.E.2d 642

Third, additional circumstantial authenticate regarding the contents of the communications is often the best way to authenticate authorship. For example, it may be persuasive evidence of authorship if a communication refers to facts or events known only to the author ("Remember that time we kissed behind the Post Office?"), refers to facts or events of particular interest to the author ("I can't wait for the Star Trek convention next week!"), or uses terms or nicknames that are characteristic of the author ("My little tomato, no one can have you if I can't."),[13] Similarly, it may be persuasive evidence of authorship if there is a connection between the communication and a precipitating event in which the author was involved. For example, when a threatening message is sent from the defendant's email address to the defendant's neighbor a few minutes after the two had a verbal altercation, the temporal proximity of the encounter and the email tends to show that the defendant is the author of the email. And it may be persuasive evidence of authentication where there are follow-up communications, linked to the author, referring to or repeating the contents of the original electronic communication, as when the defendant's threatening email is followed up with a face-to-face threat referring to the email.

Case Summaries Regarding Rule 901(b)(4)

SUFFICIENT EVIDENCE OF AUTHENTICITY

Commonwealth v. Johnson, 21 N.E.3d 937, 952 (Mass. Dec. 23, 2014) (ruling, in a harassment case, that the prosecution sufficiently authenticated emails between a defendant and a cooperating witness where the witness testified that the emails were "signed using [the defendant's] typical signature," the witness testified that he had exchanged many emails with the defendant using the same address over the past decade, and the emails referenced the harassing acts at issue in the case).

(Ga. 2010), *with* State v. Andrews, 293 P.3d 1203, 1206 (Wash. Ct. App. 2013) ("[T]estimony as to the defendant's phone number and signature sufficiently authenticated pictures of received text messages.").

13. *See generally* State v. Francis, ___ S.W.3d ___, No. ED 100009, 2014 WL 1686538, at *11 (Mo. Ct. App. Apr. 29, 2014) (collecting cases and stating that authentication may be established by, for example, "an admission by the author that the number from which the message was received is his number and that he has control of that phone," testimony from "the person receiving the message testifying that he regularly receives text messages from the author from this number," or "something distinctive about the text message indicating the author wrote it, such as a personalized signature"); *In re* F.P., 878 A.2d 91 (Pa. Super. Ct. 2005) (instant messages were properly authenticated as having been authored by the defendant where he used his name in the conversation and the content of the conversation referred to a long-running dispute with the victim).

Culp v. State, ___ So. 3d ___, No. CR-13-1039, 2014 WL 6608543 (Ala. Crim. App. Nov. 21, 2014) (holding, in a domestic violence case, that the prosecution sufficiently authenticated threatening emails as having been written by the defendant where the victim testified that she had helped the defendant set up the account from which the emails were sent, each email contained the defendant's picture and screen name, many emails concluded with the defendant's initials, and several emails contained slang terms for drugs that were typically used by the defendant).

State v. Koch, 334 P.3d 280, 289 (Idaho 2014) (collecting cases and ruling, in a child sexual abuse case, that a text message sent to the complainant's mother was properly authenticated as having been authored by the defendant; although "more than just confirmation that the number belonged to the person in question is required when the message's authentication is challenged," the contents of the message in question, including a reference to a recent fight between the defendant's daughter and the complainant, also showed that the defendant was the author; the court also analyzed several other electronic communications, ruling that most, but not all, were adequately authenticated by similar circumstantial evidence).

State v. Wilkerson, ___ N.C. App. ___, 733 S.E.2d 181 (2012) (text messages were sufficiently authenticated as being written by the defendant where a witness reported the defendant's suspicious driving on the victim's street and testified that the defendant appeared to be using a cell phone as he drove; the cell phone from which the messages were sent was found on the defendant's person; the text messages referenced an item stolen from the victim; and cell site data was interpreted by experts to establish that the phone traveled from the area of the defendant's home to the area of the victim's home and back).

Gulley v. State, 423 S.W.3d 569 (Ark. 2012) (sufficient circumstantial evidence authenticated the defendant's authorship of three text messages; messages came from cellular phone number assigned to the defendant; two of the messages referred to facts and circumstances known to the defendant; the third text message announced that the defendant would be dropped off at the victim's house and was followed by his arrival there the night she was killed).

Campbell v. State, 382 S.W.3d 545, 550 (Tex. App. 2012) (noting that "the fact that an electronic communication on its face purports to

originate from a certain person's social networking account is generally insufficient standing alone to authenticate that person as the author of the communication"; finding that contents of Facebook messages were authenticated by speech patterns in messages that were consistent with the defendant's patterns of speech, by references to an incident and potential charges a few days after the incident occurred, and by the victim's testimony that, while she once had access to the defendant's account, she did not at the time the messages were sent and did not write the messages).

Tienda v. State, 358 S.W.3d 633 (Tex. Crim. App. 2012) (internal content of MySpace postings, including photographs of the defendant, comments, and music, and a subscriber report listing the owner of two of three accounts as having an email address that contained the defendant's name and zip code and a third account as having an email address that included the defendant's nickname, were sufficient to permit a reasonable juror to find that MySpace postings for all three accounts were created and maintained by the defendant).

State v. Williams, 191 N.C. App. 254 (2008) (unpublished) (instant messages purportedly exchanged between the defendant and the victim were properly authenticated by circumstantial evidence as being authored by the defendant where the victim testified that she and the defendant exchanged instant messages regularly, that the defendant's email address was the one from which the messages originated, and that the content of the messages included details known only to the defendant and the victim).

Dickens v. State, 927 A.2d 32 (Md. Ct. Spec. App. 2007) (authentication requirements were satisfied where threatening text messages were linked to the defendant by direct and circumstantial evidence, including references to facts known by few people, conduct consistent with the contents of the message, and references to seeing the minor child of the defendant and the victim).

State v. Taylor, 178 N.C. App. 395 (2006) (text messages were sufficiently authenticated by circumstantial evidence as being written by the victim where the messages indicated that the author would be driving a car of the same make and model as the victim's and the author twice referred to himself by the victim's name; there was also sufficient authentication of the text messages as being messages to and from a particular cellular phone number where there was expert testimony

regarding the service provider database from which the messages were retrieved and the service provider's business practice of storing such messages).

INSUFFICIENT EVIDENCE OF AUTHENTICITY

Smith v. State, 136 So. 3d 424, 434 (Miss. 2014) (ruling, in a murder case, that the prosecution failed to authenticate Facebook messages purportedly sent from the defendant to his wife [and mother of the child victim] as having been composed by the defendant; the court reasoned that social media accounts may easily be hacked or fabricated, so authentication requires more than showing that a message comes from an account with the purported author's "name and photograph"; in this case, "[n]o other identifying information from the Facebook profile, such as date of birth, interests, hometown, or the like, was provided" and the witness did not explain how she identified the messages as coming from the defendant; the court noted that the messages did not appear to be part of a conversation between the two).

State v. Lukowitsch, ___ N.C. App. ___, 752 S.E.2d 258 (2013) (unpublished) ("[T]he trial court properly excluded the content of the text messages because defendant failed to present any evidence to authenticate the text messages as having been sent by [a certain party].").

Rodriguez v. State, 273 P.3d 845 (Nev. 2012) (trial court abused its discretion in admitting text messages that the State claimed were sent by the defendant, a co-defendant, or both, using the victim's cell phone because the State failed to present sufficient evidence corroborating the defendant's identity as the person who sent the messages).

Griffin v. State, 19 A.3d 415 (Md. 2011) (printed pages of a MySpace account allegedly belonging to the defendant's girlfriend upon which appeared a post indicating that "SNITCHES GET STITCHES" were not properly authenticated, and it was prejudicial error to admit them into evidence; the court concluded that because of the risk of camouflaged identities and account manipulation on social networking sites, "a printout of an image from such a site requires a greater degree of authentication than merely identifying the date of birth of the creator and her visage in a photograph on the site in order to reflect that [the defendant's girlfriend] was its creator and the author of the 'snitches get stitches' language").

State v. Eleck, 23 A.3d 818 (Conn. App. 2011) (trial court did not abuse its discretion in excluding evidence of Facebook messages purportedly sent from State's witness's account to the defendant; a reference in the messages to acrimonious history did not sufficiently establish that the State's witness authored the messages such that it was an abuse of discretion to exclude the evidence), *aff'd on other grounds*, 100 A.3d 817 (2014)).

3. Business Records

Courts in some jurisdictions have addressed whether electronic communications may be authenticated as the business records of a social media company or an electronic communications service provider. Those courts have considered Fed. R. Evid. 902(11) or its state equivalents. The federal version of Rule 902(11) designates as self-authenticating "[t]he original or a copy of a domestic record that meets the requirements of [Fed. R. Evid.] 803(6)(A)-(C) [the business records exception to the hearsay rule], 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." The rule requires that the proponent of such evidence give the opposing party advance notice of the proponent's intent to offer it.

The Fourth Circuit recently held that screenshots of two defendants' Facebook pages, among other evidence, could be admitted as Facebook's business records.[14] However, a Colorado appellate court reached a contrary result, reasoning that "even though an arguable business relationship exists between Facebook and its users, there was no evidence presented that Facebook substantially relies for any business purpose on information contained in its users' profiles and communications."[15] At least for now, the issue is only of academic interest in North Carolina, as North Carolina has not adopted a version of Rule 902(11) and business records are not self-authenticating in North Carolina's courts.

---

14. United States v. Hassan, 742 F.3d 104, 133 (4th Cir. 2014) (finding no abuse of discretion in district court's decision to admit screenshots of defendants' Facebook pages and YouTube videos posted by defendants as self-authenticating business records).

15. People v. Glover, ___ P.3d ___, No. 13CA0098, 2015 WL 795690 (Colo. App. Feb. 26, 2015) (ruling that the defendant's Facebook messages and profile were not admissible as business records under Colorado's analogue of Fed. R. Evid. 902(11)).

C. Authentication of Tracking Data

As discussed in chapter 3 and elsewhere in this book, GPS data may come into criminal cases in several ways: because law enforcement placed a tracking device on a suspect's vehicle; because a suspect was wearing a GPS tracking bracelet as a condition of probation or pretrial release; because law enforcement seized a cell phone or other device containing GPS data from a suspect; and so on. Although each situation presents slightly different considerations, it is often possible to authenticate such data under N.C. R. Evid. 901(b)(1) (testimony of a witness with knowledge that the data is what it is claimed to be), Rule 901(b)(9) (concerning "[e]vidence describing a process or system used to produce a result and showing that the process or system produces an accurate result"), or some combination of the two.

The leading case in North Carolina is *State v. Jackson*.[16] The defendant committed a sexual assault while wearing a GPS tracking device as a condition of his pretrial release. The supervisor of the electronic monitoring unit testified regarding how the tracking device worked. The defendant argued that the tracking data was not properly authenticated, but the court of appeals ruled to the contrary. However, the court did not analyze the authentication issue in detail—instead focusing mainly on whether the data were inadmissible hearsay—so the opinion is useful mainly for cases that have similar facts.

A few cases from other jurisdictions provide more general guidance. Most courts seem satisfied if a witness who possesses a working familiarity with the GPS system explains how it functions, how the data were collected, and what the data mean.[17] Several cases have focused on the qualifications and experience necessary to authenticate the data. Courts generally have ruled that the witness need not be an expert so long as he or she is familiar with the technology.[18]

---

16. ___ N.C. App. ___, 748 S.E.2d 50 (2013).

17. *See, e.g.*, United States v. Espinal-Almeida, 699 F.3d 588, 612, 613 (1st Cir. 2012) (ruling that data taken from a GPS device seized from a boat used for drug trafficking were properly authenticated by the testimony of the lab analyst who examined the device; the analyst provided a "good amount of testimony about the processes employed by the GPS," allowing the court to apply Fed. R. Evid. 901(b)(9), which permits a witness to describe a process or system and thereby authenticate the result of the process or system; the court ruled that expert testimony was not required to authenticate the data, noting that the analyst was "knowledgeable, trained, and experienced in analyzing GPS devices").

18. *Id. See also* United States v. Brooks, 715 F.3d 1069, 1078 (8th Cir. 2013) (a bank robber was apprehended based on a GPS device that was placed surreptitiously in the loot bag; the trial judge properly took judicial notice of the "accuracy and reliability of GPS technology" generally, and the testimony of an

By contrast, evidence about cell site location information typically is introduced by an expert witness, and courts have disagreed about the extent to which such experts may pinpoint a phone's location, as opposed to identifying a general area in which the phone was located or simply describing the location of the towers to which the phone connected.[19]

---

employee of the security company that supplied the device was sufficient to admit the data generated by the device in question; although the witness apparently lacked a "scientific background," he had worked for the company for eighteen years, "had been trained by the company . . . knew how the device worked, and . . . had demonstrated the device for customers dozens of times"); United States v. Thompson, 393 F. App'x 852 (3d Cir. 2010) (unpublished) (a bank robber was apprehended based on a GPS device that was placed surreptitiously in the loot bag; the GPS data was authenticated at trial by an employee of the security company that supplied the device; he explained how the device worked, and he was properly permitted to testify as a lay witness rather than an expert, given that his knowledge was based on his personal experience with such devices).

19. *Compare* United States v. Evans, 892 F. Supp. 2d 949, 955–57 (N.D. Ill. 2012) (ruling that an FBI agent with extensive training in cell phone investigations could testify as an expert about how cellular networks operate and could testify about which towers interfaced with the defendant's cell phone at various times, but could not estimate the defendant's location using "granulization," a system for determining which of two "closely positioned towers" serves which nearby locations, because granulization does not account for the possibility that a phone may make contact with a tower that is not the closest one due to physical obstructions or network traffic, and because granulization "remains wholly untested by the scientific community"), *and* State v. Payne, 104 A.3d 142, 145–55 (Md. 2014) (ruling that a detective "needed to be qualified as an expert . . . before being allowed to testify . . . [about] the communication path" of the defendants' cell phones, i.e., "the location of cell phone towers through which particular calls were routed and . . . the locations of those towers on a map in relation to the crime scene"; the court noted that "[t]here are a variety of factors affecting to which tower a cell phone will connect, beyond merely the distance" between the phone and the available towers and ruled that the witness "engaged in a process to derive his conclusion [about the location of the defendants' phones] that was beyond the ken of an average person"), *with* United States v. Machado-Erazo, 950 F. Supp. 2d 49, 55–58 (D.D.C. 2013) (ruling that an FBI agent with extensive training in cell phone investigations could testify as an expert to the "general location where a cell phone would have to be located to use a particular cell tower and sector," distinguishing *Evans* as involving an attempt to identify a phone's specific location within an area of overlapping coverage by multiple towers and noting that "many cases" have admitted testimony similar to that at issue in this case), *and* United States v. Jones, 918 F. Supp. 2d 1, 4–6 (D.D.C. 2013) (ruling that an FBI agent with extensive training in cell phone investigations could testify as an expert regarding the location of cell towers in a relevant area, the coverage sectors of the towers, and "where the cell phones must have been when they connected to each tower," because such testimony is "based on reliable methodology" and has been "widely accepted by numerous courts").

D. Authentication of Evidence Seized from a Defendant's Digital Device

Many cases involve evidence that is seized from a digital storage device, such as a computer, disc drive, or cell phone. Child pornography cases may involve images; fraud cases may involve accounting records; and homicide cases may involve information that sheds light on the defendant's motive or the method he or she used to commit the crime. Such evidence normally is authenticated by testimony about the retrieval of the evidence and its preservation, unaltered, until trial.[20] This is similar to the authentication procedure for physical evidence.

A defendant may argue that he did not place the evidence on the digital device—that a virus put it there or that someone else with access to the device was responsible for the presence of the evidence. Such an argument may well be critical to the defendant's culpability and proper for jury consideration, but it is largely irrelevant to authentication, as it does not relate to the identity or genuineness of the evidence. Similarly, in child pornography cases, whether images show real or simulated children may be an important factor in the defendant's guilt or innocence, but it probably should not be viewed as an authentication issue. So long as the images accurately reflect the data obtained from the defendant's digital storage device, they have been authenticated.[21]

---

20. *See generally* United States v. Salcido, 506 F.3d 729, 733 (9th Cir. 2007) ("[T]he government properly authenticated the videos and images . . . by presenting detailed evidence as to the chain of custody [and] how the images were retrieved from the defendant's computers."); Midkiff v. Commonwealth, 694 S.E.2d 576 (Va. 2010) (images retrieved from the defendant's computer were properly authenticated by testimony that they were retrieved by copying the defendant's hard drive and then copying the images in question onto a DVD, from which the images used at trial were generated); Bone v. State, 771 N.E.2d 710 (Ind. Ct. App. 2002) (images were properly authenticated by testimony that they were retrieved from the defendant's computer and printed out).

21. *See, e.g.*, United States v. Edington, 526 F. App'x 584, 591 (6th Cir. 2013) (unpublished) ("The government must produce evidence sufficient to support a finding that the item is what the government claims it is—in this case, a video that the defendant received or possessed. This can be done by offering testimony from an investigator who was present when the video was retrieved and can describe the process used to retrieve it"; the government does not need to show that the video depicts actual children, as that is an issue for the jury to determine); *Salcido,* 506 F.3d at 733 ("While [the defendant] frames [the prosecution's alleged failure to establish that the videos and images in question depicted real, rather than virtual, children] as an issue of authenticity, this argument is more properly considered a challenge to the sufficiency of the evidence.").

E. Authentication of Web Pages

Web pages are often important evidence in criminal cases. Such evidence might include a Facebook wall posting from a defendant admitting guilt; Mapquest directions reflecting the driving distance between the defendant's home and the victim's residence; or a Google Maps printout showing an overhead view of the crime scene. Courts have been skeptical about the origins and authentication of material printed from websites generally.[22] However, the specific authentication issues regarding web pages vary based on the type of page at issue.

For example, social media postings present authorship issues similar to those with electronic communications, discussed above.[23] Different considerations arise with mapping websites like Mapquest and Google Maps. These sites

22. *In re* Yopp, 217 N.C. App. 489, 495 (2011) ("internet printout[]" used to show that two banks had merged "was not authenticated as a public record and was inadmissible; the mere fact that a document is printed out from the internet does not endow that document with any authentication whatsoever"); Rankin v. Food Lion, 210 N.C. App. 213, 217 (2011) (plaintiff attempted to use two documents to establish identity of the proper corporate defendant; "[o]ne of these documents appears to consist of a page printed from the website of the North Carolina Secretary of State, while the other appears to consist of an internet posting" about a defendant; these documents were not authenticated and were not admissible); United States v. Jackson, 208 F.3d 633, 638 (7th Cir. 2000) ("[The defendant] needed to show that the web postings in which the white supremacist groups took responsibility for the racist mailings actually were posted by the groups, as opposed to being slipped onto the groups' web sites by [the defendant] herself, who was a skilled computer user"; but the defendant did not do so, and the websites were not authenticated).

23. For additional cases specifically concerning social media postings, see *United States v. Hassan*, 742 F.3d 104, 133 (4th Cir. 2014) (screenshots of Facebook pages were properly authenticated as having been authored by the defendants where investigators had "track[ed] the Facebook pages and Facebook accounts to [the defendants'] mailing and email addresses via internet protocol addresses"); *United States v. Vayner*, 769 F.3d 125, 131 (2d Cir. 2014) ("[W]e conclude that the district court abused its discretion in admitting the VK web page, as it did so without proper authentication under [Federal] Rule [of Evidence] 901. The government did not provide a sufficient basis on which to conclude that the proffered printout was what the government claimed it to be—*Zhyltsou's* profile page—and there was thus insufficient evidence to authenticate the VK page and to permit its consideration by the jury."); *Parker v. State*, 85 A.3d 682 (Del. 2014) (ruling, in an assault case, that Facebook posts were properly authenticated as having been written by the defendant in part because they "referenced the altercation" in question and were created on the same day that the assault took place); and *Moore v. State*, 763 S.E.2d 670 (Ga. 2014) (ruling, in a murder case, that Facebook posts were properly authenticated as having been written by the defendant where the defendant's picture appeared on the Facebook page, the page contained details about the defendant, such as his nickname, hometown, and girlfriend, and

offer maps, driving directions, and driving times. The maps often are admitted based on the testimony of a witness that the maps fairly and accurately represent the area shown.[24] The distance measurements available on the sites may be the subject of judicial notice, though driving times may be hearsay.[25] Finally, information from government websites, like the state prison system's website, may be self-authenticating under Rule 902(5), which provides that "[b]ooks, pamphlets, or other publications purporting to be issued by public authority" are self-authenticating.[26]

II. Original Writing/Best Evidence Rule

A second issue that arises with regard to electronic evidence concerns the original writing or "best evidence" rule. Generally, if a piece of evidence is a writing, a recording, or a photograph and the proponent seeks to prove its contents, N.C. R. Evid. 1002 requires the introduction of the original of the writing, recording, or photograph.

Electronic writings such as emails, text messages, and social media postings are "writings" within the meaning of the original writing requirement. N.C. R. Evid. 1001(1) states that "writings" consist of "letters, words, sounds, or numbers, or their equivalent, set down by handwriting, typewriting, printing, photostating, photographing, magnetic impulse, mechanical or

---

the posts matched the "structure and style" of other communications from the defendant).

24. State v. Brown, 1 So. 3d 504 (La. Ct. App. 2008) (court erred in excluding Mapquest printout depicting crime scene; witness should have been allowed to testify that it fairly and accurately showed the scene; any inaccuracies went to weight, not admissibility).

25. People v. Stiff, 904 N.E.2d 1174 (Ill. App. Ct. 2009) (taking judicial notice of the distance between two residences based on Google Maps); Jianniney v. State, 962 A.2d 229, 230 (Del. 2008) (noting that "many courts have taken judicial notice of facts derived from internet map sites" but ruling that estimates of driving times, as opposed to distances, are hearsay not within any exception).

26. G.S. 8C-902(5). *See, e.g.*, Williams Farms Produce Sales, Inc. v. R & G Produce Co., 443 S.W.3d 250, 259 n.7 (Tex. App. 2014) ("[W]e hold that documents printed from government websites [here, a docket sheet printed from a federal court's website] are self-authenticating."), Firehouse Rest. Group, Inc., v. Scurmont, LLC, No. 4:09-cv-00618-RBH, 2011 WL 3555704, at *4 (D.S.C. Aug. 11, 2011) (unpublished) ("Records from government websites are generally considered admissible and self-authenticating."); Williams v. Long, 585 F. Supp. 2d 679, 689 (D. Md. 2008) ("The printed webpage from the Maryland Judiciary Case Search website is self-authenticating under [Federal] Rule [of Evidence] 902(5).").

electronic recording, or other form of data compilation." Courts have recognized that electronic writings of various kinds meet this definition.[27] Digital photographs also fall within the rule. Thus, in cases in which the contents of a digital writing or photograph are at issue, the proponent must satisfy the original writing requirements.[28]

Some electronic text may not be a writing within the scope of the rule. For example, when a witness seeks to testify about the phone number from which a call originated, based on the witness's observation of the number through caller ID, the opposing party may argue that the caller ID information is a "writing" the content of which the proponent is seeking to prove and that the original writing requirement therefore applies. However, it probably is not, as the number is generated by a computer rather than being "set down by handwriting, typewriting" or the like, as required by the rule.[29]

When it is necessary to comply with the rule, various "originals" may exist. A printout of data stored on an electronic device is an "original."[30] In the case of text messages, the cellular phone displaying the text message also constitutes an "original."[31] Furthermore, even if an "original" is not available,

27. *See, e.g.*, State v. Espiritu, 176 P.3d 885 (Haw. 2008) (finding text messages to be a writing).

28. *See* Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534 (discussing criminal cases in which the proponent sought to prove the content of electronic writings). *See also generally* Hon. Paul W. Grimm et al., *Back to the Future:* Lorraine v. Markel American Insurance Co. *and New Findings on the Admissibility of Electronically Stored Information,* 42 Akron L. Rev. 357 (2009) ("[I]f there is no non-documentary proof of the occurrence, and the only evidence of what transpired is contained in a writing, then the original writing rule applies."). *Cf.* State v. Branch, 288 N.C. 514 (1975) (holding that witness could testify to a conversation he heard even though a recording of the conversation also existed; the conversation, not the content of the recording, was what was at issue).

29. State v. Schuette*,* 44 P.3d 459, 464 (Kan. 2002) ("Caller ID displays by their nature . . . cannot be printed out or saved on an electronic medium. [The defendant's argument] . . . is akin to contending that a clock must be produced before a witness can testify as to the time he or she observed an accident."). Even if a court were to rule that caller ID information constitutes a "writing," testimony about the writing probably would be admissible under N.C. R. Evid. 1004(1) on the theory that the "original" had been lost or destroyed without bad faith.

30. *See* N.C. R. Evid. 1001(3).

31. *See, e.g.*, State v. Winder, 189 P.3d 580 (Kan. Ct. App. 2008) (unpublished) (excusing production of cell phone containing text message, which the court assumed constituted an original); *Espiritu*, 176 P.3d 885 (trial court properly allowed witness to testify regarding contents of text messages when witness no longer had the cellular phone on which she received the messages; in ruling that the witness no longer had the "actual text messages," the court implicitly

in most instances, a duplicate is admissible to the same extent as an original.[32] A photograph of an electronic writing—for example, a photograph of a text message—may be admitted as a duplicate.[33]

Finally, neither an original nor a duplicate is required in the circumstances described in N.C. R. Evid. 1004. Subsection (1) of Rule 1004 describes the exception that is most likely to arise in criminal cases. It provides that the original is not required, and that a witness may testify to the contents of a writing, if all originals have been lost or destroyed—unless the proponent lost or destroyed the original in bad faith.[34] It is unclear how far courts should inquire into the loss or destruction of originals. For example, if a text message has not been retained on the recipient's phone and the recipient seeks to testify about the contents of the message, must the proponent of the testimony show that it is impossible to recover the contents from the recipient's service provider? From the sender's service provider? From the sender's phone? Case law does not yet answer these questions.[35]

---

concluded that if the witness had retained the phone, that would have constituted an original).

32. *See* N.C. R. Evid. 1003 (stating that a duplicate is admissible except when there is a genuine question about the authenticity of the original or when it would be unfair to admit a duplicate in lieu of the original).

33. *See, e.g.*, Rodriguez v. State, 449 S.W.3d 306, 2014 Ark. App. 660 (Ark. Ct. App. 2014) (ruling that a photograph of a threatening text message was admissible where the witness testified that the message had been deleted from her phone and a representative of the phone company testified that the company does not keep records of the content of text messages; "the photograph of the text was all there was"); State v. Andrews, 293 P.3d 1203 (Wash. Ct. App. 2013) (ruling that a photograph of a text message was properly admitted as a duplicate where defense counsel acknowledged having no reason to doubt the accuracy of the photograph); Dickens v. State, 927 A.2d 32 (Md. Ct. Spec. App. 2007) (photographs of text messages properly admitted).

34. *See, e.g.*, Espiritu, 176 P.3d at 892 (concluding that "bad faith cannot be inferred because the text messages were not printed out when there is no indication that such a printout was even possible").

35. *Cf. Rodriguez*, 449 S.W.3d at 313, 2014 Ark. App. at ___ (ruling that a photograph of a text message was properly admitted notwithstanding the best evidence rule and noting in the course of the discussion that "[t]he State presented an AT & T representative, who testified that the company does not keep records of the content of text messages").

III. Hearsay

The hearsay rule applies to electronic evidence as it does to other evidence. However, certain types of electronic evidence present particular hearsay concerns. This section addresses the provisions of hearsay law that are most likely to arise when dealing with electronic evidence.

A. Statements by the Defendant

When offered by the State, a statement by the defendant is an admission of a party-opponent and therefore will be subject to the hearsay exception for such statements in N.C. R. Evid. 801(d). Thus, a text message, email, or the like that is authenticated as having been written by the defendant may be admitted under the hearsay rules.

If the defendant's statement is threatening, the statement also may be considered a declaration of state of mind within the hearsay exception in N.C. R. Evid. 803(3), or it may be non-hearsay evidence of a verbal act.[36]

B. Evidence That Is Not Hearsay

Several types of electronic evidence are not hearsay. Many courts have recognized that evidence that is produced automatically by a computer is not a statement of a declarant and so simply falls outside the scope of the hearsay rules. Examples include:

- Cell phone records[37]
- Caller ID information[38]
- Logs generated by alarm systems[39]

---

36. *See* State v. Weaver, 160 N.C. App. 61 (2003) (holding that a statement of a bribe was evidence of a verbal act and was not offered for the truth of the matter asserted but, rather, to show that the statement was made).

37. Godoy v. Commonwealth, 742 S.E.2d 407, 411 (Va. Ct. App. 2013) (holding, in a rape case, that the defendant's cell phone records were properly admitted as they were "automatically self-generating" and "not governed by hearsay principles"; the court also noted that the records were not created for the purpose of litigation and so were not testimonial for purposes of Confrontation Clause analysis).

38. Inglett v. State, 521 S.E.2d 241, 245 (Ga. Ct. App. 1999) (finding no hearsay issue because caller ID information is "computer-generated data automatically appearing on the screen of the telephone").

39. State v. Gojcaj, 92 A.3d 1056, 1067 (Conn. App. Ct. 2014) ("[R]ecords that are entirely self-generated by a computer do not trigger the hearsay rule," because they aren't statements made by a declarant; thus, a log showing when an alarm system had been turned on and off was not hearsay).

- Information recorded by red light cameras[40]
- Data recorded by a tracking or monitoring device[41]

Similarly, the telephone number from which a text message was sent has been found not to constitute hearsay because such information is not a statement of a person.[42] Photographs also are not statements and so are not hearsay.[43] It is debatable whether a map constitutes a "statement" or is, like a picture, outside the realm of hearsay. If a map is a statement, it may often be admissible for the non-hearsay purpose of illustrating the testimony of a witness.[44]

C. Business Records

Some electronic evidence may be admitted as business records under N.C. R. Evid. 803(6), which concerns "records of regularly conducted activity" in any form. Courts have sometimes admitted evidence under the business records exception even where the evidence likely is not hearsay at all for the reasons set forth in the preceding section. For example, phone records are

40. People v. Goldsmith, 326 P.3d 239, 249 (Cal. 2014) (ruling that red light camera data, including date, time, and "length of time since the traffic signal light turned red" are "not statements of a person" but are electronically generated and so are not hearsay).

41. State v. Kandutsch, 799 N.W.2d 865, 879 (Wisc. 2011) (distinguishing between "computer-stored records, which memorialize the assertions of human declarants, and computer-generated records, which are the result of a process free of human intervention," and finding that tracking device data are the latter and so are not hearsay).

42. *See* State v. Schuette, 44 P.3d 459 (Kan. 2002); N.C. R. Evid. 801(a) (defining a statement as from "a person").

43. N.C. R. Evid. 801(a) defines a "statement" as "(1) an oral or written assertion or (2) nonverbal conduct of a person, if it is intended by him as an assertion." *See* State v. Patterson, 332 N.C. 409 (1992).

44. State v. Wright, 752 A.2d 1147 (Conn. App. Ct. 2000) (rejecting a defendant's hearsay argument regarding the admission of a map used to show the distance from the location of his arrest to a nearby school; a witness testified that the map was a fair and accurate representation of the area, and the court stated that the map was merely a pictorial representation of the testimony of the witness); Dawson v. Olson, 543 P.2d 499 (Idaho 1975) (map should have been admitted for illustrative purposes, though if offered as substantive evidence, the hearsay rule would apply).

often admitted as business records,[45] and GPS data may also be admitted as a business record.[46]

An issue that arises with business records is whether live testimony is required to establish the foundation for admissibility. According to N.C. R. Evid. 803(6), the foundation for the business records exception must be "shown by the testimony of the custodian or other qualified witness." By way of contrast, the federal business records rule, Fed. R. Evid. 803(6), expressly provides that the foundation may be supplied by testimony *or by a written certification* from an appropriate witness. Notwithstanding the use of the term "testimony" in the North Carolina version of the rule, appellate case law supports the use of an affidavit to satisfy the foundational requirements of the business records exception.[47]

---

45. State v. Brewington, 80 N.C. App. 42, 51 (1986) ("The [telephone] records were duly authenticated by the company's custodian for billing records and, if otherwise competent, were admissible under the business records exception to the hearsay rule."); State v. Hunnicutt, 44 N.C. App. 531 (1980) (telephone company's computerized billing and call records were properly admitted as business records). *Cf.* State v. Taylor, 178 N.C. App. 395 (2006) (noting that a telephone representative described how the records of text messages were created and maintained). Of course, the requisite foundation must be established. State v. Price, 326 N.C. 56 (1990) (holding that the trial court erred in allowing a telephone bill to be introduced to show the record of calls without the testimony of a witness about the preparation of the records), *vacated on other grounds*, Price v. North Carolina, 498 U.S. 802 (1990).

46. State v. Jackson, ___ N.C. App. ___, 748 S.E.2d 50 (2013) (the defendant committed a sexual assault while wearing a GPS tracking device as a condition of his pretrial release; the supervisor of the electronic monitoring unit testified regarding how the tracking device worked, and that established the foundation to admit the data from the device as a business record); United States v. Brooks, 715 F.3d 1069, 1079 (8th Cir. 2013) (the defendant robbed a bank and a teller slipped a GPS tracking device into the loot bag; the GPS "tracking reports fell under the business records exception").

47. *See* Simon v. Simon, ___ N.C. App. ___, 753 S.E.2d 475 (2013) (expressly rejecting the argument that the term "testimony" in N.C. R. Evid. 803(6) requires a live witness and holding that the applicability of the business records exception may be established by an affidavit from an appropriate person); *In re* S.W., 175 N.C. App. 719 (2006) (cited approvingly in *In re* S.D.J., 192 N.C. App. 478 (2008)). As authority for the use of an affidavit, *S.W.* cites *Chamberlain v. Thames*, 131 N.C. App. 705 (1998), a civil case that allowed an affidavit to be used under the specific provision regarding the use of affidavits to establish the foundation for the admission of medical and public records in N.C. R. Civ. P. 45(c). Because *Chamberlain* is a civil case applying a particular rule of civil procedure, it may not be a strong precedent for the use of affidavits in criminal cases. However, since *S.D.J.* and *Simon* have followed *S.W.*, the propriety of using affidavits appears to be settled.

The proponent may not avoid the foundation requirements of the business records exception by having a witness read from a business record for which a proper foundation has not been established.[48]

Business records generally are not testimonial, and therefore may be admitted without running afoul of the Confrontation Clause. The North Carolina Court of Appeals recently ruled that this was so even when the business records in question were GPS tracking records compiled by the North Carolina Department of Correction in connection with the monitoring of an individual on post-release supervision.[49]

48. *See* State v. Springer, 283 N.C. 627 (1973) (holding that allowing investigator to read from records violated the original writing rule).

49. State v. Gardner, ___ N.C. App. ___, ___, ___ S.E.2d ___, ___, No. COA14-646, 2014 WL 6907482, at *3 (N.C. Ct. App. Dec. 2, 2014) (reasoning that "the GPS evidence admitted in this case was not generated purely for the purpose of establishing some fact at trial. Instead, it was generated to monitor defendant's compliance with his post-release supervision conditions. The GPS evidence was only pertinent at trial because defendant was alleged to have violated his post-release conditions.").