THE WRONG ROAD TAKEN: SOCIAL MEDIA CONTENT, SELF-AUTHENTICATION AND MISAPPLICATION OF THE BUSINESS RECORDS RULE

THE HONORABLE DANIEL J. CROTHERS *

ABSTRACT

User generated social media content is increasingly becoming courtroom evidence. Worldwide social media users total nearly 3.6 billion people, with that number projected to exceed 4.41 billion by 2025. As a result, information from social media is making its way into nearly every area of litigation. This proliferation presents courts, lawyers, and litigants with emerging issues relating to admissibility of evidence discovered in its content.

The Rules of Evidence provide the framework governing admissibility of evidence. Courts are being made to navigate those rules in an ever-changing technological landscape where people can use social networking websites to easily create fictitious accounts, masquerade as another person, fabricate, and tamper with information.

This article explores whether courts are correctly making admissibility determinations and, more particularly, focuses on the correct and incorrect results when computer-stored social media content is offered as self-authenticating under the business records rule. It explains why misapplying that rule to admit computer-stored social media content often circumvents the foundational requirements designed to ensure the reliability and trustworthiness of

---

*†Justice Daniel J. Crothers has served on the North Dakota Supreme Court in Bismarck since June of 2005. Prior to taking the bench, he was a commercial litigator, a college instructor, and a legal and judicial educator. Justice Crothers received his undergraduate and law degrees from the University of North Dakota. He has written and lectured on the interaction of technology and legal and judicial ethics, discovery and admissibility of electronically stored information, judicial disqualification, ethics for new judges and their families, the ethics of independent judicial investigation, ethics for judges in leadership, developing judicial leadership in a learning organization, and more. He has made hundreds of presentations to judges, lawyers and law students throughout the United States, and in Guam, the Virgin Islands and Ukraine. Crothers is chair of the ABA Standing Committee on Professional Regulation and an adjunct faculty member at the National Judicial College at the University of Nevada-Reno. He is a past president of the State Bar Association of North Dakota and past chair of the ABA Standing Committee on Client Protection, past chair of the ABA Center for Professional Responsibility's Policy Implementation Committee, past member of the ABA President's Taskforce on Cybersecurity, and past member of the ABA Standing Committee on Ethics and Professional Responsibility.

The author expresses profound thanks to former North Dakota Supreme Court Judicial Assistant Jeanne Walstad for her substantive and editorial assistance. I could not have completed this article without her substantial drafting contributions, critical questions, and sharp editorial eye. I also thank University of North Dakota Law School Dean Michael McGinniss for his input and advice during the drafting process, and Supreme Court Law Clerk Matthew Keller and Supreme Court Judicial Assistant Susan Hartley-Wolfgram for their editorial assistance.

content. The article concludes that when user-generated social media content is offered to prove the truth of its contents, the business record nearly always falls outside the scope of Rule 803(6) and cannot be self-authenticating under Rule 902(11), 902(13) or 902(14).

I. INTRODUCTION

Social media messaging is commonplace, resulting in the content making its way into nearly every area of litigation. The proliferation of social media evidence presents judges, lawyers, and litigants with new admissibility challenges. This article considers authentication generally, and then shifts focus to the evidentiary issues arising when social media content is offered as self-authenticating under the business records rule.

I begin by reviewing social media, its current place in society, and its impact on litigation specifically in the form of electronically stored information ("ESI"). I next lay out the current evidentiary scheme governing admissibility of ESI under the Federal Rules of Evidence (or under identical or substantially similar state rules), first by reviewing the basic requirements of Rule 901 and 902, and second by reviewing Rules 803(6) and 902(11). Third, I argue why self-authentication under the business records rule for admitting computer-stored social media content is generally the wrong approach because it ignores the cognate relationship of relevancy and authentication. When courts and litigants take this inappropriate evidentiary shortcut, they circumvent the safeguards necessary to ensure the evidence is trustworthy, reliable, and authentic. Finally, I review newly enacted Rules 902(13) and (14) and urge judges and lawyers not to misuse those provisions as shortcuts for admission of third-party computer-stored social media content.

II. SOCIAL MEDIA: CONNECTING THE WORLD, PERSONALLY AND PROFESSIONALLY

Social media is defined as "forms of electronic communication (such as websites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (such as videos)."[1] Social media is an integral part of society allowing people to connect with others, personally and professionally, with ease, speed, and world-wide reach. It has rapidly transformed how people communicate, interact with the world around them, influence others, and conduct business. When people engage in social media, intentional and unintentional content is created in the form of user-generated and computer-generated ESI. This section briefly reviews social media, its use, its structure, and its growing prevalence in litigation.

A. IMPORTANCE OF SOCIAL MEDIA IN TODAY'S WORLD: HERE TODAY; HERE TO STAY

Social media usage has a prominent and growing presence in our homes, businesses, and society at large. Today, social media users are not only individuals who use social media platforms to connect with others personally. Users include companies, organizations, and entities of all types increasingly using social media to reach the public, conduct business operations, and market ideas and goods.[2] Social media even plays a large role in the distribution

1. *Social media*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/social%20media (last visited Apr. 22, 2021).

2. Sonya Strnad & Cynthia Burnside, *Plunder or Blunder: E-discovery in the Age of Social Media- Mining for Gold and Dodging the Silver Bullet*, ABA SECTION OF LITIG. 1, 4 (2012) (on file with author).

of news[3] and political messaging.[4] Frankly, imagining a current or future world without social media is virtually impossible.[5]

In 2020, 3.6 billion people were estimated to be social media users worldwide, with that number projected to increase to 4.41 billion by 2025.[6] According to a 2021 survey conducted by the Pew Research Center, approximately seven of ten individuals in the United States use social media with the most widely used platforms being YouTube and Facebook, followed by Instagram, Pinterest, LinkedIn, Snapchat, and Twitter.[7] TikTok, launched in 2016, is gaining popularity in the United States and ranks seventh in active users worldwide as of January 2021.[8]

B. GROWING PREVALENCE OF SOCIAL MEDIA IN LITIGATION

Considering the ubiquity of social media and the increasing number of users, it is no surprise social media is making its way into nearly every area of litigation confronting courts, lawyers, and litigants with the emerging issues concerning admissibility of evidence discovered in its content. These developments are not new; nor are they slowing. An article published in 2012 by the American Bar Association described the growing presence of social media in court cases:

> Given social media's prominence in everyday life and the often candid and informal nature of information it contains, lawyers may be remiss in their duties if they fail to consider social media as a source

---

3. *For Local News, Americans Embrace Digital but Still Want Strong Community Connection*, PEW RSCH. CTR. (Mar. 26, 2019), https://www.journalism.org/2019/03/26/for-local-news-americans-embrace-digital-but-still-want-strong-community-connection/ ("Nearly as many Americans today say they prefer to get their local news online as say they prefer to do so through the television set. . . . The 41% of Americans who say they prefer getting their local news via TV and the 37% who prefer it online far outpace those who prefer a printed newspaper or the radio (13% and 8%, respectively).").

4. Maeve Duggan & Aaron Smith, *The Political Environment on Social Media*, PEW RSCH. CTR. (Oct. 25, 2016), https://www.pewresearch.org/internet/2016/10/25/the-political-environment-on-social-media ("A new Pew Research Center survey of U.S. adults finds that political debate and discussion is indeed a regular fact of digital life for many social media users, and some politically active users enjoy the heated discussions and opportunities for engagement that this mix of social media and politics facilitates. . . . Among the key findings of this survey: More than one-third of social media users are worn out by the amount of political content they encounter, and more than half describe their online interactions with those they disagree with politically as stressful and frustrating.").

5. *See Social Media- Statistics & Facts*, STATISTA (Feb. 25, 2021), https://www.statista.com/topics/1164/social-networks/#dossierSummary__chapter2.

6. *Number of Social Network Users Worldwide from 2017-2025 (in Billions)*, STATISTA, http://www.statista.com/statistics/278414/number-of-world-wide-social-network-users/ (last visited Apr. 13, 2021).

7. Brooke Auxier & Monica Anderson, *Social Media Use in 2021*, PEW RSCH. CTR. (Apr. 7, 2021), https://www.pewresearch.org/internet/2021/04/07/social-media-use-in-2021/.

8. *Most Popular Social Networks Worldwide, as of January 2021, Rank by Number of Active Users (in millions)*, STATISTA (Jan. 2021), https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/.

> of potentially relevant information. In some kinds of litigation, particularly criminal, personal injury, employment and family law, social media is routinely sought. A survey of the American Academy of Matrimonial Lawyers found that 80% of its lawyers already used Facebook data in divorce cases, of which 66% considered Facebook the "unrivaled leader for online divorce evidence." However, the use of social media is not limited to just these areas of practice. It is increasingly becoming an important source of data for many other kinds of litigation, ranging from securities litigation to defamation, misappropriation of trade secrets, breach of confidentiality, breach of non-compete agreements, copyright and trademark violations, conversion, regulatory violations, etc.[9]

It is reasonable to assume the percentages and litigation areas reported in 2012 have continued to increase to present day. As technology advances and the sheer number of online communications increases, so too will the admissibility of evidence issues courts, lawyers, and litigants encounter.

C. STANDARD STRUCTURE OF SOCIAL MEDIA PLATFORMS

Although the presentation, offerings, and capabilities vary from platform to platform, social media websites are "sophisticated tools of communication where the user voluntarily provides information that the user wants to share with others."[10] In terms of usage, "no other major social media platform comes close to Facebook."[11] Therefore, while I endeavor to be platform-neutral, when necessary this article uses Facebook and its terminology to highlight who does what in terms of a social media website's function and the relationship between the platform and its users.

Facebook tells us it "builds technologies and services that enable people to connect with each other, build communities, and grow businesses."[12] Like most social media sites, Facebook does not charge users for using its products and services. Rather, "businesses and organizations pay [Facebook] to show [users] ads for their products and services."[13] Facebook collects, uses, stores, mines, and shares personal data its users supply and targets advertising to its

---

9. Strnad & Burnside, *supr*a note 2, at 5.

10. Indep. Newspapers, Inc. v. Brodie, 966 A.2d 432, 438 n.3 (Md. 2009).

11. John Gramlich, *Ten Facts About Americans and Facebook*, PEW. RSCH. CTR. (May 16, 2019), https://www.pewresearch.org/fact-tank/2019/05/16/facts-about-americans-and-facebook.

12. *See Terms of Service*, FACEBOOK, https://www.facebook.com/terms.php (last visited Mar. 2, 2021).

13. *Id*. ("Instead of paying to use Facebook and the other products and services [Facebook] offer[s], by using the Facebook Products covered by these Terms, [a user] agree[s] that [Facebook] can show [the user] ads that businesses and organizations pay [Facebook] to promote on and off the Facebook Company Products.").

users based on interests and activities derived from the personal data.[14] Facebook shares collected data with other entities including advertisers, third-party partners, vendors, academics, service providers, regulators, and law enforcement under certain circumstances.[15] Facebook does not purport to verify the reliability or the genuineness of the content.[16] On the contrary, under Facebook's Terms of Service, a user owns "the intellectual property rights (things like copyright or trademarks) in any such content that [the user] create[s] and share[s] on Facebook . . . ."[17] Facebook specifies its terms do not diminish a user's rights to the content and users are free to share the content.[18] In exchange, the user gives Facebook "legal permissions (known as a 'license')" to use the content.[19] However, Facebook, and other social media platforms, appear to engage in some form of fact checking of users' content.[20]

---

14. *Id*. (explaining that Facebook uses "personal data, such as information about [a user's] activity and interests, to show [the user] ads that are more relevant to [the user]"); *see also Data Policy*, FACEBOOK, https://www.facebook.com/about/privacy/update (last visited Mar. 2, 2021) (describing information Facebook collects from users including "information about [users'] interests, actions and connections—to select and personalize ads, offers and other sponsored content that [Facebook] shows [its users]").

15. *Data Policy*, *supra* note 14 (explaining the kinds of data Facebook collects from its users and how that data is used and shared with the public, the user's audience, and other Facebook partners).

16. *Terms of Service*, *supra* note 12 (explaining its products are provided "as is," and Facebook makes "no guarantees that they always will be safe, secure, or error-free, or that they will function without disruptions, delays, or imperfections. . . . We do not control or direct what people and others do or say, and we are not responsible for their actions or conduct (whether online or offline) or any content they share (including offensive, inappropriate, obscene, unlawful, and other objectionable content).").

17. *Id*.

18. *Id*.

19. *Id*.

20. During the last year it has become widely known that several social media sites "fact check" some user posts. *See, e.g.*, Savannah Behrmann, *'Contain Potentially Misleading Information': Twitter Fact-Checks Trump's Tweets*, USA TODAY (May 27, 2020, 2:14 PM), https://www.usatoday.com/story/news/politics/2020/05/26/twitter-fact-checking-president-trump-tweets/5263437002/ ("Twitter fact-checked and labeled some of President Donald Trump's posts as misleading on Tuesday."). Regarding this and COVID-19, Twitter stated, "Content that is demonstrably false or misleading and may lead to significant risk of harm (such as increased exposure to the virus, or adverse effects on public health systems) may not be shared on Twitter." *COVID-19 Misleading Information Policy*, TWITTER, https://help.twitter.com/en/rules-and-policies/medical-misinformation-policy (last visited Apr. 22, 2021). Twitter also explained: "Our current misleading information policies cover: synthetic and manipulated media, COVID-19, and civic integrity. If we determine a Tweet contains misleading or disputed information per our policies that could lead to harm, we may add a label to the content to provide context and additional information." *Our Range of Enforcement Options*, Twitter, https://help.twitter.com/en/rules-and-policies/enforcement-options (last visited Apr. 22, 2021). Facebook and Instagram also conduct a fact-checking program under the following philosophy: "We're committed to fighting the spread of misinformation on Facebook and Instagram. In many countries and regions, we work with independent, third-party fact checking organizations who are certified through the non-partisan International Fact-Checking Network (IFCN) to identify, review and take action on this content." *Fact-Checking on Facebook,* FACEBOOK, https://www.facebook.com/business/help/ (search in search bar for "Fact-Checking on Facebook"; then follow "Fact-Checking on Facebook" hyperlink) (last visited Apr. 22, 2021).

As part of creating an account, "Facebook 'requires users to provide a name and email address to establish an account. Account holders can, among other things, add other users to their "friends" list and communicate with them through Facebook chats, or messages.'"[21] After registering, Facebook users "create their own individual web pages (their profiles) on which they post their own personal information, photographs and videos, and from which they can send and receive messages to and from others whom they have approved as their 'friends.'"[22] The registration is not subject to verification.

It is easy to open a legitimate or fictitious Facebook account and create a profile on the website.[23] "[A]nyone at least thirteen years old with a valid email address could create a profile."[24] The ease with which individuals can open an account and communicate using social media does not come without consequences. The website's easy process to create a profile and lack of verification was described by the Mississippi Supreme Court in *State v. Smith*:

> To create a profile, a person must go to www.facebook.com, enter his or her full name, birth date, and e-mail address, and register a password. Facebook then sends a confirmation link to the registered e-mail, which the person must click on to complete registration. Not only can anyone create a profile and masquerade as another person, but such a risk is amplified when a person creates a real profile without the realization that third parties can "mine" their personal data. Friends and strangers alike may have "access to family photos, intimate details about one's likes and dislikes, hobbies, employer details, and other personal information," and, consequently, "the desire to share information with one's friends may also expose users to unknown third parties who may misuse their information." Thus, concern over authentication arises "because anyone can create a fictitious account and masquerade under another person's name or can gain access to another's account by obtaining the user's username

---

21. Commonwealth v. Mangel, 181 A.3d 1154, 1159 (Pa. Super. Ct. 2018) (quoting United States v. Browne, 834 F.3d 403, 405 (3d Cir. 2016)).

22. Commonwealth v. Meola, 125 N.E.3d 103, 107 n.1 (Mass. App. Ct. 2019) (quoting 2 MCCORMICK ON EVIDENCE § 227, at 20 (2013 & Supp. 2016)).

23. Smith v. State, 136 So. 3d 424, 432 (Miss. 2014) (citing Samantha L. Millier, Note, *The Face-Book Frontier: Responding to the Changing Face of Privacy on the Internet*, 97 KY. L.J. 541, 544 (2008-09)); Griffin v. State, 19 A.3d 415, 421-22 (Md. 2011)); *see also* Campbell v. State, 382 S.W.3d 545, 550 (Tex. App. 2012) (internal citations omitted) ("[F]acebook presents an authentication concern that is twofold. First, because anyone can establish a fictitious profile under any name, the person viewing the profile has no way of knowing whether the profile is legitimate. Second, because a person may gain access to another person's account by obtaining the user's name and password, the person viewing communications on or from an account profile cannot be certain that the author is in fact the profile owner.").

24. *Smith*, 136 So. 3d at 432 (quoting Nathan Petrashek, Comment, *The Fourth Amendment and the Brave New World of Online Social Networking*, 93 MARQ. L. REV. 1495, 1506 (Summer 2010)).

> and password," and, consequently, "the potential for fabricating or tampering with electronically stored information on a social networking site" is high and poses challenges to authenticating printouts from the website.[25]

Courts and commentators recognize the high potential for fabricating and tampering with social media content makes authenticating and admitting evidence from it challenging for courts.[26] Social media platforms also recognize the high potential for fabricating accounts.[27]

In making admissibility decisions relating to evidence discovered from social media content, courts must face the unavoidable reality: To properly do their function requires understanding the form of the evidence offered. To arrive at the right answer, courts also must consider the right question. For example, in determining admissibility of social media content, courts should consider, among other intricacies particular to ESI, whether the content constitutes a statement and whether the statement is computer-generated. In *Foundations of Digital Evidence*, George Paul stresses the importance for courts to recognize the difference between computer-generated and computer-stored evidence in making admissibility decisions.[28] According to Paul, the primary distinction lies in identifying where the electronic statement originated. "If the system made the statement, it is 'computer-generated.'"[29] However, "[i]f a person input[s] a statement into the system that then preserved a record of it, it is 'computer-stored.'"[30] The Federal Rules of Evidence already acknowledge some ESI is system-generated rather than generated by a person and, as such, is treated differently.[31]

Social media sites contain both computer-generated and computer-stored information.[32] For example, information about when a user logs into an account and the identity of those with whom a user directly communicates

---

25. *Id*. (internal citations omitted); *Griffin*, 19 A.3d at 421-22 (observing "anyone can create a fictitious account and masquerade under another person's name or can gain access to another's account by obtaining the user's username and password"); *see also Campbell*, 382 S.W.3d at 550.

26. *Smith,* 136 So. 3d at 432.

27. *See, e.g*., *Community Standards Enforcement Report, Facebook Transparency*, FACEBOOK, https://transparency.facebook.com/community-standards-enforcement#fake-accounts (last visited Dec. 22, 2020) ("[E]stimate that fake accounts represented approximately 5% of our worldwide monthly active users (MAU) on Facebook during Q4 2020.").

28. GEORGE L. PAUL, FOUNDATIONS OF DIGITAL EVIDENCE 115-18 (2008).

29. *Id*. at 115; *see also* Orin S. Kerr, *Computer Records and the Federal Rules of Evidence*, 49 U.S. ATT'YS BULL. 25, 26 (March 2001) ("The difference hinges upon whether a person or a machine created the records' contents.").

30. PAUL, *supra* note 28, at 115.

31. *See, e.g*., FED. R. EVID. 902(13) (providing for self-authentication of "[a] record generated by an electronic process or system that produces an accurate result . . . .").

32. Kerr, *supra* note 29, at 26 (citing People v. Holowko, 486 N.E.2d 877, 878-79 (Ill. 1985) (explaining that "computer records that contain text often can be divided into two categories: computer-generated records, and records that are merely computer-stored.")).

is computer-generated content.[33] By contrast, a user's upload of a video or picture, or the content of a user's post, is computer-stored information.[34] Understanding the difference between generated and stored information is "a step in the right direction for courts."[35] When a court applies "a blanket label of computer-generated to all digital evidence, [it] necessarily obscure[s] many important points of the analysis" in that "computer-stored information is often, if not almost always, hearsay."[36] As will be explored later, that distinction becomes important in determining if social media content is admissible.[37] In turn, understanding the basic tenets of authentication under Rules 901 and 902 is essential to determining when admission of social media evidence is appropriate.

III. CONSIDERING ADMISSION OF COMPUTER-STORED SOCIAL MEDIA CONTENT INTO EVIDENCE—RELEVANCY, AUTHENTICATION, AND THE BUSINESS RECORDS RULE

Admissibility of ESI has been described as requiring satisfaction of five evidentiary "hurdles."[38] Relevancy and authentication are the two evidentiary

---

33. *See, e.g.*, PAUL, *supra* note 28, at 115-116 (citing Tatum v. Commonwealth, 440 S.E.2d 133 (Va. Ct. App. 1994) ("[C]omputer-generated evidence is the product of electronic processes, or the statements an information system makes . . . ."); *see also* Kerr, *supra* note 29, at 26 ("Computer-generated records contain the output of computer programs, untouched by human hands. Log-in records from Internet service providers, telephone records, and ATM receipts tend to be computer-generated records. Unlike computer-stored records, computer-generated records do not contain human 'statements,' but only the output of a computer program designed to process input following a defined algorithm.").

34. *See, e.g.*, PAUL, *supra* note 28, at 115 (explaining that "computer-stored evidence is a repetition of data originally entered by a human"); *see also* Kerr, *supra* note 29, at 2 (stating "[c]omputer-stored records refer to documents that contain the writings of some person or persons and happen to be in electronic form. E-mail messages, word processing files, and Internet chat room messages provide common examples.").

35. PAUL, *supra* note 28, at 116.

36. *Id.*

37. *Id.* at 116 n.2 (citing State v. Robinson, 272 Neb. 582, 724 N.W.2d 35 (Neb. 2006) (illustrating the potential for unclear analysis that can occur when courts do not consider the distinction between computer-generated and computer-stored evidence). As Paul explained:

> [I]n *State v. Robinson*, an individual convicted of first-degree murder claimed that cell phone records showing the physical location of certain calls at certain times should be excluded as hearsay. Computer systems automatically recorded each time a phone call was made and what number[s] were connected. At the same time, the information about who owned the cell phones at each end of any recorded call was manually entered and stored in the computer system. Thus, when the prosecution offered the cell phone records as evidence, those records were the product of both computer-generated information and computer-recorded statements by human beings . . . . The court did not make any such distinction in its analysis, but instead applied the business records exception to the hearsay rule and held that these records were admissible.

Id. (citations omitted).

38. In *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534 (D. Md. 2007), the United States District Court for the District of Maryland undertook an analysis of the evidentiary rules and caselaw governing the admissibility of ESI. The *Lorraine* court described the requisite process to admit ESI as "a series of hurdles to be cleared by the proponent of the evidence." *Id.* at 538. The Court noted

hurdles or thresholds foremost to this article. Consideration of their close relationship, along with proper application of the business record rule, is essential to correctly making admissibility determinations for social media content.

A. RELEVANCY

Whether an item is relevant under Rule 401 is directly related to whether under Rule 901 the item is what the proponent claims it to be. Fully understanding and appreciating the interrelationship of relevancy and authenticity requires a review of the purpose for each rule.

Relevancy answers the question whether a piece of evidence matters. Simply put, does the item have a logical place in the particular legal dispute?[39] Under Rule 401, evidence is relevant if "(a) it has any tendency to make a fact more or less probable than it would be without the evidence; and (b) the fact is of consequence in determining the action."[40] The cases uniformly demonstrate relevancy is a low threshold that generally is not difficult to achieve.[41] And, evidence satisfying the threshold is presumptively admissible unless provided otherwise under "the United States Constitution; a federal statute; [the federal] rules; or other rules prescribed by the Supreme Court."[42] Notwithstanding its relatively low elevation, the threshold remains meaningful nonetheless.

"Relevancy is not an inherent characteristic of any item of evidence but exists only as a relation between an item of evidence and a matter properly

---

that "[f]ailure to clear any of these evidentiary hurdles means that the evidence will not be admissible," and specifically outlined the hurdles as:

> (1) is the ESI relevant as determined by Rule 401 (does it have any tendency to make some fact that is of consequence to the litigation more or less probable than it otherwise would be); (2) if relevant under 401, is it authentic as required by Rule 901(a) (can the proponent show that the ESI is what it purports to be); (3) if the ESI is offered for its substantive truth, is it hearsay as defined by Rule 801, and if so, is it covered by an applicable exception (Rules 803, 804 and 807); (4) is the form of the ESI that is being offered as evidence an original or duplicate under the original writing rule, or if not, is there admissible secondary evidence to prove the content of the ESI (Rules 1001-1008); and (5) is the probative value of the ESI substantially outweighed by the danger of unfair prejudice or one of the other factors identified by Rule 403, such that it should be excluded despite its relevance. *Id*.

39. *See* FED. R. EVID. 401 advisory committee note to 1972 proposed rules (extolling use of the Rule's language because "it has the advantage of avoiding the loosely used and ambiguous word 'material'").

40. *Id*. ("Relevancy is not an inherent characteristic of any item of evidence but exists only as a relation between an item of evidence and a matter properly provable in the case. Does the item of evidence tend to prove the matter sought to be proved? Whether the relationship exists depends upon principles evolved by experience or science, applied logically to the situation at hand . . . .").

41. *Lorraine*, 241 F.R.D. at 541 (explaining that "[t]o be relevant it is enough that the evidence has a *tendency* to make a consequential fact even the least bit more probable or less probable than it would be without the evidence. The question of relevance is thus different from whether evidence is *sufficient* to prove a point.") (citation omitted).

42. FED. R. EVID. 402.

provable in the case."[43] As such, the question becomes: "Does the item of evidence tend to prove the matter sought to be proved?"[44] Additionally, "there is a distinction between the admissibility of evidence and the weight to which it is entitled in the eyes of the fact finder . . . ."[45] The evidence need not carry any specific weight to be relevant;[46] "it is sufficient if it has 'any tendency' to prove or disprove a consequential fact in the litigation."[47] "[E]vidence can have this tendency only if it is what the proponent claims it is, i.e., if it is authentic."[48] Accordingly, relevancy and authentication determinations are intertwined. In other words, "[a]uthentication represents a special aspect of relevancy in that evidence cannot have a tendency to make the existence of a disputed fact more or less likely if the evidence is not that which its proponent claims."[49]

Determining relevancy involves various considerations: What fact is the proponent seeking to prove with the evidence? Is the fact to be proven material to deciding the case? Is the evidence probative of the fact to be proven? Is the evidence what its proponent claims it to be, thereby making the existence of the disputed fact more or less likely with the evidence?

If the proffered evidence is not relevant, the inquiry ends because the rules of evidence plainly provide "irrelevant evidence is not admissible."[50] However, if the proffered information is relevant, the evidence also must be determined authentic to be admitted.

B. AUTHENTICATION

While relevancy aims to determine whether evidence pertains to issues before the court, authenticity focuses on whether the proffered item is genuine or real.[51] In the context here, a proponent of social media content must

---

43. FED. R. EVID. 401 advisory committee's note to 1972 proposed rules.

44. *Id.*

45. *Lorraine*, 241 F.R.D. at 541.

46. *See* FED. R. EVID. 401 advisory committee's note to 1972 proposed rules (explaining that "[t]he standard of probability under the rule is 'more * * * probable than it would be without the evidence.' Any more stringent requirement is unworkable and unrealistic. . . . Dealing with probability in the language of the rule has the added virtue of avoiding confusion between questions of admissibility and questions of the sufficiency of the evidence.").

47. *Lorraine*, 241 F.R.D. at 541.

48. United States v. Browne, 834 F.3d 403, 409 (3d Cir. 2016) (citing United States v. Rawlins, 606 F.3d 73, 82 (3d Cir. 2010)).

49. Commonwealth v. Meola, 125 N.E.3d 103, 110 (Mass. App. Ct. 2019) (quoting United States v. Branch, 970 F.2d 1368, 1370 (4th Cir. 1992)).

50. FED. R. EVID. 402.

51. *Authentication*, BLACK'S LAW DICTIONARY (11th ed. 2019) ("authentication n. (18c) 1. Broadly, the act of proving that something (as a document) is true or genuine, esp. so that it may be admitted as evidence; the condition of being so proved <authentication of the handwriting>.").

demonstrate that the item is what the proponent claims it is.[52] The interrelationship between relevancy and authentication constantly must be kept in mind. Authenticity is closely connected with relevancy because the actual tendency of an item of evidence to prove or disprove a fact of consequence depends on the evidence being what it is claimed to be.[53] As noted, authentication of ESI generally, and social media content particularly, presents a variety of challenges for courts.[54]

As a general proposition, "[t]he degree of authentication does not vary simply because a record happens to be (or has been at one point) in electronic form."[55] Similarly, the requirements for proper authentication are not different merely because a proponent seeks self-authentication under Rule 902 rather than providing testimony or extrinsic evidence under Rule 901. Therefore, this subsection first reviews the basic tenets of authentication under the framework of Rule 901 and Rule 902 before focusing on whether evidence is a business record under Rules 803(6) and 902(11).

1. Rule 901. Authentication By Direct or Circumstantial Evidence

Under Rule 901(a), "[t]o satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is."[56] Evidence is properly authenticated if the proponent provides "facts that are sufficient to support a reasonable jury determination that the evidence he had offered is authentic."[57] The proponent is not required "to rule out all possibilities inconsistent with authenticity, or prove beyond any doubt that the evidence is what it purports to be."[58] Rather, "Rule 901(a) treats preliminary

52. *Lorraine*, 241 F.R.D. at 542.

53. *See infra* Section III.C (discussing relationship of relevancy, authentication, and the business record).

54. United States v. Browne, 834 F.3d 403, 405 (3d Cir. 2016) ("The advent of social media has presented the courts with new challenges, . . . including in the way data is authenticated under the Federal Rules of Evidence—a prerequisite to admissibility at trial.").

55. Kerr, *supra* note 29, at 26.

56. FED. R. EVID. 901(a); *see also* United States v. Jones, 107 F.3d 1147, 1150 n.1 (6th Cir. 1997).

57. Tienda v. State, 358 S.W.3d 633, 638 (Tex. Crim. App. 2012).

58. Jones v. State, 572 S.W.3d 841, 848 (Tex. App. 2019) (quoting Campbell v. State, 382 S.W.3d 545, 549 (Tex. App. 2012)); *see also* Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 541-42 (D. Md. 2007) (holding that to ensure trustworthiness, the "requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims").

questions of authentication and identification as matters of conditional relevance according to the standards of Rule 104(b)."[59] "The rest is up to the jury."[60]

Rule 901 does not specify the amount of proof required to authenticate. Rather, the "type and quantum of evidence required is related to the purpose for which the evidence is offered, and depends upon a context-specific determination whether the proof advanced is sufficient to support a finding that the item in question is what its proponent claims it to be."[61] The burden of proof is low and requires only prima facie evidence.[62] Ultimately, determining if the evidence is what the proponent claims is a matter for the jury.[63] In other words, "[a]uthentication does not conclusively establish the genuineness of an item; it is a foundation that a jury may reject."[64] If the foundational evidence offered to establish authenticity is weak, "the opposing party 'remains free to challenge the reliability of the evidence, to minimize its importance, or to argue alternative interpretations of its meaning, but these and similar other challenges go to the weight of the evidence—not to its admissibility.'"[65]

Authentication under Rule 901 can be accomplished in a variety of ways. Rule 901(b) identifies ten allowable methods of authentication with extrinsic evidence: (1) testimony of a witness with knowledge, (2) nonexpert opinion about handwriting, (3) comparison by an expert witness or the trier of fact, (4) distinctive characteristics and the like, (5) opinion about a voice, (6) evidence about a telephone conversation, (7) evidence about public records, (8) evidence about ancient documents or data compilations, (9) evidence about

59. United States v. Reilly, 33 F.3d 1396, 1404 (3d Cir. 1994) (quoting Jack B. Weinstein & Margaret A. Berger, 5 WEINSTEIN'S EVIDENCE ¶ 901(a)[01] at 901-15 (1993)).

60. United States v. Vayner, 769 F.3d 125, 130 (2d Cir. 2014) (holding "[t]he ultimate determination as to whether the evidence is, in fact, what its proponent claims is thereafter a matter for the jury."); *see also Lorraine*, 241 F.R.D. at 541-42.

61. *Vayner*, 769 F.3d at 130 (internal citation omitted) (internal quotation marks omitted).

62. *See* People v. Glover, 2015 COA 16, ¶ 30, 363 P.3d 736 (explaining the burden "presents a low bar; only a prima facie showing is required"); State v. Green, 830 S.E.2d 711, 714 (S.C. Ct. App. 2019) (quoting United States v. Davis, 918 F.3d 397, 402 (4th Cir. 2019) ("The court decides whether a reasonable jury could find the evidence authentic; therefore, the proponent need only make 'a prima facie showing that the 'true author' is who the proponent claims it to be.") (quotation marks omitted).

63. *Vayner*, 769 F.3d at 130.

64. United States v. Khorozian, 333 F.3d 498, 506 (3d Cir. 2003); *see also* FED. R. EVID. 104(e).

65. *Vayner*, 769 F.3d at 131 (quoting United States v. Tin Yat Chin, 371 F.3d 31, 38 (2d Cir. 2004)).

a process or system, and (10) methods provided by a statute or rule.[66] The enumerated methods in Rule 901(b) are not exclusive.[67]

For decades, courts have applied the rules of evidence to admit traditional forms of evidence. However, authenticating ESI presents a variety of issues due to rapid technology advancements that are "often new to many judges" and the "complexity" or "novelty" of ESI, with the heightened possibility of manipulation, requires greater scrutiny of "the foundational requirements" to ensure reliability.[68] Although like traditional evidence in many respects, issues relating to admission of ESI have prompted consideration of whether ESI requires different rules.

a. Rule 901: To Change or Not To Change; That was the Question

In October 2014, the Federal Rules of Evidence Advisory Committee considered proposals to amend Rule 901 to provide detailed grounds for authenticating ESI.[69] The Committee decided rulemaking was not the appropriate response to concerns over admission of ESI.[70] The Committee's primary rationale was that the federal rules were broad and flexible enough to accommodate admission of ESI.[71] The Committee also recognized that adopting new rules detailing authentication of ESI was problematic for reasons including that weighing authenticity factors cannot easily be encapsulated in a rule and must be determined on a case-by-case basis.[72] The Committee cautioned, "the deliberate nature of the rulemaking process raises the danger that specifically stated grounds of authenticity for electronic evidence will be outmoded before they are even enacted. Such rules would probably have to be constantly amended to keep up with technology."[73] Ultimately, the Committee did not recommend proposed amendments to Rule 901 that would have provided detailed standards for authenticating ESI.[74]

Courts also have struggled with the question whether the current evidentiary rules adequately accommodate attempted admission of ESI. Ultimately,

---

66. *See* FED. R. EVID. 901(b)(1)-(10).

67. FED. R. EVID. 901(b) advisory committee's note to 1972 proposed rules (stating the methods listed are "not intended as an exclusive enumeration of allowable methods but are meant to guide and suggest, leaving room for growth and development in this area of the law").

68. Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 543-44 (D. Md. 2007) (quoting Jack B. Weinstein & Margaret A. Berger, WEINSTEIN'S FEDERAL EVIDENCE § 900.06[3] (Joseph M. McLaughlin ed., Matthew Bender (2d ed. 1997))).

69. *See* ADVISORY COMM. ON EVIDENCE RULES, MINUTES OF THE MEETING OF OCTOBER 24, 2014, at 8.

70. *See id.* at 9.

71. *See id.*

72. *See id.*

73. *See id.*

74. *See id.*

they generally agree the current evidentiary rule scheme is broad and flexible enough to address admissibility of ESI. For example, in *State v. Green*,[75] the Court of Appeals of South Carolina acknowledged "[s]ocial media messages and other content may appear to pose unique authentication problems, but these problems dissolve against the framework of Rule 901."[76] The Court explained, "[s]ocial media messages and content are writings, and evidence law has always viewed the authorship of writings with a skeptical eye."[77] The Court stressed Rule 901 "does not care what form the writing takes, be it a letter, a telegram, a postcard, a fax, an email, a text, graffiti, a billboard, or a Facebook message."[78] All that matters is whether the proposed evidence can be authenticated to avoid fraud.[79] The *Green* court further explained:

> The vulnerability of the written word to fraud did not begin with the arrival of the internet, for history has shown a quill pen can forge as easily as a keystroke, letterhead stationery can be stolen or manipulated, documents can be tricked up, and telegrams can be sent by posers. Viewed against this history, the argument that social media should bear a heavier authentication burden because such a "modern" medium is particularly vulnerable to fraudsters may be seen for what it is: old wine in a new bottle.[80]

The Pennsylvania Superior Court also rejected the argument that unique rules for authentication are needed. That Court stated, "[w]e see no justification for constructing unique rules for admissibility of electronic communications . . . ."[81] The Sixth Circuit similarly concluded, "it is not at all clear . . . why our rules of evidence would treat electronic photos that police stumble across on Facebook one way and physical photos that police stumble across lying on a sidewalk a different way."[82]

---

75. 830 S.E.2d 711 (S.C. Ct. App. 2019).

76. *Green*, 830 S.E.2d at 714.

77. *Id.* (citing 2 MCCORMICK ON EVIDENCE § 221 (7th ed. 2016)) (explaining that rather than assuming authorship, evidence law adopts "the position that the purported signature or recital of authorship on the face of a writing is not sufficient proof of authenticity to secure the admission of the writing into evidence").

78. *Id.*

79. *Id.* (citing 2 MCCORMICK ON EVIDENCE § 221) (explaining Rule 901 was enacted to deter fraud).

80. *Id.* at 714-15.

81. *In re* F.P., 878 A.2d 91, 95 (Pa. Super. Ct. 2005) (explaining that "[e]ssentially, appellant would have us create a whole new body of law just to deal with e-mails or instant messages. . . . We believe that e-mail messages and similar forms of electronic communications can be properly authenticated within the existing framework of [the rules of evidence][.]").

82. United States v. Farrad, 895 F.3d 859, 879-80 (6th Cir. 2018).

In contrast, other courts[83] and commentators argue the current evidentiary rule scheme does not sufficiently accommodate ESI:

> The current evidentiary scheme comprises three main historical policies: (1) the notion of authentic writings, exemplified by the search for an "original" object tying certain people, acting at a certain time, to certain permanently recorded information; (2) the rule against hearsay, giving litigants the right to test factual statements through cross examination, unless there was an accepted policy reason not to do so; and (3) the notion that evidence, particularly evidence implicating specialized knowledge, be generally scientific in that it be subject to a "test" of its hypotheses or methodologies. These policies are all stressed by digital evidence . . . . There is now a new world of [digital] evidence. New foundations are necessary.[84]

Recently, in *State v. Allcock*,[85] the Vermont Supreme Court reviewed the competing views among courts and concluded "the rules of evidence already in place for determining authenticity" are sufficient for evaluating ESI.[86] The Court noted "the typical authentication rules are sufficient for social media communications, although we emphasize that courts must be careful not to treat social media accounts as any more self-authenticating than other comparable communications."[87] The *Allcock* court cautioned:

> [I]n determining the authenticity of social media evidence, courts must be sure not to apply a more lenient standard of authenticity compared to other types of documents. A mere assertion that a Facebook page belongs to a specific person is no more self-authenti-

---

83. *See, e.g.*, Griffin v. State, 19 A.3d 415, 423 (Md. 2011) (adopting heightened standard for authenticating ESI); Parker v. State, 85 A.3d 682, 685-86 (Del. 2014) (same); Sublet v. State, 113 A.3d 695, 712 (Md. 2015) (same).

84. 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, 361-62 (2015) (quoting GEORGE L. PAUL, FOUNDATIONS OF DIGITAL EVIDENCE 13-14 (2007)).

85. 2020 VT 60, 237 A.3d 648.

86. *See Allcock*, 2020 VT 60, ¶ 13 (quoting Tienda v. State, 358 S.W.3d 633, 638-39 (Tex. Crim. App. 2012) (holding "[c]ourts and legal commentators have reached a virtual consensus that, although rapidly developing electronic communications technology often presents new and protean issues with respect to the admissibility of electronically generated, transmitted and/or stored information, including information found on social networking web sites, the rules of evidence already in place for determining authenticity are at least generally adequate to the task"); *see also* State v. Hannah, 151 A.3d 99, 106 (N.J. App. Div. 2016) (reasoning that "a tweet can be easily forged, but so can a letter or any other kind of writing" and declining to "create a new test for social media postings"); *Parker*, 85 A.3d at 687 ("Although we are mindful of the concern that social media evidence could be falsified, the existing Rules of Evidence provide an appropriate framework for determining admissibility.").

87. *Allcock*, 2020 VT 60, ¶ 10 (applying V.R.E. 901, the State's equivalent to FED. R. EVID. 901).

> cating than a flyer posted in a public square that includes the statement, "This message is from Jane Doe." Absent sufficient other evidence that such a flyer was, in fact, written by or on behalf of Jane Doe, the statements in the flyer would not be admissible as Jane Doe's statements.[88]

While courts may not agree on whether different rules are needed to accommodate ESI, all courts recognize that "[u]ltimately, however, [for paper and electronic records] it all boils down to the same question of assurance that the record is what it purports to be."[89]

b. Rule 901 Foundation: Type, Quantum, Approach

As with traditional evidence, a proponent can authenticate computer-stored social media evidence using a variety of evidence. The Third Circuit explains that "it is no less proper to consider a wide range of evidence for the authentication of social media records than it is for more traditional documentary evidence."[90] The Court recognized the additional challenges presented by the intricacies arising in authenticating ESI generally and those particular to social media content:

> The authentication of electronically stored information in general requires consideration of the ways in which such data can be manipulated or corrupted, . . . and the authentication of social media evidence in particular presents some special challenges because of the great ease with which a social media account may be falsified or a legitimate account may be accessed by an imposter. . . . But the authentication rules do not lose their logical and legal force as a result.[91]

The foundational evidence used for authentication under Rule 901 may be direct or circumstantial. Often, "distinctive characteristics" of a document alone can provide circumstantial evidence sufficient for authentication.[92] A proponent may use the nonexclusive methods identified under Rule 901(b)

---

88. *Id.* ¶ 15.

89. *In re* Vee Vinhnee, 336 B.R. 437, 445 (B.A.P. 9th Cir. 2005); *see also Parker*, 85 A.3d at 687 (holding "[t]he requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.") (citation omitted).

90. United States v. Browne, 834 F.3d 403, 412 (3d Cir. 2016).

91. *Id.*

92. United States v. Vayner, 769 F.3d 125, 132 (2d Cir. 2014) (citing FED. R. EVID. 901(b)). *See, e.g.*, United States v. Maldonado-Rivera, 922 F.2d 934, 957 (2d Cir. 1990) (holding when writing was not a matter of common knowledge that "distinctive characteristics of the document itself, such as its appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with the circumstances" may provide sufficient foundation for authentication).

or methods outside the list to do so.[93] Regardless of the method used to authenticate social media content under Rule 901, the expectation is clear:

> [T]he proponent of social media evidence must present direct or circumstantial evidence that tends to corroborate the identity of the author of the communication in question, such as testimony from the person who sent or received the communication, or contextual clues in the communication tending to reveal the identity of the sender.[94]

Courts must be flexible and "consider the unique facts and circumstances in each case—the purpose for which the evidence is being offered—in deciding whether the evidence has been properly authenticated."[95] Courts and commentators[96] recognize cases seemingly are split into two primary methods of authenticating social media. These historical methods have been used to teach what has become referred to as the Maryland Approach[97] and the Texas Approach.[98] While an analysis of those approaches is not necessary for purposes of this article, the Delaware court's description of the differences is instructive:

> Under the Maryland approach, social media evidence may only be authenticated through the testimony of the creator, documentation of the internet history or hard drive of the purported creator's computer, or information obtained directly from the social networking site. Unless the proponent can demonstrate the authenticity of the social media post to the trial judge using these exacting requirements, the social media evidence will not be admitted and the jury cannot use it in their factual determination. Under this approach, social media evidence is only authenticated and admissible where the proponent can convince the trial judge that the social media post was not falsified or created by another user. . . . The Texas approach involves a lower hurdle than the Maryland approach, because it is for the jury—not the trial judge—to resolve issues of fact, especially

---

93. FED. R. EVID. 901(b)(1)-(10).

94. Commonwealth v. Mangel, 181 A.3d 1154, 1162 (Pa. Super. Ct. 2018); *see also Vayner*, 769 F.3d at 130 (stating the "proof of authentication may be direct or circumstantial") (citation omitted); *see, e.g.*, United States v. Vazquez-Soto, 939 F.3d 365, 374 (1st Cir. 2019) (holding that "[a] photograph's contents, buttressed by indirect or circumstantial evidence, can form a sufficient basis for authentication even without the testimony of the photographer or some other person who was present at the time it was taken.") (citation omitted).

95. *Mangel*, 181 A.3d at 1161.

96. *See, e.g.*, Paul W. Grimm, et al., *Authentication of Social Media Evidence*, 36 AM. J. TRIAL ADVOC. 433, 437 (2013) (explaining that courts are split and describing *Griffin* and *Tienda* as examples of the varying approaches).

97. Griffin v. State, 19 A.3d 415, 425 (Md. 2011) (adopting Maryland approach); *but see* Sublet v. State, 113 A.3d 695, 712 (Md. 2015).

98. Tienda v. State, 358 S.W.3d 633, 638 (Tex. Crim. App. 2012) (adopting Texas approach).

where the opposing party wishes to challenge the authenticity of the social media evidence.[99]

It is notable that, although in *Griffin* the Maryland Court of Appeals required "greater scrutiny" to authenticate social media communications, the Court later relaxed the standard and adopted the rationale under *United States v. Vayner*.[100] In doing so, the Maryland Court subsequently held in *Sublet* that an item be what it is purported to be "is satisfied if sufficient proof has been introduced so that a reasonable juror could find in favor of authenticity or identification."[101] Thus, the Maryland Court more closely aligned with both the Texas approach and the plain words of Rule 901.

Regardless of the approach utilized, courts acknowledge that authorship is key to determining whether the proffered social media content is what it is purported to be. Authorship "may be met with various forms of evidence, including 'testimony that an item is what it is claimed to be' or evidence of 'the appearance contends, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances."[102] The type and quantum of foundational evidence necessary to establish authorship varies. However, caselaw establishes that corroborating evidence is necessary tying the person to the content beyond merely confirming the social media account is registered to the alleged author.[103]

c. Rule 901 Cases: Properly Rejecting ESI Because of Insufficient Foundation

Courts repeatedly have rejected social media content for lack of proper authentication under Rule 901 when sufficient foundational evidence linking the defendant to the content was not presented.[104] In doing so, the tribunals have correctly focused on the lack of evidence connecting the purported author to the computer-stored content.

A textbook example of how social media evidence should be authenticated under Rule 901, and what considerations appellate courts should em-

---

99. Parker v. State, 85 A.3d 682, 688 (Del. 2014).

100. *Sublet,* 113 A.3d at 715 (quoting United States v. Vayner, 769 F.3d 125, 129-30 (2d Cir. 2014)).

101. *Id.* (quoting *Vayner*, 769 F.3d at 129-30).

102. United States v. Vazquez-Soto, 939 F.3d 365, 373 (1st Cir. 2019) (citing FED. R. EVID. 901(b)(1), (4)).

103. *See, e.g.,* People v. Glover, 2015 COA 16, ¶ 30, 363 P.3d 736 (applying C.R.E. 901, the State's equivalent to FED. R. EVID. 901, the Court explains that to demonstrate authorship in the context of social media requires "additional corroborating evidence of authorship . . . beyond confirmation that the social networking account is registered to the party purporting to create those messages").

104. The sample of cases provided is not intended to be an exhaustive list of cases holding for the proposition advanced.

ploy in reviewing those cases, can be found by reviewing the Vermont Supreme Court's decision in *State v. Allcock*.[105] There, the defendant argued the trial court erred in admitting inculpatory Facebook messages purportedly authored by the defendant.[106] Salient facts underlying the *Allcock* case included the following:

> The police then executed a search warrant and obtained data from Facebook regarding the page registered in defendant's name, in the form of the Facebook Business Record. The record listed the account holder's name, email addresses, phone numbers, and internet protocol (IP) addresses. It identified "Christina Allcock" as the account holder, but there was no testimony at trial about whether the listed email addresses, phone numbers, and IP addresses belonged to defendant.[107]

Vermont's pertinent rules of evidence are similar to the federal rules. Under the Vermont rules, the Court concluded:

> We hold that the authentication of social media accounts should be assessed under the same standard as any other evidence: a threshold determination of whether "sufficient evidence exist[s] to 'support a finding that the matter in question is what its proponent claims.'" However, even under that standard, we hold that the admission of the Facebook messages was an abuse of discretion.[108]

In route to its holding, the Court in *Allcock* made the following important conclusions:

- "[T]he authentication of social media accounts should be assessed under the same standard as any other evidence: a threshold determination of whether 'sufficient evidence exist[s] to "support a finding that the matter in question is what its proponent claims."'"[109]
- After discussing the Maryland and the Texas approaches, held "[w]e agree that trial courts should evaluate the authenticity of social media communications under the same standard as other evidence."[110]

105. 2020 VT 60, 237 A.3d 648.
106. *Allcock*, 2020 VT 60, ¶ 1.
107. *Id.* ¶ 6.
108. *Id.* ¶ 9 (citation omitted).
109. *Id.*
110. *Id.* ¶ 14.

- "[I]n determining the authenticity of social media evidence, courts must be sure not to apply a more lenient standard of authenticity compared to other types of documents."[111]
- "A mere assertion that a Facebook page belongs to a specific person is no more self-authenticating than a flyer posted in a public square that includes the statement, 'This message is from Jane Doe.'"[112]
- "[T]he messages cannot be authenticated merely by the fact that the account from which the messages were sent purported to be that of defendant Christina Allcock."[113]
- "[T]he fact that the Facebook Business Record showed that the account was registered in defendant's name likewise does not provide sufficient information from which a jury could conclude that the account belonged to defendant and that she sent the messages at issue. It proves that the messages were sent from an account that purportedly belongs to defendant—but that fact was and is undisputed."[114]
- "[T]he fact that police were directed to defendant's site by a person who purportedly messaged with defendant does not advance the analysis at all."[115]
- "The question for purposes of authentication is whether there is sufficient evidence that defendant actually sent the messages from the 'Christina Allcock' account. The recipient did not testify about his basis for believing that the messages in question did, in fact, come from defendant; in fact, there is no record evidence that he even held such a belief. In short, as to the question whether the messages could be authenticated as having come from defendant, the trooper's passing reference to a report from a person who received the messages adds nothing."[116]
- "[T]he fact that the police officers reviewed the Facebook account at issue and concluded that it was defendant's is irrelevant. The question before the court was whether there was sufficient evidence from which the jury could conclude that defendant sent the messages at issue. The police officers' conclusion that there

111. *Id.* ¶ 15.

112. *Id.*

113. *Id.* ¶ 17. The Court also noted, "[i]t is not only theoretically possible for a person to set up a social media account purporting to belong to someone else; it is relatively common. By November 2019, Facebook had removed more than five billion fake accounts in 2019, up from 3.3 billion in 2018." *Id.* ¶ 18 (citation omitted).

114. *Id.* ¶ 20.

115. *Id.* ¶ 21.

116. *Id.*

was evidence connecting the messages to defendant is not evidence . . . ."[117]

- "Finally, without further evidence, there is nothing about the content of the messages that authenticates them as having been written by the defendant."[118]

In *United States v. Vayner*,[119] the Second Circuit Court of Appeals vacated the district court and remanded for a retrial, holding the false identification document offered by the government was not properly authenticated under Fed. R. Evid. 901 because the defendant was not linked to the page.[120] There, the defendant was charged with transfer of a false identification document.[121] The Court ruled the prosecution did not provide a sufficient basis on which a jury could find the proffered website printout was what it was claimed to be—the defendant's profile page from a Russian social networking website similar to Facebook.[122] The Court determined the government did not present extrinsic evidence tying the defendant to creating the page or showing he was responsible for its content.[123] In deciding the evidence was inadmissible for lack of proper authentication, the Court held "the mere fact that a page with [defendant's] name and photograph happened to exist on the Internet at the time of [the special agent's] testimony does not permit a reasonable conclusion that this page was created by the defendant or on his behalf."[124]

Similarly, in *Commonwealth v. Mangel*,[125] the Superior Court of Pennsylvania affirmed the trial court, holding Facebook messages were not properly authenticated under Pa. R. Evid. 901[126] when the government did not present direct or circumstantial evidence connecting the defendant to creating the Facebook account, authoring the chat messages, or posting the photograph of the bloody hands.[127] The fact the account had the defendant's name, hometown, and high school was not sufficient to authenticate that he actually authored the content in the chat messages.[128] It was significant to the Court that the government failed to establish the time (lack of date and

117. *Id.* ¶ 22.
118. *Id.* ¶ 23.
119. 769 F.3d 125 (2d Cir. 2014).
120. *Vayner*, 769 F.3d at 127.
121. *Id.*
122. *Id.* at 132.
123. *Id.* at 131.
124. *Id.* at 132.
125. 181 A.3d 1154 (Pa. Super. Ct. 2018).
126. *Mangel*, 181 A.3d at 1164 (applying PA. R. EVID. 901, the State's equivalent to FED. R. EVID. 901).
127. *Id.* at 1163.
128. *Id.*

timestamps) the posts and messages were made.[129] Further, the posts about the incident did not reference the defendant; rather, others did in their response posts.[130] The Court also was critical in that the posts and messages were ambiguous and did not specifically relate to the alleged incident, and the government did not provide evidence of distinctive characteristics showing the defendant was the author.[131]

In the interest of space, I simply note that many other courts have rejected social media evidence for lack of proper authentication under Rule 901.[132] In the final analysis, those courts also concluded insufficient foundation linked the content to the individual, thereby failing to establish what it purported to be.

d. Rule 901 Cases: Improperly Admitting ESI Without Sufficient Foundation

In contrast to the cases above, some courts have admitted user-generated social media content as properly authenticated under Rule 901 based on what I believe was inadequate foundation. For example, in *United States v. Quintana*,[133] the Sixth Circuit held that even if the district court erred in authenticating the Facebook records the government submitted as self-authenticating business records,[134] the error was harmless because circumstantial evidence linked the defendant to the account, establishing proper authentication under Rule 901.[135] In *Quintana*, the defendant argued "his name, two emails (one of which was his name, and the other his moniker), and a telephone number—did not contain sufficient 'distinctive characteristics' under Fed. R. Evid.

---

129. *Id.*

130. *Id.*

131. *Id.* at 1163-64.

132. Examples of jurisdictions that have held social media content was not properly authenticated include United States v. Jackson, 208 F.3d 633, 638 (7th Cir. 2000) (holding a website posting was not properly authenticated because the proponent did not establish the group actually authored the posting instead of merely improperly accessing the website); State v. Smith, 136 So.3d 424, 434 (Miss. 2014) (holding the State failed to make a prima facie showing the defendant actually sent the message; the name and photograph on a Facebook printout did not sufficiently link the alleged author to the message); Dering v. State, 465 S.W.3d 668, 672 (Tex. 2015) (holding a Facebook post on a third party's account by other persons was not properly authenticated when the witness was not the owner of the account on which the post was made or the owner of any alleged posters accounts); Sublet v. State, 113 A.3d 695, 672-73 (Md. 2015) (holding exclusion of evidence was appropriate because the Facebook timeline was not properly authenticated after a witness testified she did not author the posts, others had access to her account, passwords, and regularly posted on her account; and no evidence was presented establishing unique characteristics supporting authentication); State v. Allcock, 2020 VT 60, ¶¶ 16-27, 237 A.3d 648 (holding the trial court improperly admitted Facebook messages because the State failed to offer sufficient evidence to properly authenticate them and explaining what the State could have but failed to do to properly authenticate).

133. United States v. Quintana, 763 F. App'x 422 (6th Cir. 2019).

134. The district court did err, as is more fully discussed below. *See infra* note 135.

135. *Quintana*, 763 F. App'x at 427.

901(b)(4) to authenticate the records given that the government offered no evidence linking him to the email addresses and phone number."[136] The *Quintana* court acknowledged "the government could have done more to connect the Facebook profile to Quintana" like tracking Facebook pages and accounts to IP addresses and telephone numbers.[137] Nonetheless, the Court concluded the foundation was sufficient to support authentication under Rule 901 because evidence established "an account in defendant's name, an email address with his name and moniker, a location linked to defendant, dates that correspond to witness testimony, and a picture of defendant."[138]

In *Commonwealth v. Meola*,[139] the Massachusetts Court of Appeals affirmed the district court, holding a social media message and an attached sexually explicit video were properly authenticated under Mass. G. Evid. 901 through "confirming circumstances" linked to the defendant.[140] The Court explained that a judge making the threshold determination that a defendant sent the message may consider circumstantial evidence and look to confirming circumstances sufficient for a reasonable jury to find the defendant authored the message.[141] The Court held that confirming circumstances included the message was sent from the account in the defendant's name, the video revealed highly intimate and personal details about the defendant and was self-authored, and the message included a profile picture of the defendant's biological daughter.[142]

e. Rule 901 Cases: Properly Admitting ESI With Sufficient Foundation

In comparison, other courts have admitted evidence from social media content as properly authenticated under Rule 901 when sufficient circumstantial evidence linked the defendant to the content. The following cases are both instructive and worthy of emulation.[143]

In *United States v. Barnes*,[144] the Fifth Circuit Court of Appeals affirmed the district court, holding the government presented sufficient foundational

---

136. *Id.* at 426.

137. *Id.* at 427 (citing United States v. Hassan, 742 F.3d 104, 133 (4th Cir. 2014)).

138. *Id.* The *Quintana* court relied on *United States v. Farrad*, 895 F.3d 859 (6th Cir. 2018), which held that admitting the photographs taken from Facebook as self-authenticating business records was error; however, the error was harmless because the records were properly authenticated under Rule 901 through extrinsic evidence. *Farrad*, 895 F.3d. at 880.

139. 125 N.E.3d 103 (Mass. App. Ct. 2019).

140. Commonwealth v. Meola, 125 N.E.3d 103, 113-14 (Mass. App. Ct. 2019) (applying MASS. G. EVID. 901, the State's equivalent to FED. R. EVID. 901).

141. *Id.* at 115.

142. *Id.*

143. This is merely a sample of cases and is not intended to be an exhaustive list of cases holding for the proposition reviewed.

144. 803 F.3d 209 (5th Cir. 2015).

evidence to authenticate the Facebook and text messages.[145] Specifically, a witness testified she saw the quadriplegic defendant use the website, recognized his account on the website, and the message matched his way of communicating.[146] She also testified the defendant could send messages from his cell phone, she spoke to him at the phone number in the texts, and the text messages indicated they were from him.[147] The Court concluded sufficient evidence was presented to link the defendant to the text message content.[148] The Court reasoned that, although the witness "was not certain that [the defendant] authored the messages, conclusive proof of authenticity [was] not required for the admission of disputed evidence" because "the jury holds the ultimate responsibility for evaluating the reliability of the evidence."[149]

In *United States v. Browne*,[150] the Third Circuit Court of Appeals affirmed the district court, holding the Facebook message "chats" were properly authenticated under Fed. R. Evid. 901 because the postings were properly authenticated by extrinsic evidence including witnesses' testimony that established accuracy of the chat logs and linked them to the defendant.[151] The Court initially concluded the chats were not self-authenticating evidence under 902(11) and 803(6), the business records rule.[152] The *Browne* holding will be discussed in more detail later under a review of the business records rule.

In *United States v. Encarnacion-Lafontaine*,[153] the Second Circuit Court of Appeals affirmed the district court, holding the Facebook messages were properly authenticated under Fed. R. Evid. 901 by relying on circumstantial evidence linking the defendant to the accounts.[154] The Court concluded significant evidence existed from which a jury could reasonably find the defendant controlled the accounts used to make threats resulting in criminal charges.[155] Specifically, the Court determined the government presented enough evidence showing the Facebook accounts used to send the threats were accessed from IP addresses connected to computers near the defendant's apartment; patterns of account access showed the same person controlled the accounts; the accounts were used to send messages to other individuals connected to the defendant; the defendant had motive to make the

145. *Barnes*, 803 F.3d 209 at 217.
146. *Id*.
147. *Id*.
148. *Id*.
149. *Id*. (citing United States v. Barlow, 568 F.3d 215, 220 (5th Cir. 2009)).
150. 834 F.3d 403 (3d Cir. 2016).
151. *Browne*, 834 F.3d at 415.
152. *Id*. at 411.
153. 639 F. App'x 710 (2d Cir. 2016).
154. *Encarnacion-Lafontaine*, 639 F. App'x at 713.
155. *Id*.

threats; and limited people, including the defendant, knew the information contained in the messages.[156]

In *United States v. Lewisbey*,[157] the Seventh Circuit Court of Appeals affirmed the district court, holding that text messages and Facebook posts relating to a gunrunning business were linked to the defendant and properly authenticated under Fed. R. Evid. 901.[158] The Court concluded that "[t]o authenticate the text messages, the government needed only to 'produce evidence sufficient to support a finding' that the messages were actually sent and received" by the defendant.[159] The Court concluded the government met its burden by establishing an iPhone and a Samsung cell phone belonged to the defendant evidenced by the location where each device was confiscated. Further, the Court noted the defendant admitted the posts were his, and circumstantial evidence linked him to the Facebook account on which the posts were made including his nickname, date of birth, address, email address, and more than 100 photos of him matched photos on his cell phones.[160]

In *United States v. Barber*,[161] the Seventh Circuit Court of Appeals affirmed the district court, holding social media records and messages used in a firearms case were properly authenticated under Fed. R. Evid. 901.[162] The defendant argued the government failed to lay sufficient foundation to establish the Facebook account was his.[163] A digital-media collection specialist testified the website account was "friends" with many of the defendant's known associates; the account had pictures of the defendant; the account was linked to a cell phone number the defendant provided to others, and testimony of his friend confirmed the defendant used Facebook to coordinate in-person meetings.[164] The Court concluded the evidence presented was enough for a reasonable jury to conclude that the account belonged to the defendant.[165]

These cases, and others,[166] demonstrate the type and quantum of foundational evidence necessary to authenticate social media content as admissi-

156. *Id.*
157. 843 F.3d 653 (7th Cir. 2016).
158. *Lewisbey*, 843 F.3d at 658.
159. *Id.*
160. *Id.* at 658-59.
161. 937 F.3d 965 (7th Cir. 2019).
162. *Barber*, 937 F.3d at 970-71.
163. *Id.* at 969-70.
164. *Id.*
165. *Id. at* 971.
166. *See, e.g.*, State v. Green, 830 S.E.2d 711, 715-16 (S.C. Ct. App. 2019) (holding, in a murder and desecration of human remains case, that direct messages from the victim's Facebook account contained sufficient distinctive characteristics for authentication under Rule 901 in that messages were from the Facebook account associated with the defendant's girlfriend, mentioned the name of his girlfriend's sister, and stated his home address); Commonwealth v. Danzey, 210

ble under Rule 901 varies. The cases also demonstrate the foundational evidence presented must be sufficient to support that the item in question is what its proponent claims it to be. If the proponent claims the proffered evidence to be a factual assertion made by an individual, foundational evidence linking the individual to the content must be presented.

2. Rule 902. Self-authentication

Rule 902 provides for self-authenticating certain types of evidence without the need for extrinsic evidence. The main difference between Rules 901 and 902 is that, under Rule 902, the foundation establishing self-authenticity is found on the face of the evidence with no extrinsic evidence necessary.[167] This does not mean the authentication requirement under Rule 902 is lower than the requirement under Rule 901.[168] Rather, it means the authentication requirement that "the item is what the proponent claims" under Rule 901 may be satisfied by a different means.[169] Both rules require enough foundational evidence for a reasonable person to find that "the item is what the proponent claims it is."[170]

Rule 901 establishes what a proponent must do "[t]o satisfy the requirement of authenticating,"[171] and Rule 902 lays out the "items of evidence

---

A.3d 333, 339-40 (Pa. Super. 2019) (holding ample evidence supported defendant owned the Facebook and Instagram accounts; further photographic evidence of postings in a stalking and harassment prosecution case were properly authenticated under PA. R. EVID. 901, the State's equivalent of FED. R. EVID. 901, by circumstantial evidence showing the defendant owned the accounts and posts contained contextual clues linking the defendant to the victim); United States v. Vazquez-Soto, 939 F.3d 365, 373 (1st Cir. 2019) (holding photographic evidence from Facebook was properly authenticated under Rule 901 because a jury could reasonably infer the photos were taken during a time when he claimed to be totally disabled and receiving federal disability benefits; some photos bore date stamp, others included similar features); People v. Dominguez-Castor, 2020 COA 1, ¶¶ 58-60, 469 P.3d 514 (holding the Facebook messages properly authenticated under COLO. R. EVID. 901, the State's equivalent to FED. R. EVID. 901, and the content of the messages were not inadmissible hearsay relying on a variety of circumstances including the phone belonged to the defendant and he had the phone when he was arrested, the account was registered in the defendant's name and was created using his email address, the messages were sent through the Facebook messenger on his phone, no evidence the other individual had access to or possessed the phone code, the messages on his phone also referred to his plan to leave the state, and there was no evidence he told the other person of his travel plans); State v. Sample, 228 A.3d 171, 198 (Md. 2020) (holding sufficient circumstantial evidence was presented to show a reasonable juror could find it was more likely than not the social media profile belonged to defendant; the unfriending happened the day after the attempted armed robbery; the defendant had incentive to distance himself from Mayo; and evidence established the SoLo Haze profile belonged to Sample and the claude.mayo.5 profile belonged to Mayo). This is merely a sample of additional cases and is not intended to be an exhaustive list of cases holding for the proposition reviewed.

167. Paul W. Grimm, et al., *Authenticating Digital Evidence*, 69 BAYLOR L. REV. 1 n.82 (2017).

168. *See infra* Section III.C.

169. *Compare* FED. R. EVID. 901, *with* 902.

170. FED. R. EVID. 901(a).

171. *Id.*

[that] are self-authenticating" and "require no extrinsic evidence of authenticity in order to be admitted."[172] It is unimportant to the factfinder whether the required foundational evidence is presented through direct evidence (Rule 901), extrinsic evidence (Rule 901), or certification (Rule 902). All that is important is that sufficient foundational evidence is presented. As commentators have observed, the provision allowing for self-authentication enacted as Rule 902 easily could have been included under the methods for authentication enumerated in Rule 901(b) without losing its function.[173]

Rule 902 provides twelve nonexclusive examples of self-authentication; the remainder of this article focuses on subsection (11) allowing for self-authentication of business records.[174] Because compliance with Rule 902(11) requires satisfying Rule 803(6)(A)-(C), courts typically analyze the authenticity issue in tandem with the business records hearsay rule. However, that analysis sometimes mistakenly converts a Rule 902(11) authentication consideration into a Rule 803(6) reliability-of-the-evidence determination. The converted analysis is a mistake because, while the questions whether an item is reliable and whether it is genuine are similar, the rules serve different purposes.[175] As explained by a California Court of Appeals, "[A]uthentication alone does not overcome other rules of evidence, such as the hearsay rule. There is a difference between the foundational device of authentication and substantive rules of admissibility of evidence, such as the hearsay rule."[176] The Court concluded, "[t]hus, authentication of a writing is independent of the question of whether the content of the writing is inadmissible as hearsay."[177]

a. Rule 902(11) and Rule 803(6): Working In Concert

Under Rule 902(11), Fed. R. Evid., extrinsic evidence of authenticity is not required for a business record that satisfies Rule 803(6)(A)-(C). A helpful

---

172. FED. R. EVID. 902.

173. Grimm, et al., *supra* note 167, at n.82 (stating the "factors in Rule 902 could have just been added to the list of factors in Rule 901(b) without any loss of utility"). The commentators explained "[t]he examples of authenticity provided in Rule 901(b) essentially are given the same effect as the conditions establishing self-authentication under Rule 902, i.e., when met, they satisfy the admissibility standard and the authenticity question becomes a matter of weight for the jury." *Id*.

174. *See, e.g*., FED. R. EVID. 902(11) ("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.").

175. *See* Stockinger v. Feather River Comty. Coll., 4 Cal.Rptr.3d 385, 395 (Cal. Ct. App. 2003).

176. *Id*.

177. *Id*.

explanation of the interplay between these two rules is found in the drafting Committee's notes. In April 1999, the Advisory Committee on Evidence of the United States Judicial Conference reviewed, and subsequently adopted, amendments to Rule 803(6) and 902(11).[178] The Rule 803(6) amendment added that the foundation for admissibility of a business record could be established by "a certification that complies with Rule 902(11)" rather than live testimony. The Rule 803(6) amendment was intended to provide a path for admission of records without the cost and inconvenience of calling a witness at trial.[179]

> As amended, Rule 803(6), Fed. R. Evid. provides:
>
> The following are not excluded by the rule against hearsay, regardless of whether the declarant is available as a witness:
>
> . . .
>
> (6) Records of a Regularly Conducted Activity. A record of an act, event, condition, opinion, or diagnosis if:
>
> (A) the record was made at or near the time by—or from information transmitted by—someone with knowledge;
>
> (B) the record was kept in the course of a regularly conducted activity of a business, organization, occupation, or calling, whether or not for profit;
>
> (C) making the record was a regular practice of that activity;
>
> (D) all these conditions are shown by the testimony of the custodian or another qualified witness, *or by a certification that complies with Rule 902(11) or (12) or with a statute permitting certification*; and
>
> (E) the opponent does not show that the source of information or the method or circumstances of preparation indicate a lack of trustworthiness.[180]

The Rule 902(11) amendment provided a way of "authenticating certain business records, other than through the live testimony of a foundation witness."[181] It was "intended to work in tandem with the amendment to Evidence Rule 803(6)" while providing "similar treatment for domestic records, and

178. *See* ADVISORY COMM. ON EVIDENCE RULES, MINUTES OF THE MEETING OF APRIL 12-13, 1999, at 15-19.

179. *See id*. at 15.

180. FED. R. EVID. 803(6) (emphasis added).

181. *See* ADVISORY COMM. ON EVIDENCE RULES, MINUTES OF THE MEETING OF APRIL 12-13, 1999, at 16.

foreign records in civil cases, as [was] provided for foreign records in criminal cases. . . ."[182] As such, Rule 902(11) was amended to provide:

> The following items of evidence are self-authenticating; they require no extrinsic evidence of authenticity in order to be admitted:
>
> . . .
>
> (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.[183]

Thus, self-authentication under Rule 902(11) requires that the document be a domestic record that "was made at or near the time by—or from information transmitted by—someone with knowledge;" "was kept in the course of a regularly conducted activity of a business, organization, occupation, or calling, whether or not for profit;" and "making the record was a regular practice of that activity."[184]

The history illustrates that 902(11) was intended to work with Rule 803(6) to provide a path for admission of records without the cost and inconvenience of calling a foundational witness at trial.[185] The amendments were not intended to lower the bar necessary for proper authentication or to shortcut a proper analysis of authenticity, relevancy, or hearsay.

In *Rambus, Inc. v. Infineone Technologies AG*,[186] the Court described the relationship between Rule 902(11) and Rule 803(6):

> Thus, the most appropriate way to view Rule 902(11) is as the functional equivalent of testimony offered to authenticate a business record tendered under Rule 803(6) because the declaration permitted by Rule 902(11) serves the same purpose as authenticating testi-

182. *See id*.

183. FED. R. EVID. 902(11).

184. *Compare* FED. R. EVID. 902(11), *with* FED. R. EVID 803(6)(A)-(C).

185. *See, e.g., In re* Vee Vinhnee, 336 B.R. 437, 444 (B.A.P. 9th Cir. 2005) (citing 5 WEINSTEIN § 900.06[2][a]) (explaining that "because the business record foundation commonly covers the ground, the authenticity analysis is merged into the business record analysis without formal focus on the question")).

186. 348 F. Supp. 2d 698 (E.D. Va. 2004).

> mony. Therefore, the declaration must satisfy the substantive criteria set forth in Rule 902(11) in order to lay a proper foundation for admission of the record.[187]

The *Rambus* court was mostly correct. However, it is distracting if not misleading to conceptualize the process as one satisfying Rule 902(11). Rather, for admission under Rule 902(11), satisfaction of Rule 803(6) is required—but not for the sake of reliability under the hearsay rules. Instead, an inquiry whether computer-stored social media content qualifies as a business record must be answered by considering under the authenticity rules whether the item is genuine. Succinctly asked, can a court find the evidence is what the proponent purports based on the certificate from a person who claims it to be a business record?

C. UNDERSTANDING RULE 803(6), FED. R. EVID., THE BUSINESS RECORDS RULE

The origin of the business records rule is found in the English common law "shop book" rule.[188] American courts recognized the English shop book rule and it evolved over the years through common law.[189] Eventually, the concept was codified first as the Commonwealth Fund Act and the Uniform Business Records as Evidence Act, then as the Business Records Act, and finally in 1975 as Federal Rule of Evidence 803(6).[190]

The purpose of the business records rule is to "capture records that are likely accurate and reliable in content, as demonstrated by the trustworthiness of the underlying sources of information and the process by which and purposes for which that information is recorded."[191] The rationale behind the rule lies in the belief that reliability and trustworthiness can be presumed because of the regularity with which a standard business record is kept, its use and importance to the business of the business, how it is kept, and the duty on an employee to accurately keep the record.[192] To qualify under the rule, a record must be a regular conducted activity shown to satisfy all the elements under Rule 803(6)(A)-(C) through "testimony of the custodian or another qualified witness, or by a certification that complies with Rule 902(11)."[193]

---

187. *Rambus*, 348 F. Supp. 2d at 701.

188. PAUL, *supra* note 28, at 120 ("The purpose was to circumvent the prohibition against a party appearing as its own witness. By 1832, the shop-book rule was firmly grounded in English common law, and its scope included all entries made in the ordinary course of business.").

189. *Id.* at 121 (citing MCCORMICK ON EVIDENCE § 286 (5th ed. 1999)).

190. *Id.*

191. United States v. Browne, 834 F.3d 403, 410 (3d Cir. 2016).

192. *See generally* PAUL, *supra* note 28, at 121 (quoting Rudolph J. Peritz, *Computer Data and Reliability: A Call for Authentication of Business Records Under the Federal Rules of Evidence*, 80 NW. U. L. REV. 956, 964 (1986)).

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

The authentication threshold is the same regardless whether the elements are satisfied through testimony or certification.[194]

In *Jackson v. Household Finance Corporation III*,[195] the Florida Supreme Court laid out the business records elements and explained ways those elements can be proven:

> The records proponent can present that information in one of three ways: (1) provide a witness—either the records custodian or other qualified witness—to testify under oath at trial to the statutory requirements; (2) present a certification or declaration from the records custodian or other qualified person that complies with sections 90.803(6)(c) and 90.902(11), Florida Statutes;[196] or (3) stipulate with the opposing party to the admissibility of the documents as business records.[197]

Although the issue in *Jackson* related to witness testimony and not certification from a records custodian, the Court's conclusion is instructive:

> [T]he records proponent's witness must do more than merely echo the statutory elements of the exception and identify employment and familiarity with a different company. The witness must demonstrate that he personally has the sufficient knowledge to affirm the statutory elements of the business records exception by demonstrating personal knowledge of the methods utilized by the business regarding the records at issue, such as how the records were created, what they were used for, and how they were maintained. Otherwise, the business records exception to the hearsay rule becomes a magic-words test rather than a requirement that the records proponent demonstrate the reliability of the business records.[198]

The Court, in *Lorraine v. Markel American Ins. Co.*,[199] also stressed that merely reciting the statute does not satisfy the business records foundational requirement:

> It is necessary, however, that the [foundational] witness provide factual specificity about the process by which the electronically stored information is created, acquired, maintained, and preserved without alteration or change, or the process by which it is produced if the result of a system or process that does so, as opposed to boilerplate,

---

194. *See* Rambus, Inc. v. Infineone Techs. AG, 348 F. Supp. 2d 698, 701 (E.D. Va. 2004).

195. 298 So.3d 531 (Fla. 2020).

196. *Jackson*, 298 So.3d at 543 (Polston, J., dissenting) (applying 90.803(6)(c) and 90.902(11), the State's equivalent to FED. R. EVID. 803(6) and 902(11)).

197. *Id.* (citing Yisrael v. State, 993 So.2d 952, 956-57 (Fla. 2008)).

198. *Id.* at 550.

199. 241 F.R.D. 534 (D. Md. 2007).

> conclusory statements that simply parrot the elements of the business record exception to the hearsay rule . . . .[200]

Thus, to qualify under the business records rule, sufficient foundation must be presented either through testimony at trial or by certification under Rule 902(11) to satisfy the elements of a business record under Rule 803(6). A mere recitation of the elements is not enough.[201] As discussed below, certification by a qualified person that a platform stores user-generated social media content cannot link the author to the content or show the business substantially relied on the content for any business purpose. In the context of Rule 803(6), the custodian cannot testify that the statement contained in the message was made at or near the time by "someone with knowledge."[202] "Messages between users of such a social media platform are thus significantly different from those that the business records exception was designed to encompass."[203] Therefore, "social media communications, when offered to prove the truth of what a user said, fall outside the scope of Rule 803(6), and thus are not self-authenticating under Rule 902(11) when offered for that purpose."[204]

1. Cases Properly Rejecting Evidence Not Satisfying Rules 902(11) and 803(6)

Courts have rejected attempts to authenticate social media content as a business record when the elements of a business record cannot be met through certification, the content's relevancy centers on authorship, and the content was not shown to be compiled as part of a regularly conducted business activity.[205]

In *United States v. Browne*,[206] the Third Circuit Court of Appeals affirmed the district court holding that Facebook message "chats" were not self-authenticating under Fed. R. Evid. 902(11) and 803(6), the business records rule; rather, they required authentication under Fed. R. Evid. 901 by extrinsic evidence.[207] Specifically, the Third Circuit held the defendant's social media postings were not records of a regularly conducted business activity and, thus, were not self-authenticating.[208] The Court noted "any argument to

200. *Lorraine*, 241 F.R.D. at 545-46.
201. *See id.* at 570-72.
202. *Id.* at 570-71.
203. State v. Griffith, 449 P.3d 353, 356 (Ariz. Ct. App. 2019).
204. *Id.* at 357.
205. The cases reviewed in this section are not intended to be exhaustive, but rather are samples of cases instructive for the proposition reviewed.
206. 834 F.3d 403 (3d Cir. 2016).
207. *Browne*, 834 F.3d 403.
208. *Id.* at 409.

the contrary misconceives the relationship between authentication and relevance" and the "purpose of the business records exception."[209]

In *Browne*, Facebook provided sets of chats and a records custodian's certification that the documents "were made and kept by the automated systems of Facebook in the course of regularly conducted activity as a regular practice of Facebook . . . made at or near the time the information was transmitted by the Facebook user."[210] However, the Court concluded Facebook did not claim it relied on the contents of the postings in the course of its business.[211] The custodian only attested the communications took place between the respective Facebook accounts.[212] Because the relevancy of the Facebook records centered on authorship of content, and not merely that communications occurred, the Court ruled the business records rule could not be used to authenticate the posts. Instead, the government was required to submit enough evidence for a jury to "reasonably find, by a preponderance of the evidence, that Browne and the victims authored the Facebook messages at issue."[213] According to the Court, concluding the government satisfied its authentication obligation simply by submitting an attestation would "amount to holding that social media evidence need not be subjected to a 'relevance' assessment prior to admission."[214] The Court explained proper authentication required the government to offer both evidence the webpage existed and the content was tied to the defendant.[215]

In *United States v. Farrad*,[216] the Sixth Circuit Court of Appeals reversed the district court's holding social media photographs of the defendant were properly authenticated under Fed. R. Evid. 902, but affirmed admission under 901.[217] The government offered, as a self-authenticating business record, photos of the defendant with a firearm taken from his Facebook account.[218] The photos also showed his tattoos and distinctive features of his apartment.[219] Farrad argued the photos did not qualify as a business record because Facebook could not authenticate "who took the pictures, when the pictures were taken, by whom or at what time, what they actually showed."[220]

---

209. *Id.*
210. *Id.* at 406.
211. *Id.* at 410.
212. *Id.*
213. *Id.*
214. *Id.*
215. *Id.* (citing United States v. Vayner, 769 F.3d 125, 132 (2d Cir. 2014); United States v. Southard, 700 F.2d 1, 23 (1st Cir. 1983)).
216. 895 F.3d 859 (6th Cir. 2018).
217. *Farrad*, 895 F.3d at 877.
218. *Id.* at 865.
219. *Id.*
220. *Id.* at 877.

The Circuit Court concluded the district court erred by finding the photographs self-authenticating business records under Fed. R. Evid. 902(11) and 803(6), but the error was harmless because the photographs were nonetheless properly authenticated by extrinsic evidence under Fed. R. Evid. 901(a).[221]

In *State v. Griffith*,[222] the Arizona Court of Appeals affirmed the Superior Court's holding a Facebook message the State offered to prove the truth about a user selling stolen property did not fall within Ariz. R. Evid. 803(6), the business record rule, and therefore, was not self-authenticating under Ariz. R. Evid. 902(11).[223] However, the Court determined the Facebook message was admissible under Rules 801(d) and 901(a).[224] The State offered a Facebook message that included a picture of an iPad to prove Griffith had the stolen iPad and was trying to sell it.[225] Griffith argued the trial court abused its discretion by admitting the Facebook records as business records because they were hearsay, not subject to the rule, and not properly authenticated.[226] The State had offered the evidence as a business record but did not present a certification from Facebook.[227] Regardless, the Court observed that "when the ultimate relevance of a document obtained from a social media platform turns on the fact of authorship, the foundation requirements of Rule 803(6)(D) are inadequate to authenticate it because, as is the case here, they simply do not show who authored the message."[228] The Court concluded that "social media communications, when offered to prove the truth of what a user said, fall outside the scope of Rule 803(6), and thus are not self-authenticating under Rule 902(11) when offered for that purpose."[229]

Likewise, in *People v. Glover*,[230] the Colorado Court of Appeals affirmed the district court, holding a Facebook webpage did not qualify as a self-authenticating business record under Colo. R. Evid. 902, but the printouts were properly authenticated under Colo. R. Evid. 901 using circumstantial evidence.[231] Circumstantial evidence established the account was registered in the defendant's name, the webpage contained his personal photographs, a witness identified the account belonged to him and was the account the witness used to communicate with him, the defendant's telephone

---

221. *Id.*

222. 449 P.3d 353 (Ariz. Ct. App. 2019).

223. *Griffith*, 449 P.3d at 356.

224. *Id.* at 357 (applying ARIZ. R. EVID. 803(6), 902(11) and 901, the State's equivalent to FED. R. EVID. 803(6), 902(11), and 901).

225. *Id.* at 356.

226. *Id.* at 355.

227. *Id.* at 355-56.

228. *Id.* at 357.

229. *Id.*

230. 2015 COA 16, 363 P.3d 736.

231. *Glover*, 2015 COA 16, ¶¶ 14-34 (applying COLO. R. EVID. 901 and 902, the State's equivalent to FED. R. EVID. 901 and 902).

number was used to verify the account, and another witness testified to using the webpage to communicate with the defendant about the murder.[232] The Court held that a proponent of social media content is required to show: (1) the record was from the social media platform, and (2) the defendant made the record.[233] The Court explained 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."[234] Therefore, "the Facebook printouts were neither authenticatable" under Rule 902 nor "admissible" under Rule 803.[235]

2. Cases Improperly Admitting Evidence Under Rules 902(11) and 803(6)

Standing in contrast to the correct application of Rule 902(11) and Rule 803(6) recited above, several courts have incorrectly applied the rules.[236] Those courts admitted social media content as self-authenticating under Rule 902(11) and Rule 803(6), after mistakenly treating user-provided computer-stored information as if it was the platform's computer-generated information.[237]

In *United States v. Hassan*,[238] the Fourth Circuit Court of Appeals held the government properly authenticated Facebook pages under Rule 902(11) and satisfied Rule 901 by using the IP address evidence to track a Facebook account to the defendant's email address.[239] In *Hassan*, the Court described the admissibility of evidence process taken in authenticating under Rule 902 as follows:

> [T]he 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

232. *Id.* at 743.

233. *Id.* at 741.

234. *Id.* at 740.

235. *Id.* at 741.

236. The cases listed in this section are not exhaustive, but rather they are samples of cases instructive for the proposition reviewed.

237. *See supra* Section II.C (explaining that social media platforms collect, use, store, mine, and share user-provided information but do not purport to verify the reliability or the genuineness of the content). Although various social media sites engage in some efforts to stop distribution of what they deem to be misinformation, I do not believe the scope of those efforts at this time approximate anything close to satisfying the Fed. R. Evid. 803(6)(C) requirement that verifying the accuracy of a user's post be "a regular practice of that activity" such that self-authentication as a business record would be permissible.

238. 742 F.3d 104 (4th Cir. 2014).

239. *Hassan*, 742 F.3d at 133.

> 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.[240]

The Court pointed out that it "required the government, pursuant to Rule 901, to prove that the Facebook pages were linked to Hassan and Yaghi,"[241] which was accomplished merely by "tracking the Facebook pages and Facebook accounts to Hassan's and Yaghi's mailing and email addresses via internet protocol addresses."[242] Essentially, the Court held that because Facebook stores user content in the regular course of its business, its records are self-authenticating under Rule 902(11) and Rule 803(6). However, in doing so, the Court provided no analysis of the requirements of those rules.[243]

In *United States v. Recio*,[244] the Fourth Circuit Court of Appeals held the district court correctly admitted Facebook messages as properly authenticated by a custodian's certificate indicating the record containing the message was made at or near the time it was transmitted by the Facebook user.[245] The Court held the government sufficiently linked the Facebook user to the defendant by showing the account's username was the defendant's name, the email address included the defendant's name, and the defendant was in over one hundred pictures posted to the account including one that wished him a happy birthday.[246] The defendant argued someone else may have accessed the account.[247] The Court held, "without any evidence of unauthorized access, the jury could find that [the defendant] was the true author of the post."[248] The Court observed that "what matters is not whether a jury could find that [the defendant] did not author the post in question, but rather whether the jury could reasonably find that he did."[249] Again, the Court provided no analysis explaining how the certification satisfied the admission requirements under Rule 803(6).

---

240. *Id.* at 133.

241. *Id.* at 132-33.

242. *Id.* at 133.

243. *See* United States v. Denton, 944 F.3d 170 (4th Cir. 2019). Where the Court again incorrectly dismissed an appellant's challenge to admission of social media content. There, the Court dismissively held "Denton nevertheless seeks to conjure error by stressing that the business record certification provided the foundation for improper testimony from Special Agent Babits regarding the contents of Denton's Facebook records." *Id.* at 184.

244. 884 F.3d 230 (4th Cir. 2018).

245. *Recio*, 884 F.3d at 237. The *Recio* court does not specifically reference Rule 902; however, it notes authentication was made by a custodian's certificate. *Id.* (citing United States v. Hassan, 742 F.3d 104, 133-34 (4th Cir. 2014). In *Hassan*, the Court applied Rule 902. *Hassan*, 742 F.3d at 121-33.

246. *Recio*, 884 F.3d at 236-37.

247. *Id.* at 237.

248. *Id.*

249. *Id.*

In *Murray v. State*,[250] a Texas Court of Appeals held the trial court properly authenticated a user's Facebook content under Tex. R. Evid. 902.[251] The Court described the authentication process taken:

> [T]he State proffered evidence of Murray's Facebook account by way of a "Certificate of Authenticity of Domestic Records of Regularly Conducted Activity" executed by Facebook's Records Custodian. This Certificate of Authenticity sufficiently complied with the requirements of self-authentication outlined in Rule 902(10)(B), obviating the State's need to produce extrinsic evidence to authenticate the properly admitted Facebook evidence. Because the State satisfied the requirements of Rule 902(10), it presented sufficient facts to support a reasonable jury determination that the Facebook evidence proffered was authentic.[252]

The evidence proffered in *Murray* consisted of photographs, comments, and private messages.[253] The Court noted the State was "not required to conclusively establish that the defendant authored the messages; rather, the State must present prima facie evidence such that a reasonable jury could find the defendant created the content of the Facebook pages."[254] According to the Court, the State satisfied that requirement:

> [T]he State introduced sufficient circumstantial evidence of photographs, comments, and private messages from the Facebook account to establish a prima facie case such that a reasonable jury could find Murray created and maintained the contents of the Facebook account. Consistent with [the victim's] testimony that Murray took photos of her and posted them on Facebook, photos of [the victim] were posted on the Facebook account bearing the name "Allen Murray". [The victim] identified Murray as the other person in one picture with her. The post relating to that photograph of [the victim] reads "For sale hmu" and shows "August 24" as the date of the post.[255]

The Court further noted the private messages between the account user and another person, "appeared on Murray's Facebook account in the late hours of August 24, 2013, and the early hours of August 25, 2013."[256] Unfortu-

250. 534 S.W.3d 540 (Tex. App. San Antonio 2017).
251. *Murray*, 534 S.W.3d at 545 (applying the State's equivalent to the FED. R. EVID. 902(11)).
252. *Id.*
253. *Id.* at 543.
254. *Id.* at 546.
255. *Id.* at 545.
256. *Id.*

nately, the Court failed to provide any analysis addressing whether the Facebook records custodian's certificate of authenticity established how the user-provided content, *i.e.*, the photographs, comments, and private messages, were Facebook's business records, used for Facebook's business purposes, rather than simply a subscriber's computer-stored information.

In *Ryder v. State*,[257] the Texas Court of Appeals affirmed the trial court, holding numerous sexually explicit Facebook pictures and messages, offered as State's exhibits 1-30, were properly authenticated through witness testimony and circumstantial evidence under Tex. R. Evid. 901, and State's exhibits 37, 37-A, and 37-B were properly authenticated under Tex. R. Evid. 902.[258] The Court held the Rule 902 exhibits were properly authenticated because they "contained (1) Facebook's business records pertaining to the messages in exhibits 1-30, and (2) a 'Certificate of Authenticity of Domestic Records of Regularly Conducted Activity' that complied with the requirements of self-authentication under Tex. R. Evid. Rule 902."[259] The Court made no effort to explain how the user-supplied content complied with the requirements of Rule 803(6) as Facebook's business records.

In *People v. Curry*,[260] the Illinois Court of Appeals affirmed the trial court holding the user's account information including name, address, telephone number, and email address was a properly authenticated business record under Ill. R. Evid. 803(6) and Ill. R. Evid. 902(11).[261] The State submitted a certification from Facebook and a four-page document containing the account information, content, and transmission log of messages from an account with the defendant's name.[262] The certification provided "the records were made and kept by Facebook in the course of its regularly conducted activity and as part of its regular business practice."[263] The Court held that information was sufficient to authenticate the account information under the business records rule, but the content required additional foundation to authenticate.[264] As to the account information, the Court did not explain how the certification satisfied the elements under the business records rule, or how it provided sufficient information from which a jury could find the account belonged to the defendant. As to the content, circumstantial evidence established the defendant was the author, he personally knew the victim and her

257. 581 S.W.3d 439 (Tex. Ct. App. 2019).

258. *Ryder*, 581 S.W.3d at 454 (applying TEX. R. EVID. 901 and 902, the State's equivalent to FED. R. EVID. 901 and 902).

259. *Id.* at 455.

260. 2020 IL App. (2d) 180148.

261. *Curry*, 2020 IL App. (2d) 180148, ¶ 61 (applying ILL. R. EVID. 803(6) and 902(11), the State's equivalent to FED. R. EVID. 803(6) and 902(11)).

262. *Id.* ¶ 23.

263. *Id.* ¶ 52.

264. *Id.* ¶¶ 51-57.

family, he had personal knowledge of the incident, and he knew the victim had reported the incident to the police.[265]

In *Commonwealth v. Manivannan*,[266] the Superior Court of Pennsylvania vacated the district court's order excluding evidence as not properly authenticated under Pa. R. Evid. 902 and Pa. R. Evid. 803, the self-authenticating business records rule.[267] That portion of the ruling was consistent with the correct application of law. What makes this case unusual is that the appellant argued the certification letter, rather than the underlying evidence sought to be admitted, was inadequately supported. With the issue so framed, the Court held that an unsigned letter from Comcast, an Internet service provider, which identified the IP address, was not properly authenticated under Rule 902.[268] The IP address allegedly belonged to the defendant who had unlawfully accessed the victim's email account on five occasions. The Court reasoned that the certification letter (rather than information about the IP address or the screenshot contents sought to be admitted) was not shown to be a record of regularly conducted business activity and only evidenced the defendant's connection to the IP address. The Court explained that the letter was not self-authenticating because "there is no discernable correlation between this document and the evidence it purports to authenticate."[269] The government did not present testimony but rather sought to authenticate the letter by certification.[270]

In sum, courts admitting social media content as self-authenticating under Rule 902(11) and Rule 803(6) sometimes mistakenly treated user-provided computer-stored information as if it were the platform's computer-generated information. Even if the platform uses customer-supplied content to attach relevant advertising, that business purpose makes no effort to verify the reliability or the genuineness of the information.[271] In those circumstances, the courts usually accept the erroneous argument that the authentication requirement is satisfied by attestation from a custodian of the platform.

---

265. *Id.* ¶ 57.

266. 186 A.3d 472 (Pa. 2018).

267. *See Manivannan*, 186 A.3d at 481 (applying PA. R. EVID. 902(11) and 803(6), the State's equivalent to FED. R. EVID. 902(11) and 803(6)).

268. *Id.*

269. *Id.* at 481.

270. *Id.* Also confounding in this case, the Court ultimately held the screenshot printouts displaying the contents of the officer's search were admissible. *Id.* at 483. The Court explained the printouts were not offered to prove the defendant unlawfully accessed the email, but rather they were offered to describe the progression of the officer's investigation. *Id.* No explanation was provided indicating how the progression of the officer's investigation was relevant to the case, or whether that is what the proponent purported the screenshots to be.

271. *See supra* Section II.C (explaining that social media platforms collect, use, store, mine, and share user-provided information but do not purport to verify the reliability or the genuineness of the content).

However, a mere recitation of the statutory elements under the business records rule is not enough. When relevancy of the content hinges on authorship, a record custodian's certification alone cannot speak to the truth of the user-provided content.[272] For that information, sufficient foundational evidence must be introduced for a jury to reasonably find authorship.

D. RELATIONSHIP OF RELEVANCY, AUTHENTICATION, AND THE BUSINESS RECORDS RULE

Admitting user-supplied social media content based only on a certificate from the social media platform overlooks the relationship of relevance and authentication, and the requirement that evidence must be relevant to be admitted.[273] Evidence is relevant only when it has "any tendency to make" a fact of consequence "more or less probable than it would be without the evidence."[274] "[E]vidence can have this tendency only if it is what the proponent claims it is, i.e., if it is authentic."[275]

Rule 902(11) provides that "records of a regularly conducted activity" that fall under the business record rule may be authenticated with a certificate from the records custodian *only* if that certificate provides enough evidence to satisfy that the requirements under (A)–(C) are met.[276] Those foundational requirements are designed to ensure the trustworthiness of content received into evidence. As one commentator explains: "[t]he theory underlying the business records rule is similar to the theory underlying other rules—unusual reliability, which is inferred from the belief that regularly kept records have a high degree of accuracy. Their very regularity and continuity are presumed to train the recordkeeper in habits of precision."[277]

When computer-stored social media content is offered by certification to prove the factual assertions in it, a proponent cannot establish that the record "was made at or near the time by—or from information transmitted by—someone with knowledge;" "was kept in the course of a regularly conducted activity of a business, organization, occupation, or calling, whether or not for profit;" and "making the record was a regular practice of that activity."[278] For example, if the proponent offers social media content claiming it to be a statement someone made, proper authentication requires evidence the webpage

---

272. *See supra* Section II.B (general discussion of the interrelationship between relevancy and authentication).

273. *See, e.g.*, United States v. Browne, 834 F.3d 403, 410 (3d Cir. 2016) (describing authentication as an "aspect[] of relevancy that [is] a condition precedent to admissibility").

274. FED. R. EVID. 401.

275. *Browne*, 834 F.3d at 409.

276. *See* FED. R. EVID. 902(11).

277. *See* PAUL, *supra* note 28, at 121-22 (quoting Peritz, *supra* note 192, at 963).

278. *See* FED. R. EVID. 803(6)(A)-(C).

existed and the content was tied to the alleged author.[279] As noted, courts recognize that "[a]uthorship presents an unusual challenge for authenticating social media communications due to the 'ease with which someone can assume the identity of another on Facebook.'"[280] Therefore, to determine authorship in the context of social media, "*additional corroborating evidence of authorship is required beyond confirmation that the social networking account is registered to the party purporting to create those messages*."[281] Because determining authorship is key, and linking the content to the author is central to determining relevancy and authentication, the content from social media postings are not of the kind of evidence that satisfy the elements of Rule 803(6).[282]

When social media information is offered to prove the truth of its contents (truth of a statement made by a person), it does not qualify as a business record and falls outside the scope of Rule 803(6); therefore, it cannot be self-authenticating under Rule 902(11).[283] Rather, when offered for that purpose, foundation establishing the author and linking the author to the content must be made through direct or extrinsic evidence under Rule 901.[284]

Even when a business relationship exists between a social media platform and its users, evidence must be presented establishing the platform substantially relies on the offered evidence for a business purpose and that business purpose relies on the accuracy of the information.[285] In rejecting authentication of Facebook content under Rule 902 as a business record, the *Browne* court explained:

> Here, 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

---

279. People v. Glover, 2015 COA 16, ¶ 23, 363 P.3d 736.

280. People v. Dominguez-Castor, 2020 COA 1, ¶ 56, 469 P.3d 514 (quoting People In Interest of A.C.E-D., 2018 COA 157, ¶ 46, 433 P.3d 153 Colo. App. 2018).

281. *Glover*, 2015 COA 16, ¶ 30 (emphasis added).

282. *See generally* United States v. Farrad, 895 F.3d 859, 879-80 (6th Cir. 2018) (holding "it is not at all clear . . . why our rules of evidence would treat electronic photos that police stumble across on Facebook one way and physical photos that police stumble across lying on a sidewalk a different way").

283. State v. Griffith, 449 P.3d 353, 357 (Ariz. Ct. App. 2019).

284. *See, e.g.*, *id.* (relying on United States v. Browne, 834 F.3d 403, 409 (3d Cir. 2016)) (explaining that "[b]ecause the State claimed the message was sent by Griffith himself, the State was required to provide 'some indicia of authorship' to satisfy its authentication obligation before the message could be admitted into evidence").

285. For example, social media platforms scan user content to display pertinent and relaxed advertising. *See*, *e.g.*, *Data Policy*, *supra* note 14 (describing information Facebook collects from users including "information about [user's] interests, actions and connections—to select and personalize ads, offers and other sponsored content that [Facebook] shows you."). To that extent, the platform is using user content for a business purpose. However, the platform's business purpose does not include verifying or relying on accuracy of the information.

> 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.[286]

Under Rule 902(11), the business record certification may be sufficient to authenticate computer-generated information like to show a webpage existed at a particular time, a communication occurred between certain accounts, or a communication occurred at a certain time and date.[287] However, the certification cannot be used for an attempted admission of computer-stored, user-created information if relevancy depends on authenticity of the content.

IV. PREDICTING THE FUTURE AND URGING PROPER APPLICATION OF NEW RULES 902(13) AND (14)

In 2014, the Judicial Conference Advisory Committee on Evidence Rules addressed concerns relating to the cost and efficiency in admitting certain types of ESI. The Committee recommended adding subsections (13) and (14) under Rule 902 to allow the use of business record type certifications for authenticating system-generated data and data copied from an electronic device.[288] The proponents claimed subsections (13) and (14) would make authentication easier and less costly for system-generated and data copied electronic evidence that are, "under current law, likely to be authenticated under Rule 901 but only by calling a witness to testify to authenticity."[289] The proposed subsections became effective December 1, 2017,[290] and provide:

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

---

286. United States v. Browne, 834 F.3d 403, 410 (3d Cir. 2016) (citing United States v. Jackson, 208 F.3d 633, 637-38 (7th Cir. 2000) (holding that Internet Service Providers' ability to retrieve information that their customers posted online did not turn the posts that appeared on the website of a white supremacist group into the ISP's business records under Rule 803(6))); *cf. In re* Application of U.S. for Historical Cell Site Data, 724 F.3d 600, 611 (5th Cir. 2013) (defining business records for Fourth Amendment purposes as "records of transactions to which the record-keeper is a party," is in contradistinction to "[c]ommunications content, such as the contents of letters, phone calls, and emails, which are not directed to a business, but simply sent via that business").

287. *Browne*, 834 F.3d at 411.

288. *See* ADVISORY COMM. ON EVIDENCE RULES, MINUTES OF THE MEETING OF OCTOBER 24, 2014, at 9.

289. *See id.* at 9-12.

290. *See* FED. R. EVID. 902(11) advisory committee note to 2017 amendment.

> (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).[291]

The deliberate mention of self-authentication under Rule 902(11) raises a question whether it also triggers compliance with Rule 803(6)(A)-(C), the business records rule. If so, lawyers and judges might believe the cross-reference suggests a connection between the business records rule and subdivisions (13) and (14) other than utilizing the same certification compliance structure and notice requirements for the differing self-authenticating circumstances. While some temptation might exist to draw a connection between 902(13) and (14) and 803(6)(A)-(C) for purposes of shortcutting the authenticity and relevancy analyses, the amendment's history shows no such connection was intended. Rather, the Committee's intent in referencing Rule 902(11) in subdivisions (13) and (14) merely was to utilize the methodology established under subdivision (11). The Committee explained:

> The self-authentication proposals, by following Rule 902(11)'s provision covering business records, essentially leave the burden of going forward on authenticity questions to the opponent of the evidence. Under Rule 902(11), 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.[292]

The Committee intended Rule 902(13) and (14) to have "the same effect of shifting to the opponent the burden of going forward (not the burden of proof) on authenticity disputes."[293] In response to a concern that a certification does not speak to the accuracy of the underlying information in the proffered item, a Committee member explained:

---

291. FED. R. EVID. 902(13)-(14).

292. *See* ADVISORY COMM. ON EVIDENCE RULES, MINUTES OF THE MEETING OF OCTOBER 24, 2014, at 10-11.

293. *See id.*

> The certificates that would be prepared under proposed Rules 902(13) and (14) would not be *certifying the accuracy of any contents or any factual assertions*. They would only be certifying that the evidence to be introduced was generated by the machine (Rule 902(13)) or is a copy of the original (Rule 902(14)).[294]

The Committee noted "a certificate offered as proof of authenticity of a webpage *does not dispose of a hearsay exception with respect to the content of the webpage*."[295] Additionally, the Committee made clear that the intent of the amendments was to allow for self-authentication of certain electronic evidence without reducing challenges on content of that evidence on other grounds such as hearsay, relevance, or the right to confrontation:

> The reference to the "certificate requirements of Rule 902(11) and (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 certificate under this Rule can establish only that the proffered item has satisfied the admissibility requirements for authenticity. The opponent remains free to object to the admissibility of the proffered item on other grounds – including hearsay, relevance, or in criminal cases the right to confrontation.... 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.[296]

The Advisory Committee Reporter also explained that the proposed amendments were not intended to create a "backdoor hearsay exception[:]"[297]

> Rules 902(11) and (12) end up doing more than authenticating a document. They also work together with Rule 803(6) to establish the foundation requirements for the business records exception to the hearsay rule. One possible concern is that the proposed additions to Rule 902, because they are modeled after the existing Rules, might be read to operate as a hearsay exception—but without tying into any of the exceptions established under the Federal Rules.

---

294. *See id*. (emphasis added).

295. *See id*. at 11-12 (emphasis added).

296. FED. R. EVID. 902 advisory committee's note to 2017 amendment.

297. ADVISORY COMMITTEE ON EVIDENCE RULES, AGENDA FOR COMMITTEE MEETING OF OCTOBER 24, 2014, at 217 (addressing the memorandum to the Advisory Committee on Evidence Rules from Daniel J. Capra about possible amendments to Rule 902 for authenticating machine-generated data and electronic information through hash value) (emphasis added).

> Thus, the relationship between authentication and hearsay—as applied to machine-generated data and digital data authenticated by hash value—needs to be investigated.
>
> That investigation indicates that a rule of authentication for machine-generated data does not end up creating a backdoor hearsay exception—because machine-generated data is not hearsay in the first place. *See, e.g.*, *United States v. Moon*, 512 F.3d 359 (7th Cir. 2008) (readings taken from an infrared spectrometer and a gas chromatograph was not hearsay because "data is not 'statements' in any useful sense.").
>
> On the other hand, proposed Rule 902(14) could cover items that are hearsay—for example, a computer file, or digital information on a storage device. It will be important, then, to emphasize that the Rule deals with authentication only and does not purport to answer any questions about the hearsay content of the information authenticated. That is, the Rule is unlike Rule 902(11) and (12), which work together with a hearsay exception to handle both hearsay and authentication issues. The disclaimer to Rule 902(14) is probably best added to the note rather than the text—it is not customary in the evidence rules to state in the text what a rule does not do, nor would that appear necessary in this instance as the proposed rule does not on its face attempt to tie into a hearsay exception of any kind.[298]

Analogous to Rules 902(11) and (12) allowing certification of business records, Rules 902(13) and (14) merely permit a person with knowledge to certify the foundation necessary to establish the authenticity of computer-generated information and information in the form of a copy of original data taken from an electronic device. As noted, the Committee viewed those circumstances as rarely subject to authentication dispute.[299]

The amendments under subsections (13) and (14) allowing for self-authentication under certain limited circumstances were not intended to lower the foundational requirements necessary for proper authentication or to shortcut a proper analysis of authenticity or relevancy. Judges and lawyers therefore should not read Rules 902(13) and (14) as a means of admitting third party, computer-stored social media content. Rather, the Rules should be applied narrowly to only permit limited use of these certifications.

---

298. *Id.*

299. *See* ADVISORY COMM. ON EVIDENCE RULES, MINUTES OF THE MEETING OF OCTOBER 24, 2014, at 9-12.

V. CONCLUSION

Self-authentication under Rules 902(11) and 803(6) does not change or reduce the requirement for authentication that must be met under Rule 901(a). Rather, it merely changes the manner a proponent may utilize to meet the requirement. When appropriate, self-authentication allows for an easier, less expensive method of achieving admissibility, but it does not reduce the admissibility requirement. In the end, a "proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is."[300] Evidence is properly authenticated only if the proponent provides foundation sufficient to support a reasonable determination the evidence offered is authentic.[301]

As this article illustrates, computer-stored social media content offered to prove the truth of the matter asserted nearly never qualifies as a business record when a person outside the business provides the content in question. This proposition is true because the social media user (or an imposter) has no duty to report or record accurately, and in the conduct of its regular business activity the social media platform does not rely on accuracy of the information. Therefore, using the business record rule to admit user-generated social media content ignores the essential relationship of relevancy and authentication, and abandons the mission of ensuring evidence is reliable and genuine.

300. FED. R. EVID. 901(a); *see also* United States v. Jones, 107 F.3d 1147, 1150 n.1 (6th Cir. 1997).

301. Tienda v. State, 358 S.W.3d 633, 638 (Tex. Crim. App. 2012).