COMMENT

WHEN IS A TWEET NOT AN *ADMISSIBLE* TWEET? CLOSING THE AUTHENTICATION GAP IN THE FEDERAL RULES OF EVIDENCE

SIRI CARLSON†

INTRODUCTION

Whether referred to as the Information Age or the Digital Age, today's world is awash in just that: digital information. The creation, communication, and storage of digital information have transformed over the past three

† Research Editor & Philanthropy Editor, Volume 164, *University of Pennsylvania Law Review*. J.D. Candidate, 2016, University of Pennsylvania Law School; B.A., 2009, Luther College. I extend my deepest gratitude to Professor David Rudovsky for his guidance and advice in writing this Comment, to my colleagues on the *Law Review*, especially Do Hee Jeong, Andrew Schlossberg, and the associate editors who assisted with the editing process, and to my family.

decades. Today, people use computers, tablets, and smartphones to share public and private messages, photographs, and videos with each other. In particular, communication through social media platforms has increased dramatically over the past fifteen years. While it is challenging to predict what communication advances will be made in the coming years, increasing use of digital communications such as social media suggests that global reliance on these methods of connecting will only continue to grow.[1]

The proliferation of social media has naturally led to the increased use of information found on social media to resolve legal disputes. In criminal and civil cases, evidence obtained from social media helps the parties tell their stories and provides proof of disputed facts.[2] As with all evidence, concerns over relevance,[3] authenticity,[4] prejudice,[5] and reliability[6] arise.[7] However, evidence from social media and other digital communications create distinct admissibility concerns. Debates over authenticity of digital evidence fall into two distinct yet overlapping categories of inquiry: normative and procedural.

On a normative level, the debate centers on whether the threshold inquiry for authentication should be more than the minimal showing currently required under the Federal Rules of Evidence (Rules) 901 and 104.[8] Even if one accepts the current, minimal threshold for authentication, a procedural question still exists under the current Rules: Can the suggested modes of authentication provided in Rule 901 adequately guide courts in admitting these new forms of evidence, or do concerns over digital evidence authenticity require specific guidance?

While the Rules provide multiple, nonexhaustive illustrations for authenticating evidence,[9] application of these examples has divided both state and federal courts over the appropriate authentication method and the sufficient threshold authenticity requirement for social media and other

1 *See* RICHARD WIKE & RUSS OATES, PEW RESEARCH CTR., EMERGING NATIONS EMBRACE INTERNET, MOBILE TECHNOLOGY 2, 9 (2014) (stating that "[t]he internet has also made tremendous inroads" in the emerging and developing world, and "[o]nce people have access to the internet, they tend to engage in social networking").

2 *See infra* Section I.B.

3 *See* FED. R. EVID. 402 (prohibiting the admission of irrelevant evidence).

4 *See* FED. R. EVID. 901, 902 (providing standards for authenticating and self-authenticating evidence).

5 *See* FED. R. EVID. 403 (granting the court authority to exclude relevant evidence when the risks of its prejudicial effect substantially outweighs its probative value).

6 *See* FED. R. EVID. 803 (stating the exceptions to the rule against hearsay).

7 For an overview of legal issues beyond evidentiary concerns raised by social media content, including both procedural and substantive issues, see generally John G. Browning, Keynote Address, *Social Media and the Law*, 68 U. MIAMI L. REV. 353 (2014).

8 *See infra* subsection II.B.1.

9 *See, e.g.,* FED. R. EVID. 901(b) (offering ten examples, such as the testimony of a witness with knowledge, nonexpert opinion about handwriting and distinctive characteristics of an item).

digital communications.[10] The inconsistencies in application and outcome suggest that modifications specifically addressing these new forms of communication would better promote uniform and consistent admissibility rulings to a greater degree than continued, albeit creative, application of the current authentication examples under Rule 901.[11]

Social media communication is only part of the larger field of digital communications, including email and text messaging, and the even broader field of electronically stored information such as computer files. However, the growing use of social media—combined with courts' differing approaches to authentication—provides a good lens for viewing the shortcomings of applying the current Rules to newer communication formats.[12] The Rules' authentication requirements have not changed since the inception of now-widely utilized advances in communication technology.[13] Yet many scholars and even courts do not advocate for revising authentication requirements.[14] They point to the current Rules' nonexhaustive nature, the ability to combine examples to authenticate digital evidence,[15] the challenge of creating an effective Rule,[16] and the inevitability of a cohesive approach once courts apply the current Rules in a similar fashion.[17] However, the increasing need for and the continued inconsistencies in admitting social media and other digital communications support modifying the Rules to contain explicit procedures for authenticating these types of evidence.[18]

By providing clear guidance on how to sufficiently authenticate digital communications for admissibility purposes, the Rules can address some of the

---

10 *See infra* Section II.A.

11 *See infra* subsection II.B.2.

12 These considerations apply to other forms of digital or electronically stored evidence that pose similar authentication concerns. *See infra* Part III.

13 *See* Jonathon L. Moore, *Time for An Upgrade: Amending the Federal Rules of Evidence to Address the Challenges of Electronically Stored Information in Civil Litigation*, 50 JURIMETRICS 147, 148 (2010) ("[T]hroughout these vast technological and societal changes, the Federal Rules of Evidence have essentially remained static.").

14 *See* Aviva Orenstein, *Friends, Gangbangers, Custody Disputants, Lend Me Your Passwords*, 31 MISS. C. L. REV. 185, 202 n.107 (2012) (listing courts and commentators who argue that the current Rules are sufficient to authenticate social media evidence).

15 *See, e.g.*, Andrew B. Delaney & Darren A. Heitner, *Made for Each Other: Social Media and Litigation*, 85 N.Y. ST. B.A. J., Feb. 2013, at 10, 14 (noting that Rule 901(a) allows circumstantial evidence reflecting the "contents, substance, internal pattern, or other distinctive characteristics" of the electronically stored information for authentication).

16 *See* ADVISORY COMM. ON EVIDENCE RULES, MINUTES OF THE MEETING ON OCTOBER 24, 2014, at 27 (Apr. 17, 2015), http://www.uscourts.gov/rules-policies/archives/agenda-books/advisory-committee-rules-evidence-april-2015 [https://perma.cc/T2PN-ZUFG] (discussing the complicated nature of a proposed amendment to Rule 901 and the likelihood of obsolescence).

17 *See infra* subsection II.B.1.

18 *See, e.g.*, Moore, *supra* note 13, at 193 (arguing that approaching evidentiary issues, including authentication, for electronically stored information on a case-by-case basis will lead to "uncertainty, inefficiencies, and varying standards . . . .").

mistrust of newer communication formats and appropriately cabin this consideration from the threshold determination.[19] This approach is preferable to one in which courts establish guidance over time.[20] After nearly two decades of exposure to the new communication technologies and their widespread and growing use, alterations to the Rules for authentication are appropriate.[21] Social media's widespread popularity provides a wealth of digital evidence available for litigation. This evidence will only increase in amount and salience in both civil and criminal litigation. Authenticity of this type of evidence is a threshold consideration directly affecting its relevancy and ultimate admissibility.[22] As such, creating uniform authentication procedures for social media content and other digital communications grows in urgency as access to, use of, and the variety of this information continues to expand.[23]

Part I of this Comment provides a brief overview of social media and its increasing prevalence as a communication tool and as evidence. Part II examines the current approach to authentication under Rule 901, including its application in federal court decisions, and the need to address the gap[24] in authentication for digital communications. Finally, Part III discusses possible updates for the Rules by synthesizing multiple commentators' approaches and proposing changes to the Rules that would improve consistency to rulings on admissibility.

I. THE LENS OF SOCIAL MEDIA

Most readers will have at least a passing familiarity with various forms of social media. Due to widespread use, the functions associated with websites such as Facebook, Twitter, and MySpace are part of general cultural and

19 As argued by Judge Grimm and others, most concerns over the possibility of manipulation under the current bar for threshold authenticity should actually be determinations for the factfinder. Paul W. Grimm et al., Keynote Address, *Authentication of Social Media Evidence*, 36 AM. J. TRIAL ADVOC. 433, 469 (2013) ("Rule 901(b)(3) . . . allows the fact finder (usually the jury) to authenticate social media evidence . . . .").

20 *See infra* subsection II.B.1.

21 The need to adjust to new types of technology is not a new problem for the law. *See* Orenstein, *supra* note 14, at 203 (stating that "[e]vidence law is conservative by nature and slow to adapt to new forms of technology").

22 *See infra* notes 64–68 and accompanying text.

23 The various types of content on social media include written text, audio recordings, photographs, and video.

24 In asking symposium attendees whether the Rules of Evidence should "begin to reflect differences in technology, underlying different types of exhibits," Judge John Woodcock, Jr. also queried as to whether there is "a gap between what jurors assume they are seeing . . . and what they are actually seeing" when they are confronted with digital evidence. Panel Discussion, *Symposium on the Challenges of Electronic Evidence* (December 2014), *in* 83 FORDHAM L. REV. 1163, 1179 (2014) [hereinafter *Electronic Evidence Symposium*]. This gap arguably also exists between what the Rules currently authenticate and what modern communication technologies need them to authenticate.

societal understanding, both in the United States and abroad.[25] Websites such as LinkedIn, YouTube, and Instagram,[26] and platforms in other countries such as VK.com (formerly Vkontakte.ru),[27] continue to grow in popularity.[28] Due to both the general knowledge of and the wide variance in the details and features of the various platforms, this Section seeks only to highlight the salient, general qualities of social media platforms needed for the remaining discussion. It also briefly addresses the growing use of social media platforms both socially and as evidence in legal proceedings.

A. *General Features of Social Media*

Social media is defined as "forms of electronic communication (such as Web sites for social networking or microblogging) through which users create online communities to share information, ideas, personal messages, and other content . . . ."[29] While the term "social media" at one point[30] encompassed media such as blogs, social network sites, collaborative sites (including Wikipedia, a collaborative online encyclopedia), and "content communities,"

25 *See Pressroom*, MYSPACE, https://myspace.com/pressroom [https://perma.cc/V76D-QGCG] (last visited Jan. 23, 2016) (describing MySpace as "a place where people come to connect, discover, and share," and highlighting MySpace's use by the music community); *Statement of Rights and Responsibilities*, FACEBOOK, https://www.facebook.com/legal/terms/update [https://perma.cc/H7GC-76Q6] (last visited Jan. 23, 2016) (granting Facebook membership to virtually anyone over the age of thirteen with a valid email address or mobile number); *Twitter Usage/Company Facts*, TWITTER, http://about.twitter.com/company [https://perma.cc/66CV-BFSH] (last visited Jan. 23, 2016) (describing Twitter usage, including the high percentage of accesses through the mobile platform and non-U.S. accounts).

26 *See About YouTube*, YOUTUBE, https://www.youtube.com/yt/about [https://perma.cc/ UWM7-GGLL] (last visited Jan. 23, 2016) ("YouTube allows billions of people to discover, watch and share originally-created videos . . . [and] provides a forum for people to connect . . . across the globe . . . ."); *FAQ*, INSTAGRAM, https://instagram.com/about/faq [https://perma.cc/52ZL-PYW6] (last visited Jan. 23, 2016) ("Instagram is a fun and quirky way to share your life with friends through a series of pictures."); LINKEDIN, https://www.linkedin.com/company/linkedin [https://perma.cc/6MWT-CFPB] (last visited Jan. 23, 2016) (stating that LinkedIn was founded in 2003 and "[w]ith more than 380 million members worldwide . . . [it] is the world's largest professional network on the Internet").

27 *See About VK*, VK, vk.com/about [https://perma.cc/KQU8-ZCLU] (last visited Jan. 23, 2016) (stating that the platform is "the most visited site in Eastern Europe" and is headquartered in St. Petersburg, Russia).

28 *See* ANDREW PERRIN, PEW RESEARCH CTR., SOCIAL MEDIA USAGE: 2005–2015, at 2 (Oct. 8, 2015), http://www.pewinternet.org/2015/10/08/social-networking-usage-2005-2015/ [https://perma.cc/CNF9-K5NX] (reporting that sixty-five percent of American adults use social media in 2015, as compared with seven percent in 2005).

29 *Social Media*, MERRIAM-WEBSTER, http://www.merriam-webster.com/dictionary/ocial%2omedia [https://perma.cc/4MRH-P7AA] (last visited Jan. 23, 2016).

30 *See* U.S. JUDICIAL CONFERENCE COMM. ON CODES OF CONDUCT, RESOURCE PACKET FOR DEVELOPING GUIDELINES ON USE OF SOCIAL MEDIA BY JUDICIAL EMPLOYEES 9-12 (2010), http://www.uscourts.gov/uscourts/RulesAndPolicies/conduct/SocialMediaLayout.pdf [https://perma.cc/7V9L-YGV5] ("Social media and social computing refer to the wide array of Internet-based tools and platforms that increase and enhance the sharing of information.").

such as YouTube,[31] many types of earlier social media, including those focused on sharing specific types of content, have now incorporated what would have earlier been defined as purely social networking site (SNS) features into their structures.[32] Because of this overlap in use, this Comment refers to social media and SNS interchangeablely.

Social media and other digital communication formats are part of a broader category of electronically stored information and share some characteristics with other types of electronically stored information.[33] For example, the private messaging feature of social media sites is similar to both email and text messaging.[34] However, much of social media content is accessible publicly, including the ability to leave public written messages to other users.[35] The "profile" of an individual user is a "unique page" usually containing descriptions of the individual including current and historical demographic, geographic, and personal information such as an individual's interests.[36] These profiles may be completely public or accessible only to those permitted access.[37] Beyond these standard features, social media platforms vary greatly in their features, target content, and users.

Since its relatively recent inception, social media has grown in its accessibility and in global use.[38] Some brief statistics highlight this trajectory. From an initial site with limited use in 1997, there were hundreds of social

---

31 For Judge Grimm's description of "content communities" as social media sites used to share specific types of content, such as YouTube's primary focus on video sharing, see Grimm et al., *supra* note 19, at 435.

32 *See* Danah M. Boyd & Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship*, 13 J. COMPUTER-MEDIATED COMM. 210, 212 fig.1 (2008) (including the relaunching of "community sites" with SNS features and YouTube as SNSs).

33 *See* Moore, *supra* note 13, at 149-50 (describing electronically stored information as including "e-mail, Web sites and Internet postings, and computer-generated documents and data files" (internal citations omitted)).

34 Private messages are clear examples of this similarity. *See* Heather L. Griffith, Comment, *Understanding and Authenticating Evidence from Social Networking Sites*, 7 WASH. J.L. TECH. & ARTS 209, 221 (2012) (stating that some evidence from SNSs "are analogous to more familiar forms of electronic evidence," such as email and internet chat).

35 *See* Boyd & Ellison, *supra* note 32, at 211 ("What makes social network sites unique [from other computer-mediated communication] is not that they allow individuals to meet strangers, but rather that they enable users to articulate and make visible their social networks."). One general definition describes certain "key technological features" of SNSs: they (1) allow a user to create a semi-public, if not completely public, "profile" within the platform's system, (2) publicly list the individual's connections to other users, and (3) allow the user to navigate the profiles of their connections and their connections' connections. *Id.* at 210-11.

36 *Id.* at 211-13.

37 *See, e.g.*, *id.* at 213 (describing access to LinkedIn's member profiles as determined by whether the viewer is a paying member and Facebook and MySpace as allowing users to choose, to an extent, the public visibility of their profiles).

38 *See id.* at 214 (stating that the first social network site, SixDegrees.com, started in 1997).

media platforms by 2008.[39] By 2014, seventy-one percent of all American adult internet users utilized Facebook and fifty-two percent used two or more social media sites.[40] Currently, two popular sites, Facebook and Twitter, claim over one billion active users[41] and 316 million monthly active users,[42] respectively. Other sites continue to increase in membership and use.[43] Accessibility is also increasing, as users can access social media through their computers, smartphones, and tablets, with companies creating mobile platforms specifically for noncomputer use.[44]

The use of social media in current political and social movements, both nationally[45] and internationally,[46] demonstrates the widespread prevalence of this digital communication format. One widely discussed and well-known domestic example of social media's value in connecting people over wide distances began in August 2014 when protesters used social media, particularly Twitter, to organize and document activist and police interactions surrounding the fatal shooting of teenager Michael Brown by a police officer in Ferguson, Missouri.[47] This distinct form of on-the-ground documentation of events may be implicated in legal ramifications stemming from these

---

39 *Id.* at 210.

40 PERRIN, *supra* note 28, at 3.

41 *Milestones*, FACEBOOK, https://www.facebook.com/facebook/info?tab=milestone [https://perma.cc/BK2C-2CWA] (last visited Jan. 23, 2016).

42 *Twitter Usage/Company Facts*, TWITTER, https://about.twitter.com/company [https://perma.cc/68C8-36DV] (last visited Jan. 23, 2016).

43 *See* PERRIN, *supra* note 28, at 2 tbl.1 (showing at least an eight-percent growth in the number of adult users of LinkedIn, Pinterest, and Instagram from 2012 to 2014).

44 *See* PAUL D. MCGRADY, JR., MCGRADY ON SOCIAL MEDIA § 1.01 (2012) (explaining that the "defining characteristic of social media is the ability for the end user to generate at least part of the content[,]" namely through personal computers, smart phones or tablets, or text-based platforms designed purely for mobile phones with texting capability).

45 *See, e.g.*, Katie Rogers, *How #BlackonCampus Convened a Twitter Debate on Race*, N.Y. TIMES (Nov. 12, 2015), http://www.nytimes.com/2015/11/12/us/blackoncampus-hashtag-hosts-discussion-amid-college-protests.html [https://perma.cc/WH55-YBJP] (reporting on the use of the Twitter hashtag to facilitate discussion on race relations on United States college and university campuses in the fall of 2015).

46 *See, e.g.*, TOM ROSENSTIEL & AMY MITCHELL, PEW RESEARCH CTR., ARAB-AMERICAN MEDIA: BRINGING NEWS TO A DIVERSE COMMUNITY 15 (2012) (describing a study by the United States Institute of Peace that "suggests that the importance of social media was in communicating to the rest of the world what was happening on the ground" during the Arab Spring).

47 Lindsay Deutsch & Jolie Lee, *No Filter: Social Media Show Raw View of #Ferguson*, USA TODAY (Aug. 19, 2014, 11:05 AM), http://www.usatoday.com/story/news/nation-now/2014/08/14/social-media-ferguson-effect/14052495/ [https://perma.cc/32RT-RLDL] (reporting that the people in Ferguson "did [not] wait for news conferences, petitions or legal action to bring national attention to their streets . . . . They snapped a photo. They used a hashtag. And, in the span of five days, their growing, stinging social media cloud of real-time updates shaped raw public disclosure about the teen, Michael Brown . . . ").

movements.[48] Increasingly, political campaigns also utilize social media platforms to connect politicians and voters.[49] Unfortunately, social media is also used for criminal communications and networking,[50] including use among terrorist organizations.[51]

Governments' inquiries into social media use, typically connected to criminal investigations, further illustrate the importance of information gleaned from social media.[52] Law enforcement officials have "learned from years of experience that criminals are among the first to utilize technology for devious purposes," and have responded by using social media and the content created on them to investigate and prevent crime.[53] This heightened use of social media by individuals and governments for both legal and illegal purposes results in vast amounts of information potentially available in both civil and criminal legal proceedings.

48 *See* Lauren C. Williams, *How NYPD Surveillance Could Affect Eric Garner Protesters*, THINK PROGRESS (Dec. 6, 2014, 10:21 AM), http://thinkprogress.org/justice/2014/12/06/3600158/nypd-social-media-eric-garner-protests/ [https://perma.cc/DB8C-P2C9] (discussing the NYPD's monitoring of social media to track both illegal activities and legal protests, such as the Occupy Wall Street movement in 2012).

49 *See generally* AARON SMITH, PEW RESEARCH CTR., CELL PHONES, SOCIAL MEDIA AND CAMPAIGN 2014 (2014) (discussing how cell phones and social media platforms play an increasing role in how voters receive political information and follow elections news).

50 *See, e.g.*, Tienda v. State, 358 S.W.3d 633, 636 (Tex. Crim. App. 2012) (describing an officer's testimony regarding "the common use of social networking media, such as MySpace, by gangs to stay in touch with members and to 'promote' their gangs by bragging about participation in gang-related activities").

51 *See* Javier Lesaca, *Fight Against ISIS Reveals Power of Social Media*, BROOKINGS (Nov. 19, 2015, 7:30 AM), http://www.brookings.edu/blogs/techtank/posts/2015/11/19-isis-social-media-power-lesaca [https://perma.cc/CR55-FPTR] (noting that ISIS released videos on social media prior to the October 2015 Paris attacks encouraging young French citizens to join the terrorist group); *see also* Marc Santora & Stephanie Clifford, *3 Brooklyn Men Accused of Plot to Aid ISIS' Fight*, N.Y. TIMES (Feb. 25, 2015), http://www.nytimes.com/2015/02/26/nyregion/3-men-in-brooklyn-charged-supporting-isis.html [https://perma.cc/26NK-53RY] (stating that the accused were "influenced by videos posted online by the Islamic State [and] inspired by messages on social media" and that at least one of the accused had posted terroristic messages on websites supportive of ISIS).

52 *See Information Requests (Government) January 1–June 30, 2015*, TWITTER, https://transparency.twitter.com/information-requests/2015/jan-jun [https://perma.cc/33LS-67G8] (last visited Jan. 23, 2016) (showing, among other countries' requests, 2436 account information requests from governments within the United States from January through June of 2015, with 6324 accounts specified in those requests).

53 Edward M. Marsico, Jr., *Social Networking Websites: Are MySpace and Facebook the Fingerprints of the Twenty-First Century?*, 19 WIDENER L.J. 967, 967-72 (2010); *see also id.* at 968 (describing these "devious purposes" as including sexual predation, criminal gang communication and activity, blackmail, and threats). For a detailed discussion of government investigations involving social media evidence, see generally Justin P. Murphy & Adrian Fontecilla, *Social Media Evidence in Government Investigations and Criminal Proceedings: A Frontier of New Legal Issues*, 19 RICH. J.L. & TECH. 1 (2013) (discussing government investigations using publically visible information, fake SNS accounts and "friending" suspects, and subpoenas of social media platform operators).

B. *Social Media Content as Evidence*

While the use of social media and the content created through it has many societal ramifications beyond the scope of this Comment, the discussion above illustrates the widespread impact of social media as a communication and evidentiary tool. Because of its widespread use and sometimes journal-like quality,[54] the content generated on social media sites has broad applicability in many areas of the law.[55] Like any evidence used in litigation, this content must pass several evidentiary hurdles. In particular, social media content and its closely related communication cousins, email and text messaging, raise some problematic authentication concerns.

Civil and criminal litigation alike have recognized this subset of digital information as a valuable asset.[56] Depending on the posting history of the person or of the person's connections, a wealth of information about that person may be accessed, from basic information, such as the person's location at a certain time, friend and family relationships, age, marital status, or ethnic or national identification, to more intimate information such as group affiliations, political leanings, opinions, interests, personal difficulties, sexual orientation, present and past activities, future plans, romantic partners, and medical status. Any of this information could be relevant depending on the type of litigation and facts at issue.[57] Public announcements, private messages, and personal photographs may also be accessible. This wealth of information encompassing

---

54 *See* Megan Uncel, Comment, *"Facebook Is Now Friends with the Court": Current Federal Rules and Social Media Evidence*, 52 JURIMETRICS 43, 68 (2011) (stating that "[t]he content that users post—spontaneous blogs, statuses, and comments—are often stream-of-consciousness statements" that highlight a person's instant thoughts and impressions—valuable evidence in the legal world (internal citation omitted)).

55 In addition to its ability to catalog daily details of people's lives, social media content, like other forms of electronically stored information, has arguably increased in evidentiary value because of the volume of information created and the long-lasting nature of the content. *See* Moore, *supra* note 13, at 150-51 (stating that electronically stored data have "fundamental differences" from more traditional forms of evidence that make them more valuable for litigation, including the greater amount of information storage and significant level of redundancy).

56 The opportunities for using social media content in the courtroom for both civil and criminal legal actions are vast. *See* Grimm et al., *supra* note 19, at 437-38 (discussing the relevance of printouts of files from social media sites to multiple types of litigation, including defamation, personal injury, employment discrimination, and criminal cases); *see also* John G. Browning, *Digging for the Digital Dirt: Discovery and Use of Evidence from Social Media Sites*, 14 SMU SCI. & TECH. L. REV. 465, 468 (2011) (providing advice for practicing attorneys on the discovery of social media evidence and its relevance in multiple areas of litigation, including disputes over custody, divorce, trademark infringement, product liability, insurance, access to benefits, and securities). Social media content is also used in researching and impeaching parties and witnesses, and for investigating jurors. *See generally* Hayes Hunt & Brian Kint, *Juries and Social Networking Sites*, CHAMPION, Dec. 2013, at 36-38 (advising attorneys on using SNS content to research potential jurors and identify juror misconduct).

57 *See* Murphy & Fontecilla, *supra* note 53, at 3 ("The myriad and continually changing ways to share information via social media has resulted in a digital goldmine of potential evidence.").

a person's history and current status, and usually generated by that person, would be especially helpful "whenever motive, state of mind, intent, interpersonal interactions, physical health, and conduct occurring outside of public observation are at issue."[58]

Like any evidence used in litigation, social media content and other digital information must pass several evidentiary hurdles.[59] For a very simple example from the criminal context, a defendant-authored Facebook post, proffered by the prosecution, is admissible as a statement of a party,[60] and if that posted statement makes a material fact of the case more or less probable than if the statement were excluded,[61] the statement will be both relevant and admissible nonhearsay. However, to even reach the general relevance and hearsay questions, the proponent must first clear the authentication hurdle: What showing is required for a factfinder to reasonably conclude that the statement was made by the purported author?[62] While authentication issues can be resolved through litigation tools such as stipulations,[63] if the authenticity remains challenged, the judge will, at the very least, have to make a preliminary determination if enough information exists for a reasonable juror to find the evidence authentic.[64]

Authentication may be the most basic and currently challenging area of admissibility for social media and other digital communications.[65] Critical authentication questions include whether the offered evidence actually represents the social media page and whether the purported author actually

58 Grimm et al., *supra* note 19, at 472.

59 *See generally* Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534 (D. Md. 2007) (opining on the evidentiary issues of electronically stored information including relevance, authenticity, hearsay, best evidence, and unfair prejudice). The *Lorraine* opinion, authored by Judge Grimm, is widely cited in reference to admissibility concerns for all types of electronically stored information. According to Westlaw, as of January 23, 2016, *Lorraine* has been cited in 132 cases. Search Results, WESTLAW NEXT, http://next.westlaw.com (search "241 F.R.D. 534") (last visited Jan. 23, 2016).

60 *See* FED. R. EVID. 801(d)(2) (establishing that statements are not hearsay when "[t]he statement is offered against an opposing party and . . . was made by the party in an individual or representative capacity").

61 *See* FED. R. EVID. 402 (presenting the general admissibility standard of relevant evidence).

62 *See* FED. R. EVID. 901(a).

63 *See* Grimm et al., *supra* note 19, at 467 (urging litigants never to rule out that the opposing party may "stipulate to the authenticity of social media evidence").

64 *See* FED. R. EVID. 104 ("The court must decide any preliminary question about whether a witness is qualified, a privilege exists, or evidence is admissible."); *see also* Grimm et al., *supra* note 19, at 465 (stating that Rule 104's division between preliminary questions and eventual final determinations is the "best approach" to social media content authentication).

65 *See* Orenstein, *supra* note 14, at 202 ("Authentication questions are by far the most interesting issues raised by new social media.").

created the content.[66] The metadata connected to digital communications creates additional authentication issues; this important information, which can include when and where the content was created, and record any changes to it, can be manipulated both purposefully and inadvertently.[67] Because profiles on social media sites can easily be created and modified, forgery concerns repeatedly factor into authenticity determinations.[68] Fundamental authenticity questions[69] fuel both normative and procedural debates over how and when this evidence is sufficiently authentic and should be admitted into evidence. Currently, the Rules create multiple approaches to the procedural question of how digital communication evidence can meet the basic authentication requirement.

II. CURRENT APPROACHES TO SOCIAL MEDIA EVIDENCE AUTHENTICATION

A. *The Applicable Federal Rules*

Under the Federal Rules of Evidence, evidence can only be admitted if it is authentic.[70] According to the Advisory Committee, "[a]uthentication and identification represent a special aspect of relevancy," as evidence must be authentic in order for it to be relevant.[71] The special part of relevancy "falls

66 *See* MCGRADY, *supra* note 44, § 11.04 (citing authentication issues that may arise for a printout of a social media posting, such as whether the printout is actually from the social media website or whether the posting can be shown to have derived from the source the party seeking admission claims).

67 *See* Moore, *supra* note 13, at 152-53 (stating that metadata provides information about a file, such as "the date it was created, its author, when and by whom it was edited, [and] what edits were made," that does not necessarily translate onto a print-out of the information (quoting BARBARA J. ROTHSTEIN ET AL., FED. JUDICIAL CTR., MANAGING DISCOVERY OF ELECTRONIC INFORMATION: A POCKET GUIDE FOR JUDGES 3 (2007), http://www.fjc.gov/public/pdf.nsf/lookup/eldscpkt.pdf/$file/eldscpkt.pdf [https://perma.cc/Y6KR-JEQT])).

68 *See* Griffin v. State, 19 A.3d 415, 422 (Md. 2011) ("The potential for fabricating or tampering with electronically stored information on a social networking site, thus poses significant challenges from the standpoint of authentication of printouts of the site . . . ."); *see also* Colin Miller & Charles White, *The Social Medium: Why the Authentication Bar Should Be Raised for Social Media Evidence*, 87 TEMP. L. REV. ONLINE 1, 7 (2014) ("[T]he fact that a user profile is entirely self-generated can lead to significant mischief and presents an interesting conundrum for law enforcement . . . [and] it does not take much for anyone with Internet access to create a convincing fake Facebook or Twitter profile for someone he barely knows." (footnote omitted)); Moore, *supra* note 13, at 152, 157 (citing both general unreliability of information found online and the ease of outright fabrication as sources for concerns that electronic data has a higher potential to be inaccurate and altered).

69 For example, who created the content? Does the information presented in the legal setting accurately match what exists in the digital landscape? Is the information reliable and accurate?

70 FED. R. EVID. 901; *see also* United States v. Vayner, 769 F.3d 125, 129 (2d Cir. 2014) ("The requirement of authentication is . . . a condition precedent to admitting evidence."(quoting United States v. Sliker, 751 F.2d 477, 497 (2d Cir. 1984))).

71 FED. R. EVID. 901(a) advisory committee's note (citation omitted).

in the category of relevancy dependent upon fulfillment of a condition of fact and is governed by the procedure set forth in Rule 104(b)."[72] Rule 104(b) dictates the preliminary admissibility standard for relevance depending on a fact and states that "[w]hen the relevance of evidence depends on whether a fact exists, proof must be introduced sufficient to support a finding that the fact does exist."[73]

This language mirrors the standard for authentication in Rule 901(a): to satisfy the authentication or identification requirement, "the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is."[74] This sufficiency standard is met when, from the proof offered, a "reasonable juror could find in favor of authenticity or identification."[75] Once this minimal threshold is reached,[76] "[t]he ultimate determination as to whether the evidence is, in fact, what its proponent claims is thereafter a matter for the jury."[77] While authentication issues are infrequent,[78] the need to show authenticity raises the possibility that authentication requirements will pose a major hurdle for potentially important evidence.[79]

Under Rule 901, authentication of evidence happens in different ways. The text of Rule 901(b) provides a list of examples of proper authentication,[80] such as the testimony of a witness with knowledge[81] or the distinctive

---

72 *Id*.

73 FED. R. EVID. 104(b). For additional discussion on Rule 104(b), see Grimm et al., *supra* note 19, at 439-40 ("Rule 104(b), often referred to as the 'conditional relevance rule,' applies during the authentication process when there is a dispute of fact regarding whether an exhibit is authentic . . . .").

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

75 *Vayner*, 769 F.3d at 130 (citation and quotation marks omitted); *see also* FED. R. EVID. 901(a) advisory committee's note (adding that showing authenticity for relevancy is dependent on fulfilling Rule 104(b) requirements, which reserves the final determination of relevancy to the jury).

76 *See Electronic Evidence Symposium*, *supra* note 24, at 1173 (quoting Judge Grimm as stating that the authenticity threshold is "very low").

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

78 *See* FED. R. EVID. 901(a) advisory committee's note ("'Today, such available procedures as requests to admit and pretrial conference afford the means of eliminating much of the need for authentication or identification."); *see also Electronic Evidence Symposium*, *supra* note 24, at 1193 (quoting attorney John Haried as stating that "in many instances, there is no genuine dispute about the authenticity of electronic information").

79 *See* FED. R. EVID. 901(a) advisory committee's note ("[T]he need for suitable methods of proof still remains, since criminal cases pose their own obstacles to the use of preliminary procedures, unforeseen contingencies may arise, and cases of genuine controversy will still occur.").

80 *See* FED. R. EVID. 901(b) (listing "examples only—not a complete list—of evidence that satisfies the requirement"); *see also* Tienda v. State, 358 S.W.3d 633, 640-41 (Tex. Crim. App. 2012) (discussing various modes of authentication used by courts, such as the creator admitting to authorship, witness testimony, business records, contextual or circumstantial information, and the reply doctrine).

81 *See* FED. R. EVID. 901(b)(1) (elaborating that the testimony of a witness with knowledge is "[t]estimony that an item is what it is claimed to be"). A witness with knowledge could include someone who saw a document being signed or the testimony regarding the custody of an object from seizure to trial, commonly referred to as the "chain of custody." *See* FED. R. EVID. 901(b) advisory committee's note.

characteristics based on the circumstances of the evidence,[82] that show that the evidence is what the proponent claims. While explicitly nonexhaustive and intentionally broad,[83] Rule 901 gives examples of authenticating specific forms of evidence, including handwriting,[84] voice identification,[85] and telephone communication.[86] In addition, the Advisory Committee suggests certain attempts that do not satisfy the authentication standard, such as mere self-identification over the telephone.[87] In those cases, the proponent must provide additional indicia of authenticity, such as the content of the conversation or voice identification.[88]

B. *Recent Developments Regarding Changes to the Rules*

There is widespread agreement that courts' inconsistent determinations of threshold authenticity for social media and other digital evidence are undesirable.[89] However, proposed remedies for creating consistency range from requiring higher standards of authentication, to procedural modifications, to arguments that the current Rules are adequate for authenticating evidence from digital communications. The following discussion highlights some of the leading arguments and remaining points of ambiguity.

---

82 *See* FED. R. EVID. 901(b)(4) (illustrating that distinctive characteristics include "appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances"). The circumstantial evidence and distinctive features of an item provide "authentication techniques in great variety," including uniquely known facts to identify a speaker, contents of a letter that indicate it was a reply to an authenticated letter, or even language patterns. FED. R. EVID. 901(b) advisory committee's note.

83 *See* FED. R. EVID. 901(b) advisory committee's note ("The examples 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.").

84 Handwriting can be authenticated through "[a] non expert's opinion that the handwriting is genuine," FED. R. EVID. 901(b)(2), or through a comparison with an authenticated handwriting specimen by an expert witness or the fact finder. FED. R. EVID. 901(b)(3). The authentication of handwriting in subsection (2) requires a layperson's prelitigation familiarity, while subsection (3) requires that an authenticated sample or "exemplar" be available for expert comparison or comparison by a trier of fact. FED. R. EVID. 901(b) advisory committee's note.

85 *See* FED. R. EVID. 901(b)(5) (providing for voice identification "based on hearing the voice at any time under circumstances that connect it with the alleged speaker").

86 *See* FED. R. EVID. 901(b)(6) (noting that "[f]or a telephone conversation, evidence that a call was made to the number assigned at the time," either to a certain person "if circumstances, including self-identification, show that the person answering was the one called," or to a certain business, "if the call was made to a business and the call related to business reasonably transacted over the telephone").

87 FED. R. EVID. 901(b) advisory committee's note.

88 *Id.*

89 *See, e.g.*, Grimm et al., *supra* note 19, at 466, 472 (arguing that social media site usage will continue in its popularity, necessitating that "courts and lawyers . . . do a better job" in using this evidence in courts, as "[i]t serves no interest for the law to remain in its current inconsistent and unpredictable state").

1. Fitting New Evidence into Old Rules: Inconsistent Outcomes

Threshold authentication proposals for social media evidence generally follow one of two approaches.[90] The first, typified by *Griffin v. State*,[91] blends normative and procedural considerations by setting a higher bar for authenticating social media evidence than is required for other types of evidence under the Rules.[92] In *Griffin*, the defendant challenged the introduction of a MySpace profile page printout, which the prosecutor alleged the defendant's girlfriend had created to intimidate a witness in the defendant's trial for a shooting death.[93] The Maryland Court of Appeals stressed how easily social media content could be manipulated or forged and found that this type of evidence "requires greater scrutiny of 'the foundational requirements' than letters or other paper records."[94] The court then held that the State's evidence for finding threshold authenticity—a picture of the purported creator, her birth date, and location—"were not sufficient distinctive characteristics," due to the high risk of manipulability, and named various methods by which a social media page might be authenticated.[95] In courts that follow the *Griffin* approach, evidence from digital communications is not admissible "unless the court definitively determines that the evidence is authentic."[96] That a message facially purports to be from a certain email account or cell phone, or mere self-identification in a chat room, are insufficient to meet this threshold authentication requirement.[97] The courts exclude this evidence because of the "possibility that someone other than the alleged creator of the evidence created or manipulated it."[98]

The second line of cases, typified by *Tienda v. State* and generally followed in the federal court system,[99] more closely tracks the authentication requirements for other forms of evidence and defers competing accounts of

90 *See* Miller & White, *supra* note 68, at 1, 3-6 (stating that in *State v. Parker*, 85 A.3d 682 (Del. 2014), the Delaware Supreme Court described two differing approaches towards authentication requirements: the *Tienda* approach and the *Griffin* approach).

91 19 A.3d 415 (Md. 2011).

92 *See* Miller & White, *supra* note 68, at 5-6 (detailing the "stricter" approach in *Griffin*, where concerns over fraudulent postings appear to drive determinations of admissibility in addition to weight).

93 19 A.3d at 418.

94 *Id.* at 423.

95 *See id.* at 424, 427-28 (suggesting that a webpage could be authenticated through asking the purported creator, searching the computer and hard drive, or obtaining information regarding the site's creation from the social networking site operator).

96 Grimm et al., *supra* note 19, at 441; *see also* Orenstein, *supra* note 14, at 211 (identifying State v. Eleck, 23 A.3d 818 (Conn. App. Ct. 2011), as another case in this line of authentication).

97 *See* Tienda v. State, 358 S.W.3d 633, 641-42 (Tex. Crim. App. 2012) (illustrating the more stringent authentication requirement for social media evidence in the *Griffin* line of cases).

98 Grimm et al., *supra* note 19, at 455.

99 *See Electronic Evidence Symposium*, *supra* note 24, at 1178 (confirming among panel members that federal cases take the "more permissive approach" toward authentication of electronic evidence).

reliability to the factfinder.[100] In these cases, courts approach authentication more liberally and evaluate the evidence using the standard threshold requirement: namely, whether the proponent has produced sufficient evidence for a reasonable jury to find that the proffered evidence is authentic.[101] In *Tienda*, the defendant appealed a murder conviction by challenging the introduction of printouts from MySpace pages the defendant purportedly owned and maintained, which repeatedly referenced the homicide for which the defendant was on trial.[102] Finding that the trial court had not abused its discretion in admitting the profile pages, the Texas Court of Criminal Appeals opined that the pages' content sufficiently authenticated the profiles to the extent that a reasonable juror could find that the defendant created them.[103] The circumstantial evidence considered by the court included pictures of the defendant and the defendant's ankle monitor, references to the victim's death, the defendant's gang affiliation, and a clear connection between the account and an eponymous email.[104] The court acknowledged the possibility of forgery, but stated that this was "an alternate scenario whose likelihood and weight the jury was entitled to assess once the State had produced a prima facie showing" that the defendant created the page.[105]

Despite the existence of two normative approaches to authenticating social media evidence,[106] many academics,[107] courts,[108] practitioners,[109] and law

---

100 *See* Miller & White, *supra* note 68, at 4 (describing the "business as usual" approach in *Tienda*, where fabrication questions influence the weight of the evidence, not its admissibility). As discussed below, the court in *Vayner* explicitly states that it doubts the need for the approach taken in *Griffin*, yet it does not seem to completely follow the "business as usual approach" as outlined in *Tienda*. *See infra* note 108 and accompanying text.

101 *See* Orenstein, *supra* note 14, at 212-15 (outlining the more liberal approach taken by courts in California, Ohio, and Texas, including the approach taken in *Tienda*).

102 *Tienda*, 358 S.W.3d at 635-36.

103 *Id.* at 642.

104 *Id.* at 645.

105 *Id.* at 646.

106 While *Tienda* and *Griffin* are both state cases, "[m]ost state evidence codes echo the wording of Federal Rule 901." Julia Mehlman, *Facebook and MySpace in the Courtroom: Authentication of Social Networking Websites*, 8 CRIM. L. BRIEF 9, 10 (2012).

107 *See, e.g.*, Orenstein, *supra* note 14, at 222-24 (introducing a three-step process for authenticating social network evidence based on existing principles of authentication for other types of evidence).

108 *See, e.g.*, United States v. Vayner, 769 F.3d 125, 131 n.5 (2d Cir. 2014) (declining to address whether specific authentication methods or a heightened standard like the one employed in *Griffin* is required, but noting skepticism regarding heightened scrutiny).

109 *See, e.g.*, David I. Schoen, *The Authentication of Social Media Postings*, ABA (May 17, 2011) http://apps.americanbar.org/litigation/committees/trialevidence/articles/051711-authentication-social-media.html [https://perma.cc/PR28-JR6R] ("In terms of the evidentiary implications arising from [social networking platforms], the problems and the solutions are a mix of the old and the new. Traditional evidentiary principles provide a starting place for analysis.").

students[110] claim that consistent authentication for social media evidence can be accomplished within the current Rules.[111] Some contributors to the conversation have suggested that a "consensus" has been reached that the Rules "already in place for determining authenticity are at least generally adequate to the task."[112] They argue that creative combinations of the current examples can sufficiently reach the threshold consideration and any inconsistencies will eventually be resolved if courts merely apply the current Rules accurately.[113] While advocating for maintaining the current Rules does not necessarily mean that this camp finds the current bar for authentication appropriately set, the viewpoint that the current Rules are procedurally sufficient tends to correspond with a normative belief that the existing minimal threshold for authenticity is also sufficient for these forms of evidence.[114]

In one comprehensive analysis of the various state court approaches to authentication, then–U.S. Magistrate Judge Paul Grimm argued that the current rules of authentication are sufficient for evaluating and authenticating social media evidence.[115] Judge Grimm sees courts' insufficient appreciation of the interplay and operation of Rules 104(a), 104(b), and 901 as a major problem that gives rise to the differences in threshold authenticity determinations.[116] Particularly concerning to Judge Grimm is that many courts that have found social media evidence to be inadmissible "have done so based on the courts' own speculative concerns regarding the reliability of social media evidence and not because the party opposing introduction of the evidence introduced other evidence to raise a genuine dispute about authenticity."[117] The correct application of the current Rules, he argues, will result in courts admitting "clearly authentic evidence" and excluding "clearly

110 *See, e.g.*, Uncel, *supra* note 54, at 57 (arguing that "[a] deeper analysis of the current Federal Rules reveals a sufficient framework within which to work to accommodate the use of social media content as evidence in litigation").

111 The Advisory Committee on the Federal Rules of Evidence has recently decided not to pursue Amendments to Rule 901. *See infra* notes 120–26 and accompanying text.

112 Tienda v. State, 358 S.W.3d 633, 638-39 (Tex. Crim. App. 2012) (citation and quotation marks omitted).

113 *See, e.g.*, Grimm et al., *supra* note 19, at 456-66 ("If followed, the law should become more settled over time, the results should become more predictable, and this consistency should mutually benefit lawyers and judges alike.").

114 *See, e.g.*, Orenstein, *supra* note 14, at 222 ("Fear of the technology has led some courts to demand unreasonable levels of assurance of genuineness, ignoring the judges' initial screens for authenticity should not present a high hurdle to admissibility. True, Facebook pages can be faked. So can written documents.").

115 *See* Grimm et al., *supra* note 19, at 466 (advising lawyers that although "courts have widely divergent and inconsistent rulings regarding the admissibility of social media evidence[,]" they should prepare for authenticating the evidence based on the current principles of evidence).

116 *See id*. at 440 ("It is clear that the best approach for authenticating and admitting social media evidence is to follow Rules 104(a) and (b).").

117 *Id*.

inauthentic evidence"—everything between these two poles will be found "conditionally relevant and admitted for the jury to make the final determination as to authenticity."[118]

While arguing that a uniform application of the existing Rules will resolve the current inconsistency in authentication procedures, many commentators are quick to suggest guidelines to help lawyers and judges reach "predictable decisions regarding how social media evidence should be authenticated."[119] This guidebook approach was adopted by the Advisory Committee on the Rules of Evidence in April 2015, when in lieu of proposing amendments to Rule 901 that specifically address electronic evidence, the Committee decided to provide more guidance for courts and parties in a best practices guide.[120] In their discussion of attorney Greg Joseph's draft of authentication Rules for digital information,[121] members of the committee expressed concern that, while helpful, the listing of authentication factors in Joseph's proposal were "too detailed for a rule."[122] In addition, Committee members observed that rules specifically detailing grounds for authenticity of electronic evidence faced the danger of becoming "outmoded before they are even enacted,"[123] and that a list of authenticity factors would create a "weighing process" that differs in each case and "cannot be encapsulated easily in a rule."[124]

---

118 *See id*. at 440, 465 (stating that Rule 104(b) gives the fact finder the power to resolve the factual decision before determining admissibility); *see also Electronic Evidence Symposium*, *supra* note 24, at 1176 (quoting Judge Grimm as stating that "[i]f the judge makes a preliminary determination that a reasonable jury could find that it is authentic, but also, a reasonable jury could find that it is not authentic, then the trial judge does not make the final call on admissibility").

119 *Id*. at 465-66; *see also, e.g.*, Orenstein, *supra* note 14, at 222-23 (suggesting that a rebuttable presumption of authenticity be found as long as proponents "[l]ay a foundation . . . [, e]stablish ownership of the page . . . [, and] [d]emonstrate that the page owner actually wrote the post in question" using an assortment of the provided examples in Rule 901(b)); Griffith, *supra* note 34, at 215 ("Rule 901(b) illustrates several ways to authenticate evidence . . . [and a]n attorney may combine these approaches to authenticate a particular piece of evidence.").

120 ADVISORY COMM. ON EVIDENCE RULES, MINUTES OF THE MEETING ON OCTOBER 24, 2014, at 26, 27 (Apr. 17, 2015), http://www.uscourts.gov/rules-policies/archives/agenda-books/advisory-committee-rules-evidence-april-2015 [https://perma.cc/T2PN-ZUFG] [hereinafter OCTOBER 2014 MEETING]. In choosing this route, the Committee noted that a manual would be easier to amend to keep pace with advances in technology and could include more citations and information for its users. *Id.* at 27. The best practices sections drafted at the time of the October 2015 meeting included social media authentication, email authentication, and the use of judicial notice to authenticate electronic evidence. ADVISORY COMM. ON EVIDENCE RULES, MINUTES OF THE MEETING OF APRIL 17, 2015, at 31 (Oct. 9, 2015), http://www.uscourts.gov/rules-policies/archives/agenda-books/advisory-committee-rules-evidence-october-2015 [https://perma.cc/2HKQ-5WGC].

121 OCTOBER 2014 MEETING, *supra* note 120, at 26. Joseph's draft of the proposed rule was intended to "codify the [current] case law" of authenticating electronic information, including email, website evidence, and texts. *Id*.

122 *See id.* at 27 (stating a member's opinion that Joseph's proposal was "a very helpful compendium of factors that might go into the authenticity question, but that it was too detailed for a rule").

123 *Id*.

124 *Id*.

Following the current Rule 901(b) examples, however, does not create a cohesive approach between the application and result. Using a witness with personal knowledge may be limited if the alleged creator of the social media page cannot be called as a witness, which would be true in the case of a defendant who does not testify in a criminal case.[125] Even within the much-used example of distinguishing characteristics from Rule 901(b)(4),[126] attempts to authenticate social media evidence may fall short.[127] Particularly in the realm of social media, where discourse and information are at least semi-public by their nature, finding sufficient uniqueness or distinctiveness of the content is more difficult.[128] Other suggestions include utilizing the reply doctrine,[129] a system or process producing reliable results, official publications, and self-authenticating newspaper postings under Rule 902(6).[130] Reaching out beyond Rule 901 to the use of expert witnesses such as computer forensic experts[131] under Rule 702[132] may be a helpful approach where the more technical aspects of digital communications are contested. However, at best, this provides only circumstantial evidence[133] that alone may not be enough to support a reasonable juror finding that the proposed creator was in fact the author. The cost of expert testimony would create a practicability and equitability problem if expert witnesses are consistently

125 *See* FED. R. EVID. 901(b)(1) ("Testimony of a [w]itness with [k]nowledge."); *see also* Grimm et al., *supra* note 19, at 468 (suggesting that the proponent call the creator as witness and ask if the screen shot of the page at issue is accurate).

126 *See Electronic Evidence Symposium*, *supra* note 24, at 1174 (quoting Judge Grimm as commenting that "Rule 901(b)(4) is a utility player in this area").

127 *See* Grimm et al., *supra* note 19, at 469-70 (suggesting that proponents examine characteristics such as "content, whether the post replied to an earlier inquiry of posting, any distinguishing language, abbreviations, slang, punctuation, use of emoticons, nicknames, . . . date" or anything else uniquely known to the person the proponent claims authored the material).

128 *See* Miller & White, *supra* note 68, at 7 ("Because fragments of information, either crafted under our authority or fabricated by others, are available by performing a Google search . . . it does not take much for anyone with Internet access to create a convincing fake Facebook or Twitter profile for someone he barely knows." (citation omitted)); *see also supra* Section I.B.

129 *See* FED. R. EVID. 901(b)(4) advisory committee's note (stating that "a letter may be authenticated by content and circumstances indicating it was in reply to a duly authenticated one").

130 *See* Grimm et al., *supra* note 19, at 470-72 (detailing that a system or process producing reliable results requires a witness or expert who can explain how the social media was created; official publications can verify the authenticity of an interactive website sponsored by a government agency; and newspapers and periodicals can self-authenticate social media evidence including a newspaper or periodical-sponsored posting); *see also* Griffith, *supra* note 34, at 215-16 ("Rule 901(b) illustrates several ways to authenticate evidence, including [t]estimony of witness with knowledge; [d]istinctive characteristics and the like; and [p]rocess or system."(citation and quotation marks omitted)). Many of these options have no significant applicability to personal social media content.

131 *See* Orenstein, *supra* note 14, at 224 (mentioning expert testimony as an option for authentication).

132 *See* FED. R. EVID. 702 (allowing a witness who is "qualified as an expert by knowledge, skill, experience, training, or education" to testify, provided that other enumerated conditions are met).

133 Examples of circumstantial evidence include the origin city of an email or the identification of the computer on which the content was created.

needed to resolve technical evidentiary issues,[134] which could arise any time parties introduce social media evidence.[135] While some of these methods may address certain elements of social media evidence, none of the Rule 901 examples offer complete guidance for authenticating digital communications, leaving procedural gaps in which courts insert their normative concerns regarding the threshold for social media evidence.

Ongoing discussions and multiple guidelines for approaching authentication under the current Rules have not eliminated inconsistencies in approaches to authentication determinations. In *United States v. Jackson*, the defendant was charged with federal mail and wire fraud, arising out of a complicated scheme to link the United Parcel Service with white supremacist groups.[136] As a defense, the defendant sought to introduce racist postings from the white supremacist groups' websites in order to connect the groups to certain pieces of hate mail.[137] The Seventh Circuit upheld the trial court's choice not to permit the website postings, noting that the defendant needed to demonstrate that the groups had actually created the posts that claimed responsibility for the racist mail, "as opposed to being slipped onto the groups' websites by [the defendant] herself, who was a skilled computer user."[138]

The Fifth Circuit approached the authentication of social media evidence in a different manner. In *United States v. Hassan*, the defendants were convicted of multiple terrorism charges.[139] On appeal, two defendants challenged the court's admission of screenshots of Facebook profile pages and connected files, including videos from YouTube, on the grounds that they were not appropriately authenticated.[140] The trial court found that the government had met the prima facie burden for authenticity because these screenshots were self-authenticating as records of regularly conducted

134 *See* Orenstein, *supra* note 14, at 223 (suggesting that less expensive options, such as authentication through circumstantial evidence, would be better when appropriate). Expense is a particular concern for parties who have limited resources. Due to the ubiquity of social media and its broad application, any valid solution to authentication inconsistencies needs to take into account the accessibility of authentication options.

135 For a general discussion on the increased opaqueness of "second generation" evidence for laypersons, including social media, see Erin Murphy, *The Mismatch Between Twenty-First-Century Forensic Evidence and Our Antiquated Criminal Justice System*, 87 S. CAL. L. REV. 633, 638 (2014) ("[T]he adversarial rules underlying the criminal justice system assume that evidence possesses 1G [first generation] characteristics . . . [and] this conflict between the nature of evidence as imagined by the adjudicative system and the actual traits of 2G [second generation] evidence thwarts the system's capacity to safeguard the accuracy and integrity of the factfinding process.").

136 208 F.3d 633, 636 (7th Cir. 2000).

137 *Id.* at 637.

138 *Id.* at 638.

139 742 F.3d 104, 110 (4th Cir. 2014).

140 *Id.* at 132.

activity[141] and had been appropriately linked to the defendants "by tracking the Facebook pages and Facebook accounts to [the defendants'] mailing and email addresses via internet protocol addresses."[142] Because records custodians from Facebook and Google had certified the screenshots, which included the defendants' biographical information, and the prosecutor connected the social media accounts to the defendants through their IP addresses, the Fourth Circuit found no abuse of discretion in admitting the pages.[143]

The Second Circuit has also addressed the proper authentication of evidence from social media. In *United States v. Vayner*, Aliaksandr Zhyltsou successfully appealed his criminal conviction for transfer of a false identification on the grounds that the district court had improperly overruled his authentication objection to a social media page introduced by the government.[144] The Second Circuit found that the district court abused its discretion in admitting the evidence, a printed copy of a profile page on a Russian social media site, VK.com.[145]

At trial, the government's main evidence came from Vladyslav Timku, a friend of the defendant and the alleged recipient of the forged document.[146] Timku testified that Zhyltsou had sent the forgery to Timku's email from the address "azmadeuz@gmail.com," which he identified as "an email address that [he] had often used to correspond with Zhyltsou."[147] The prosecution then introduced a copy of the email, including the attached forged document that showed that it was sent to Timku from the email address "azmadeuz@gmail.com."[148] Other witnesses corroborated that the email had originated in New York City, the location of both the witness and the defendant.[149] Because no metadata was introduced regarding the computer that sent the email or any IP addresses connected to the email,[150] Timku's testimony provided the only evidentiary link between Zhyltsou and "azmadeuz@gmail.com."[151]

---

141 *See* FED. R. EVID. 902(11) (stating that certified domestic records are self-authenticating and can be admitted without extrinsic evidence of authenticity as long as a custodian of the records certifies that they meet the requirements of a "regularly conducted activity" under Rule 803(6)).

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

143 *Id.* at 133-34.

144 769 F.3d 125, 127 (2d Cir. 2014).

145 *Id.* at 127, 129 (stating that the threshold authenticity determination is reviewed for abuse of discretion).

146 *Id.* at 127. Timku testified that he had pled guilty to other charges and that he was familiar with Zhyltsou's forgery work because he had paid him for forged documents in the past. *Id.*

147 *Id.*

148 *Id.*

149 *Id.*

150 *Id.*

151 *Id.* at 127-28.

The government then presented an expert witness to introduce what the government claimed was a printout of Zhyltsou's profile on VK.com.[152] The witness who introduced the printout stated that it was from "the Russian equivalent of Facebook," the web page "purported to be the profile of [the defendant]," and the page displayed a picture of Zhyltsou.[153] Finally, the witness noted that the profile displayed a Skype screen name of Azmadeuz and named the same two employers that Timku had previously testified as Zhyltsou's and his past employers.[154] On cross examination, the witness admitted that he had only used the VK.com site to view this single page, had only a "cursory familiarity" with the website, and did not know if a user needed to verify his or her identity before creating an account.[155] In closing, the Assistant United States Attorney (AUSA) used the webpage to corroborate Timku's testimony connecting the azmadeuz@gmail.com account and the defendant.[156] In overruling the defense's objection to the printout page, the district court stated that the page was the defendant's Facebook page and that it was "fair to assume" that the information on it was from the defendant.[157] In addition, the court stated that there was "no question about the authenticity of the document so far as it's coming off the Internet now."[158] The district court admitted the printout page of the VK.com site and Zhyltsou was convicted of transferring falsified documents.[159]

In vacating Zhyltsou's conviction,[160] the Second Circuit highlighted several concerns with the proffered authentication evidence. First, the court noted the prosecution's fluctuating use of the profile page as evidence.[161] The prosecution had initially represented that the witness did not know who created the page and would testify only to its contents, but the AUSA argued in closing that Zhyltsou owned and created the page.[162] Second, the court noted that the government had failed to proffer evidence that Zhyltsou had

152 *Id.* at 128.

153 *Id.*

154 *Id.* (noting that Skype was described to the court as a "voiceover IP provider").

155 *Id.* at 128-29.

156 *Id.* at 129. The government also introduced evidence that the email account "was closed two days after Zhyltsou had an encounter with federal agents." *Id.* at 128 n.1. However, the Second Circuit stated that the questioning was related to other charges and that "[t]he defense intimated in its summation that Timku would also have had reason to delete the account at that time." *Id.*

157 *Id.* at 128. The ruling that the information on the page was provided by Zhyltsou also prevented any hearsay objections regarding that information. *Id.* at 132.

158 *Id.*

159 *Id.* at 129.

160 *Id.* at 134-35 (vacating and remanding the judgment).

161 *See id.* at 131-32 (concluding that "the government did not provide a sufficient basis on which to conclude that the proffered printout was . . . *Zhyltsou's* profile page" based on the government's inconsistent use of the VK profile page).

162 *Id.* at 131.

in fact created the page. The Second Circuit stated that it was "uncontroverted that information *about* Zhyltsou appeared on the VK page: his name, photograph, and some details about his life consistent with Timku's testimony."[163] However, the court found that the government had not presented any evidence that Zhyltsou had actually created the page or authored its contents.[164] The court drew the following analogy: if the government had tried to introduce "a flyer found on the street" with the defendant's Skype address and alleged that the flyer was written or authorized by him, "the district court surely would have required some evidence that the flyer did, in fact, emanate from Zhyltsou."[165] The court also noted a parallel to the limitations on telephone self-identification and the insufficiency of a "mere assertion of identity."[166] Unlike the Fourth Circuit, the Second Circuit noted that the VK page was not self-authenticating evidence.[167]

Finally, the court rejected the government's argument that the personal information contained on the printout was sufficient to pass the initial authentication threshold. The court noted that "the mere fact that a page with [the defendant's] name and photograph happened to exist on the Internet at the time of [the witness's] testimony does not permit a reasonable conclusion that this page was created by the defendant or on his behalf."[168] While distinctive characteristics "can sometimes alone provide circumstantial evidence sufficient for authentication," the court reasoned that the information on the page was not sufficiently distinctive—other people knew the information and some of those people "may have had reasons to create a profile page falsely attributed to the defendant."[169] The court did not clearly state what evidence would sufficiently authenticate the profile page for the trier of fact, but instead merely decided that the specific type and amount of evidence will depend on context.[170]

The above cases suggest a few areas of continuing inconsistency and ambiguity in authentication. First, courts differ on whether profile pages can be considered business records for the purpose of self-authentication under Rule 902. In *Hassan*, the court allowed the prosecution to admit the profile pages as self-authenticating business records under Rule 902(11),[171] whereas the *Vayner* court noted that none of the categories of self-authenticating

163 *Id.* at 132.

164 *Id.*

165 *Id.*

166 *Id.* (citation omitted).

167 *Id.* at 129 n.4.

168 *Id.* at 132.

169 *Id.*

170 *Id.* at 133.

171 742 F.3d 104, 133 (4th Cir. 2014) (ruling that the Facebook profile screenshots were admissible business records partly due to the certifications of Facebook and Google's records custodians).

evidence applied to the VK page.[172] The *Vayner* court did not indicate why the categories of self-authenticating evidence did not apply.[173] However, it could be because, unlike in *Hassan*, the Government in *Vayner* did not introduce the certificates from the platform's custodians.[174] It could also be a broader statement that personal profile pages are not records of regularly conducted business activity. Regardless, the lack of clarity around the categorization of social media evidence creates inconsistency in the requirements to meet the prima facie burden for admissibility.

Additionally, the threshold standards for authentication is unclear, despite the uniform admissibility standard. For instance, the *Vayner* court found that the VK page "fail[ed] under Rule 901's general authentication requirement,"[175] procedurally meaning that no reasonable juror could find that the defendant owned the profile page from the offered evidence. The court does not decide what evidence would have been sufficient to meet this bar in *Vayner*.[176] While the court stated that a photograph and a name were insufficient, the page also included the defendant's hometown and details of his employment history, as corroborated by Timku.[177] This bootstrapping was the ultimate weight on the side of inauthenticity and inadmissibility.[178] The social media page was admitted to corroborate the likely-to-be-impeached testimony of a government cooperator convicted of *crimen falsi*[179] while the government relied on that very testimony to support the page's authenticity.[180] Thus, admitting the profile page as evidence was harmful to the defendant because it "provided significant corroboration" to the only evidence linking the defendant to the handle "Azmadeuz."[181]

Even if impeachable, however, Timku's testimony and the page contained corroborating information, which, absent a fabrication argument,[182] may have

172 769 F.3d at 129 n.4 ("None of the categories enumerated in [Rule 902] (which include, inter alia, certain public records, periodicals, or business records) applies to the VK page" (emphasis omitted)).

173 *Id.*

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

175 *Vayner*, 769 F.3d at 131 n.5.

176 *Id.* at 133 ("We express no view on what kind of evidence *would* have been sufficient to authenticate the VK page and warrant its consideration by the jury.").

177 *Id.* at 132.

178 *See id.* at 133 ("Given the purpose for which the web page in this case was introduced . . . Rule 901 required that there be some basis beyond Timku's own testimony on which a reasonable juror could conclude that the page in question was . . . in fact *Zhyltsou's* profile.").

179 *Id.* at 133-34. *Crimen falsi* are crimes that involve "some element of dishonesty or false statement," such as perjury, *Crimen Falsi*, BLACK'S LAW DICTIONARY (10th ed. 2014), and are generally admissible against witnesses for impeachment purposes. FED. R. EVID. 609(a)(2).

180 *See Vayner*, 769 F.3d at 134 (discussing Timku's crimes of fraud and other acts of deception as likely bases for the jury to discount his testimony).

181 *See id.* at 134-35 (finding the district court's admission of the VK page harmful to the defendant).

182 The *Vayner* court noted that Zhyltsou also objected to the evidence at trial because it was disclosed to him prior to trial and he did not have time to have the page analyzed to establish its source. *Id.* at 128 n.2. However, the court did not address this issue as the authenticity issue was dispositive. *Id.*

allowed a reasonable juror to determine that the page was Zhyltsou's. As articulated by Judge Grimm, the current threshold for admissibility requires that evidence should be admitted and presented to the factfinder to determine its authenticity and reliability, unless it is clearly inauthentic.[183] Under this formulation, Timku's lack of credibility should come into play for threshold admissibility determinations *only* if the profile page was clearly inauthentic. Perhaps the *Vayner* court's normative stance regarding the admissibility bar played some role in its procedural approach. While the court was, perhaps correctly, concerned with the ability of the profile page to be forged, possibly by Timku,[184] the bootstrapping effect seems to be an argument for the jury to find the page inauthentic and discount the page entirely rather than as an initial threshold determination.[185] Normatively, the *Vayner* court seems to require a higher bar for the initial threshold consideration, despite its stated "skeptical" stance that a higher level of scrutiny or special methods for authenticating evidence from the Internet should be applied.[186]

Regardless of where the threshold for authenticity is set, the Rules need to provide clearer guidance on how to meet it to address concerns raised by the *Jackson* and *Vayner* courts over the heightened ability for someone other than the alleged author to create the digital communication being offered as evidence.[187] Because the format of this evidence does not fit neatly into the current examples provided by the Rules, parties and courts have navigated the determination of threshold authenticity using their own perceptions of the reliability of this evidence as a guide.[188] A court's reservations over the

183 *See* Grimm et al., *supra* note 19, at 465 (noting that courts usually look to Rules 104(a) and (b) when deciding whether to admit social media evidence).

184 *See Vayner*, 769 F.3d at 134 (opining that Timku's history of fraud "may even have led the jury to believe that Timku could have used his expertise in fabricating identities and documents to create false evidence to substantiate his testimony against Zhyltsou").

185 The court may have been able to exclude the profile page under Rule 403 if the court believed that the potential for its introduction to prejudice the defendant would substantially outweigh its probative value. The likely exclusion of evidence is reflected in the Court's analysis of the extremely limited weight of the evidence—due to bootstrapping—and its harmfulness analysis. *Id.* at 134 (finding the profile page to be "the sort of evidence that might well sway a jury confronted with a case otherwise turning solely on the word of a single witness whose credibility was weak . . . ." (citation omitted)). However, the balancing of relevance and prejudicial impact seems to be addressed as part of the authentication question, rather than as a separate consideration under Rule 403.

186 *See id.* at 131 n.5 (expressing the court's skepticism of the *Griffin* finding that there needs to be higher scrutiny of Internet-based evidence because of a "heightened possibility for manipulation").

187 *See id.* at 132 (noting that there was no evidence that the defendant had, in fact, created the page or was responsible for its contents); United States v. Jackson, 208 F.3d 633, 638 (7th Cir. 2000) (emphasizing that the defendant "needed to show that the web postings in which the white supremacist groups took responsibility for the racist mailings actually were posted by the groups, as opposed to being slipped onto the groups' web sites by [the defendant] himself . . . .").

188 *See* Grimm et al., *supra* note 19, at 440 ("[A] number of courts that excluded social media evidence have done so based on the courts' own speculative concerns regarding the reliability of social media evidence.").

increased potential for this type of evidence to be fabricated and misleading may inform its procedural threshold admissibility determination. But, in doing so, the court potentially heightens the standard for authenticating this type of evidence while maintaining that the bar for admissibility remains the same.[189] Without a clearly articulated approach, future litigants and courts will need to make case-by-case determinations of how the threshold for authenticity can be met.

2. Modernizing the Rules for Modern Evidence

While in the minority, various commentators have argued that the Rules should be amended to reflect the real differences between traditional evidence and digital evidence, including social media.[190] The most convincing arguments rest on the Rules' inability to account for the unique evidentiary concerns posed by new communication formats. While the admissibility threshold "is not a particularly high barrier to overcome,"[191] social media and similar digital evidence present distinct considerations for the purposes of authentication.[192] Unique characteristics of electronic data, including the increased ease of manipulation and heightened technological and mechanical sophistication,[193] "demonstrate the significant difference between [digital information] and traditional printed copies of information" that raise new evidentiary issues.[194]

These differences seem to be the root cause of concerns and intuitions regarding anonymity that, while not explicit, may factor into threshold considerations of the authenticity of digital evidence. Rule 901 currently

---

189 The *Vayner* court's explicit skepticism regarding heightened standards for admissibility was cited in a recent decision by the Southern District of New York denying the defendant's motion to exclude the government's evidence from forum posts, private Internet messages, and chat content. *See* United States v. Ulbricht, 79 F. Supp. 3d 466, 472, 487-88 (S.D.N.Y. 2015) (ruling on motions in limine in the upcoming trial for the alleged operator of the online black market site, Silk Road).

190 For the majority view that the current Rules can sufficiently address admissibility issues raised by social media and other digitally stored evidence, see *supra* notes 105–10 and accompanying text.

191 Grimm et al., *supra* note 19, at 457 (citing Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 542 (D. Md. 2007)).

192 *See* Moore, *supra* note 13, at 176 (arguing that some technological developments cannot be analogized to the evidence envisioned under the current Rules).

193 *See* Murphy, *supra* note 135, at 636-37 (advocating for broad systemic reforms to address "second generation forensic evidence," which encompasses evidence gleaned from GPS, DNA, and social media sites). Murphy provides the following example of the increased sophistication of this evidence: while most people can tell whether the blue dot on their GPS device roughly portrays their location, they could not explain exactly *why* the GPS erroneously "thinks" they are located in the middle of lake. *Id.* at 637-38.

194 Moore, *supra* note 13, at 153; *see also id.* at 193 (advocating for amendments to the Federal Rules in light of the inconsistent standards used by courts for admitting electronically stored information).

focuses on evidence that factfinders can "intuitively" understand,[195] such as lay testimony from a person who has some connection to the evidence at issue,[196] the factfinder's own comparisons,[197] or an official's or expert's testimony about the origins of an item.[198] For social media evidence, like many other forms of digital evidence, these more "intuitive" options face limitations when authenticity is contested, and this gap is precisely where courts may insert concerns over fakery and forgery. If the purported creator does not testify, proponents are left with options that do not sufficiently address these suspicions.[199] An expert can testify that the message moved through a certain server and was created on a certain computer, if that evidence is available and the party can afford to retain the expert.[200] However, this expert testimony may not address concerns regarding manipulation of metadata, especially when the testimony points not to a person, but to a machine.[201] As mentioned above, other methods of authentication, including distinct characteristics[202] and the reply doctrine,[203] may also fall short. Overlaying lay and expert testimony may get the proponent closer to admissibility. However, the distinct qualities in any given case create a plethora of different combinations for authentication attempts and current inconsistencies may preclude accurate predictions by proponents regarding sufficient authentication of evidence.[204]

Amending the Rule to accommodate particular evidence types is not without precedent. The Rules already provide specific authentication approaches for evidence that varies by format,[205] and the novel features of digital evidence has spurned formal changes to other areas of civil procedure, particularly discovery.[206]

---

195 *See* Murphy, *supra* note 135, at 638 ("The [current] system assumes that evidence is . . . intuitively accessible and understandable by laypeople.").

196 FED. R. EVID. 901(b)(1)–(3), (5), (6), (8), (9).

197 FED. R. EVID. 901(b)(3), (4).

198 FED. R. EVID. 901(b)(3), (7)–(9); FED. R. EVID. 902(11), (12).

199 *See* Miller & White, *supra* note 68, at 7-14 (discussing the shortcomings of applicable authentication methods for social media evidence due to the higher risk of manipulation).

200 *But see* Uncel, *supra* note 54, at 68 (noting how time consuming and costly forensic examinations can be, making them impractical to use every time social media evidence is contested).

201 *See id.* (stating that one of the basic problems with forensic examination is that it can only discover the computer that was used to create the content).

202 *See* Miller & White, *supra* note 68, at 8 ("The problem is that, as currently applied, 901(b)(4) is an analog rule in a digital world.").

203 *See id.* at 11-13 (discussing the shortcomings of the reply doctrine).

204 *See* Grimm et al., *supra* note 19, at 472 ("The current state of the law regarding admissibility of the evidence is in disarray, sending mixed and confusing messages to lawyers and judges alike and depriving them of the certainty to anticipate in advance of trial the likelihood of admission for social media evidence.").

205 *See supra* Section II.A.

206 *See* Moore, *supra* note 13, at 153-55 (discussing the "e-discovery amendments" to the Federal Rules of Civil Procedure and arguing that the amendments illustrate that digital evidence has been

Recently, the Advisory Committee on the Rules of Evidence has proposed two amendments to Rule 902 to address self-authentication for certain types of electronic evidence.[207] In addition, relying on the development of the law through judicial opinion in an area of judicial discretion—admissibility under Rule 104(a) and (b)—allows inconsistencies in authentication requirements to flourish, as threshold admissibility determinations are reviewed under the highly deferential abuse of discretion standard.[208]

Unfortunately, one hurdle to updating the Rules lies in the overemphasis of concerns regarding anonymity and potential forgery of social media content. In rejecting the sufficiency of the current Rules, proponents of amendments also tend to argue that the threshold authentication bar needs to be raised to address the increased risk of forgery.[209] While this is a legitimate concern and is followed explicitly by a line of state cases, and perhaps implicitly by cases like *Jackson* and *Vayner*, assuming that manipulation has occurred goes too far afield from reality,[210] just as an assumption of authenticity does.[211] As mentioned above, many commentators who support maintaining the Rules simultaneously support keeping the

recognized as sufficiently different to require new approaches to working with this type of evidence). In addition, Congress has recognized some of the unique concerns with electronically stored information by adopting Rule 502, "in part to address the problems of inadvertent waiver caused by the production of electronically stored information." *Id.* at 177.

207 *See* COMM. ON RULES OF PRACTICE AND PROCEDURE OF THE JUDICIAL CONFERENCE OF THE UNITED STATES, PRELIMINARY DRAFT OF PROPOSED AMENDMENTS TO THE FEDERAL RULES OF BANKRUPTCY PROCEDURE AND THE FEDERAL RULES OF EVIDENCE: REQUEST FOR COMMENT 3, at 20-22 (Aug. 2015), http://www.uscourts.gov/rules-policies/proposed-amendments-published-public-comment [https://perma.cc/4ET5-YBE3] (announcing the proposed Rules and opportunity for public comments). Proposed Rule 902(13) allows the introduction of a certificate of authentication for records "generated by an electronic process or system that produces an accurate result." *Id.* at 21. Proposed Rule 902(14) allows the introduction of a certificate of authentication for "[d]ata copied from an electronic device, storage media, or electronic file, if authenticated by a process of digital identification," such as the comparison of the hash values of the two documents. *Id.* at 22. If the amendments are approved, they would become effective December 1, 2017. *Id.* at 4.

208 *See* Moore, supra note 13, at 176 (maintaining that the appellate process does not provide sufficient refinements, because "[o]n appeal, courts are constrained by the highly deferential standard of review for trial court evidentiary rulings"); *see, e.g.*, United States v. Hassan, 742 F.3d 104, 133-34 (4th Cir. 2014) (reviewing admissibility questions of the Facebook pages and YouTube videos for abuse of discretion).

209 *See, e.g.*, Miller & White, *supra* note 68, at 6-8 (discussing social media evidence's higher risk of forgery).

210 *See, e.g.*, Orenstein, *supra* note 14, at 220-21, 224 (addressing the relative unlikelihood of fake pages and hacking, though allowing for these possibilities to contribute to a judge finding a page as inauthentic as a threshold consideration).

211 *See Hassan*, 742 F.3d. at 133 (upholding the state's self-authentication of Facebook postings as business records); *see also* Uncel, *supra* note 54, at 66-68 (advocating for judges to "accept [social media content's] inherent reliability by recognizing an informal presumption of authenticity and reliability" because it better reflects the actual use of social media, namely truthful self-promotion, and prevents the complications of relying on forensic metadata, which is time-sensitive, expensive, and only reveals the computer on which the content was created).

threshold of authenticity low,[212] and this normative disagreement may be an additional roadblock to amending the Rules to address the authentication of digital evidence.

III. SUGGESTIONS FOR AMENDING RULE 901

As reliance on social media and other digital communication forms continues to grow, the Rules need to contain explicit guidance for authenticating the newest forms of communication to avoid inconsistencies in admitting this salient evidence. Regardless of where the authentication threshold for admissibility should be set for digital evidence, the procedures for sufficiently reaching the decided-upon threshold should be uniform. By providing a clear procedure, the Rules can give the legal system more predictability and uniformity in applying the law.[213] While many of the examples given above arise in the criminal context, updating the Rules would also create more uniformity in civil cases where authentication may be at issue.[214]

In order to create consistency and uniformity in application, the Rules should provide specific approaches for authenticating the newest digital communication formats. Despite the potential appeal of cobbling together the current Rules to authenticate digital communications, the Rules themselves should be updated to better account for the pervasive changes in communication technology. Continuing to give suggestions, rather than formalizing this guidance in the Rules, will not adequately accommodate the courts' concerns that this type of evidence is more suspect and has a higher potential for manipulation. Delineating a cohesive approach will help courts avoid over-consideration of the potential for forgery in the threshold authentication analysis.[215] The spectrum of opinions discussed above and application of the current Rules to cases involving social media authentication support the perception that the Rules foster ambiguities in admissibility

212 *See* Uncel, *supra* note 54, at 66-69 (advocating for keeping the standard low, approving of courts that use a liberal approach in authenticating evidence, and warning against the detrimental effects of causing unnecessary loss of valuable evidence).

213 *See* Moore, *supra* note 13, at 175 ("[A]mendments to the rules would provide more guidance to courts and result in a more uniform approach to the admissibility of [electronically stored information], reducing the judge-dependent nature of how the rules are currently applied.").

214 *See id.* at 177-78 (detailing the monetary and time expense of preparing for the "toughest" admissibility standard, and noting that, in addition to creating uniform rulings, Rules that address the new evidentiary issues posed by electronically stored information could help limit these costs); *see also* Orenstein, *supra* note 14, at 193-94 (highlighting the important role social media evidence can play in tort and family law cases at multiple points in litigation, including evidentiary rulings at trial and motions for summary judgment).

215 *See* Orenstein, *supra* note 14, at 221 ("Issues of authentication . . . have caused much more confusion [than other evidentiary issues] perhaps because one must have a basic understanding of the technology to grapple with [the] authenticity issues.").

when they are used to authenticate newer communication formats. While it facially seems that advocates for changing the Rules face an uphill battle against the majoritarian opinion, all stakeholders seek clearer guidance and a desire for courts to approach the authentication of digital communications in a consistent manner.

The Rules should address the different methods of creating digital evidence and the different forms that digital evidence takes. For example, social media pages and email can be accessed from multiple computers and physical locations, whereas text messages may be sent from a single cell phone.[216] By explicitly providing examples of proper authentication for new forms of evidence, the Rules can appropriately address both digital evidence located in less accessible locations, such as text messages, and digital evidence that may raise more concerns over accessibility and manipulability, such as social media content. Providing examples, as the current Rules do, will not likely resolve the normative debate about the initial threshold for authenticity. However, it would make the approaches and debate clearer, and authentication more navigable.

Jonathan Moore, a Virginia attorney, has offered helpful insight into how the Rules could provide better guidance to authenticating electronically stored evidence. Like the *Tienda* approach, these amendments push concerns over fraudulent content to the factfinder.[217] Moore proposes that the example of a witness with knowledge in Rule 901(b)(1) include specific reference to the testimonial requirements for evidence that is currently available in electronic form as opposed to printout-only evidence where the electronic version is not available.[218] He would require a "heightened authentication requirement" for the printout-only evidence to address concerns over mistake and forgery due to the lack of metadata for authenticating the evidence.[219] In contrast, evidence available in digital format could be authenticated based on "chain of custody," such as the route of the email from a specific computer through various servers.[220]

Moore also provides a new illustration under Rule 901(b) for any electronically stored information:

---

216 This technology has changed in recent years with the rise of smartphones—users can also send text messages to phones from computers when they sign in with a connected account. *See infra* note 227 and accompanying text.

217 *See* Moore, *supra* note 13, at 180 (noting that the while "the potential for fraud [in the creation of the material still] exists, the opposing party can explore this possibility through cross-examination").

218 *See id*. at 180. ("Rule 901(b)(1) should be amended to read as follows: 'In the case of electronically stored information, if the evidence has previously been produced or made available in electronic form, testimony about the process by which it was obtained will suffice. Otherwise, such testimony should refer to its substantive content.'").

219 *See id*. at 179-80 (explaining when it is appropriate to prevent the "admissibility of potentially compromised evidence").

220 *See id*. at 180 (stating that when an electronic version of an email is made available, a basic chain of custody testimony suffices to authenticate it).

> The content of electronically stored information, in addition to any other method of authentication, by evidence, through testimony or otherwise, of the presence of specific technological measures. The accuracy of a specific technological measure is a fact of which a court may take judicial notice, provided such notice complies with all applicable rules.[221]

While the Rules should address concerns over forgery and manipulation, Judge Grimm's suggestion for accurate application of Rule 104(b) would sufficiently address any difference between more verifiable, electronically stored data and a physical replication only.[222] As discussed below, Rule 104(b) should be explicitly referenced in amendments to Rule 901 that pertain to newer communication formats so that courts are immediately given guidance for assessing less reliable forms of evidence and evidence where the opponent has alleged manipulation or inauthenticity. While Moore's amendments address the concerns of inauthenticity that surround digital and electronic evidence, his proposed rule for electronically stored information allows continued inconsistency by including the open-ended combinations of current examples in Rule 901(b).

To create consistency in admissibility rulings, Rule 901(b) should provide specific approaches for addressing the different types of digital communication evidence. In order to address the Advisory Committee's concerns that a proposed Rule not be too detailed nor too general,[223] amendments should address categories of information that could be used to authenticate social media and other digital evidence, including distinct content and knowledgeable witnesses, or authentication forms such as metadata. Here, guidance from those who would prefer to use Rule 901(b) as it currently stands could be incorporated with Moore's proposal for electronically stored evidence to illustrate distinct variations in these new communications. For example, an additional entry under Rule 901(b) may be

> 901(b)(12) Social media website and email content. For a website, including personal profiles from social media Internet platforms, testimony that

---

221 Moore, *supra* note 13, at 184.

222 *See* Grimm et al., *supra* note 19, at 465 ("It is clear that the best approach for authenticating and admitting social media evidence is to follow Rules 104(a) and (b). Following such an approach, courts consider evidence from all sources . . . including documents, whether electronic or hard copy . . . on a continuum.").

223 ADVISORY COMM. ON EVIDENCE RULES. *supra* note 120, at 27. The committee noted a problem with a general Proposed Rule in that the existing Rules already govern totality-of-the-circumstances–type considerations. *Electronic Evidence Symposium*, *supra* note 24, at 1191 (quoting Joseph as stating that if the Committee concluded that a generic totality of the circumstances rule would be the best approach, no amendment would be necessary).

> evidence offered in court is an accurate representation of the content at the time in question;[224] and
>
> (i) either testimony from a person with knowledge or other evidence that the purported creator either created the content or had exclusive access to distinct content information;[225] or
>
> (ii) meta-data that connects the published content with a content-creating device and testimony that the purported creator had "primary or exclusive access" to that content-creating device at the time in question.[226]

A brief comment to Rule 901(b)(12) could explain the appropriate way for metadata to provide this "chain of custody" of the email between the device used to generate the content and the eventual recipient.[227] Text messaging, another prevalent form of current communication, would receive a slightly different formulation due to the fact that text messages are generated by a single device:

> 901(b)(13) Text messages from mobile telephones. For text messages, evidence that the message was sent from a specific mobile phone and that the purported creator was in control of the mobile phone at the time in question or that the content of the message was distinctly connected to the purported creator.

The more recent emergence of "cloud" messaging—the ability to send text messages from one account over multiple devices[228]—should result in treatment like other content accessible through multiple devices under the email and website illustration. Other Rules could specifically authenticate

---

224 Grimm et al., *supra* note 19, at 180-81 ("This testimony would be similar to the approach used to authenticate photographs."); *see also* Orenstein, *supra* note 14, at 222 (describing techniques for laying a foundation for the provenance of a social media page, including having the witness "prepared to testify that the printout reflects accurately what the witness saw on the webpage").

225 *See Electronic Evidence Symposium*, *supra* note 24, at 1181 n.37 (providing Gregory Joseph's full proposed rule which allows circumstances to show that a person sent or received an email, including replies, subsequent communications or conduct that reflect knowledge from the email, names or nicknames, signature blocks, or distinctive information that "*would normally be known only* to the *person or to a discrete number or category* of people including the person").

226 *See* Moore, *supra* note 13, at 180-81 (illustrating that the fact that the email's purported author had "primary or exclusive access" could be established through "a witness [who] could testify that only the purported author of the e-mail knew the kind of information it contained" or "[t]estimony that the alleged author took action consistent with the content of the message . . . ."); *see also* Orenstein, *supra* note 14, at 223 (suggesting that ownership of the webpage and authorship of the content at issue could be established through either the testimony of a witness with knowledge, metadata, or distinctive circumstantial evidence).

227 *See* Moore, *supra* note 13, at 180 (describing the chain of custody of an email as "the e-mail's electronic routing information, introducing the routing records for each server that handled the message . . . .").

228 *See, e.g.*, *Messages*, APPLE, https://www.apple.com/ios/messages [https://perma.cc/485W-QL2R] (last visited Jan. 23, 2016) (advertising that text messages can be sent over iPhone, iPad, and iPod touch devices under one user account).

other forms of digital information, such as data stored on hard drives. Finally, Rule 901 should explicitly state the mechanism for determining the effect of the opponent's introduction of allegations and evidence of forgery (and thus lack of relevance).[229] This could be included in the specific examples above or addressed in its own section:

> 901(c) Evidence of the Proffered Evidence's Inauthenticity. As per Rule 104(b),[230] if the opponent of the proffered evidence shows sufficient evidence of forgery, fraud, or inauthenticity such that no reasonable juror could find that the purported author created the proffered evidence, the proffered evidence should be deemed inadmissible.

This explicit guidance would direct concerned threshold decisionmakers to the Rule 104 standard, and prevent admission of digital communication evidence that no reasonable juror could find that the purported author created.[231]

The above proposals build on the areas of agreement between academics and courts alike. Incorporating the suggestions for authentication under the current Rules that have wide support, such as Rule 901(b)(1)'s testimony of a person with knowledge, into a specific illustration will result in more uniform application of the current authentication standard. The normative question of whether the authentication standard is appropriate remains open, but adding specific examples for digital communication evidence to the Rules will address the gap in authenticity determinations. Specific examples will aid courts in avoiding the universally disliked inconsistency and navigate some of the underlying distrust of newer communication formats without overstating the authentication requirements or unnecessarily preventing the fact finder from considering relevant evidence.

CONCLUSION

Attempts to manipulate the current Rules to address the newest forms of communication create discrepancies in authentication determinations. These inconsistencies suggest that the disconnect between the current Rules and these new forms of communication needs to be resolved more formally. Regardless of whether the bar for authentication is appropriately set for digital evidence, the Rules can provide better guidance regarding authentication instead of

---

229 *See* Grimm et al., *supra* note 19, at 439-40 (stating that Rule 104(b) "applies during the authentication process when there is a dispute of fact regarding whether an exhibit is authentic," such as when both sides offer facts that could establish the evidence as authentic or not authentic); *see also supra* subsection II.B.1.

230 *See* FED. R. EVID. 901(a) advisory committee's note (stating that the authentication requirement "falls in the category of relevancy dependent upon fulfillment of a condition of fact and is governed by the procedure set forth in Rule 104(b)").

231 *See supra* subsection II.B.1.

relying on suggestions for how to accommodate social media and other digital evidence within the current Rules. Until more definitive examples are provided, concerns regarding the increased ability to manipulate social media and other digital communications will continue to inform threshold admissibility decisions and entrench inconsistent approaches. The increasing prevalence of this type of salient evidence, as evidenced through widespread social media use, only heightens the need for the proactive solution of providing clear approaches to digital evidence authentication.

* * * * *