Authentication of Social Media Evidence

Honorable Paul W. Grimm[†]
Lisa Yurwit Bergstrom[††]
Melissa M. O'Toole-Loureiro[†††]

Abstract

The authentication of social media evidence has become a prevalent issue in litigation today, creating much confusion and disarray for attorneys and judges. By exploring the current inconsistencies among courts' decisions, this Article demonstrates the importance of the interplay between Federal Rules of Evidence 901, 104(a), 104(b), and 401—all essential rules for determining the admissibility and authentication of social media evidence. Most importantly, this Article concludes by offering valuable and practical suggestions for attorneys to authenticate social media evidence successfully.

Introduction

Ramon Stoppelenburg traveled around the world for nearly two years, visiting eighteen countries in which he "personally met some 10,000 people on the road, slept in 500 different beds, ate some 1,500 meals[,] and had some 600 showers," without spending any money.[1] Instead, his blog, *Let-Me-Stay-For-A-Day.com*, fueled his travels.[2] He spent time each evening updating the blog, encouraging people to invite him to stay

---

[†] B.A. (1973), University of California; J.D. (1976), University of New Mexico School of Law. Paul W. Grimm is a District Judge serving on the United States District Court for the District of Maryland. In September 2009, the Chief Justice of the United States appointed Judge Grimm to serve as a member of the Advisory Committee for the Federal Rules of Civil Procedure. Judge Grimm also chairs the Advisory Committee's Discovery Subcommittee.

[††] B.A. (1998), Amherst College; J.D. (2008), University of Baltimore School of Law. Ms. Bergstrom is a law clerk in Judge Grimm's office.

[†††] B.A. (2008), University of Maryland; J.D. (2012), University of Baltimore School of Law. Ms. O'Toole-Loureiro is a law clerk in Judge Grimm's office.

The views expressed in this Article are those of the authors and not the United States District Court for the District of Maryland.

[1] Ramon Stoppelenburg, LET-ME-STAY-FOR-A-DAY.COM, http://www.letmestayforaday.com (last visited June 2, 2013).

[2] *Id.*

at their houses in exchange for having him blog about his experiences with them.[3] He accepted donations from companies (plane tickets, clothes, mobile services) in exchange for providing advertising space and shout-outs on his website.[4] Essentially, through online communications, Stoppelenburg bartered time, entertainment, and publicity for all of his travel expenses,[5] and he was featured as the Wikipedia "Leisure example" of social media usage.[6]

"Social media," a relatively new term dating back only to 2004, is defined as "forms of electronic communications (as websites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (as videos)."[7] Social media allows individuals and organizations to use the Internet to create and exchange "User Generated Content" that is "continuously modified by all users in a participatory and collaborative fashion."[8] Content is user generated if it (1) is "published either on a publicly accessible website or on a social networking site accessible to a selected group of people," as opposed to e-mailed; (2) "show[s] a certain amount of creative effort," rising above republication of existing content; and (3) is "created outside of professional routines and practices" such that it was not intended for a "commercial market."[9] Social media offers individuals opportunities for interactions with others and further offers companies and organizations opportunities to advertise their products or services.[10]

---

[3] *Id.*

[4] *Id.*; *Ramon Stoppelenburg*, WIKIPEDIA, http://en.wikipedia.org/wiki/Ramon_Stoppelenburg (last modified Mar. 17, 2013, 8:14 PM).

[5] *See* Stoppelenburg, *supra* note 1.

[6] *See Social Media*, WIKIPEDIA, http://en.wikipedia.org/wiki/Social_media (last visited Sept. 21, 2011); *see also* WIKIPEDIA, *supra* note 4.

[7] Definition of *Social Media*, MERRIAM-WEBSTER, http://www.merriam-webster.com/dictionary/social%20media# (last visited June 2, 2013).

[8] Andreas M. Kaplan & Michael Haenlein, *Users of the World, Unite! The Challenges and Opportunities of Social Media*, 53 BUS. HORIZONS 59, 61 (2010).

[9] *Id.*

[10] *See id.* at 64 ("Virtual social worlds offer a multitude of opportunities for companies in marketing (advertising/communication, virtual product sales/v-Commerce, marketing research), and human resource and internal process management . . . .").

The better-known forms of social media include weblogs, social networking sites, content communities, collaborative projects or "wikis," and virtual worlds.[11] Weblogs, commonly called "blogs," are reincarnations of what once were known as "personal web pages" and "usually display date-stamped entries in reverse chronological order."[12] Blogs typically provide either "commentary or news on a particular subject" or personal accounts of the blogger's life, and "[t]he ability for readers to leave comments in an interactive format is an important part of many blogs."[13] On microblogs, such as Twitter, users post and read "tweets"—very brief "text-based posts . . . displayed on the author's profile page and delivered to the author's subscribers."[14] Content communities enable users to share media content such as videos on YouTube and photographs on Flickr, and collaborative projects such as Wikipedia "enable the joint and simultaneous creation of content by many end-users."[15] Virtual worlds, which include social worlds such as Second Life and game worlds such as World of Warcraft, "replicate a three-dimensional environment in which users can appear in the form of personalized avatars and interact with each other as they would in real life."[16]

"Social networking" is the term for "building online communities of people who share interests or activities, or who are interested in exploring the interests and activities of others."[17] Social networking encompasses using sites such as Facebook and MySpace to "keep in touch" and "to have a presence on the web without needing to build a website" and using "business-oriented social networking site[s]" such as LinkedIn "for professional networking."[18] Through social networking sites, users may "creat[e] personal information profiles, invit[e] friends and colleagues

---

[11] *Id.* at 62-64.

[12] *Id.* at 63.

[13] U.S. JUDICIAL CONFERENCE COMM. ON CODES OF CONDUCT, RESOURCE PACKET FOR DEVELOPING GUIDELINES ON USE OF SOCIAL MEDIA BY JUDICIAL EMPLOYEES, 10-11 (2010) [hereinafter RESOURCE PACKET], *available at* http://www.uscourts.gov/uscourts/RulesAndPolicies/conduct/SocialMediaLayout.pdf.

[14] *Id.* at 11.

[15] Kaplan & Haenlein, *supra* note 8, at 62-63.

[16] *Id.* at 64.

[17] RESOURCE PACKET, *supra* note 13, at 9.

[18] *Id.* at 9-10.

to have access to those profiles" and, in some instances, communicate by posting information on their own profiles and allowing others to do the same, including "sending e-mails and instant messages between each other."[19]

In the past, Stoppelenburg's approach to social media during his travels may have seemed extreme—a hyperbole of the average person's or business's social media usage. Yet, "participation in social computing is now a daily fact of life for more than 400 million people," and "[u]ntil recently, most Internet users were mere 'consumers' of content; now many are creating their own content and interacting with other users."[20] For example, Facebook's Chief Executive Officer, Mark Zuckerberg, recently announced that "more than one billion people" worldwide are now using Facebook each month—approximately "one out of every [seven] people on the planet."[21] Moreover, the Pew Research Center reports that 66% of all adults with Internet access use various "social media platforms such as Facebook, Twitter, MySpace[,] or LinkedIn."[22] While young adults remain "the heaviest users of social networking" (86% reported in 2010), "[s]ocial networking use among [I]nternet users ages 50 and older . . . nearly doubled" in 2010.[23] The increasing prevalence of social media use amongst all demographics caught the attention of the 2012 Presidential candidates, President Barack Obama and Governor Mitt Romney.[24] Their respective campaign staffs used social networking and social media to connect with voters at unprece-

---

[19] Kaplan & Haenlein, *supra* note 8, at 63.

[20] RESOURCE PACKET, *supra* note 13, at 5.

[21] Aaron Smith et al., *Facebook Reaches One Billion Users*, CNNMONEY (Oct. 4, 2012, 9:50 AM), http://money.cnn.com/2012/10/04/technology/facebook-billion-users/index.html?hpt=hp_bn5 (internal quotation marks omitted).

[22] Aaron Smith, *Why Americans Use Social Media*, PEW INTERNET, 2 (Nov. 14, 2011), http://pewinternet.org/~/media//Files/Reports/2011/Why%20Americans%20Use%20Social%20Media.pdf.

[23] Mary Madden, *Older Adults and Social Media*, PEW INTERNET, 2 (Aug. 27, 2010), http://pewinternet.org/~/media//Files/Reports/2010/Pew%20Internet%20-%20Older%20Adults%20and%20Social%20Media.pdf.

[24] *See* Jenna Wortham, *Winning Social Media Votes*, N.Y. TIMES, Oct. 8, 2012, at B1, *available at* 2012 WLNR 21297954 ("Campaigns of Pres[.] Obama and Mitt Romney are pursuing online audiences with new intensity; seeking out votes from citizens, particularly younger ones . . . .").

dented levels throughout the campaign.[25] They just might be onto something: during the October 3, 2012 presidential debate, Twitter users posted 10.3 million tweets in a mere ninety minutes.[26] After Governor Romney mentioned "Big Bird," the star of the popular children's show *Sesame Street*, during the debate, 17,000 tweets per minute appeared referencing Big Bird and 10,000 tweets per minute referenced PBS, the channel hosting the show.[27] Social media is ubiquitous, and it is here to stay.

The base elements of Stoppelenburg's social media use were the same: he reached out to others; he communicated frequently; he made "friends"; he documented his activities; and his site provided advertising space.[28] More importantly, his considerations of the legal implications of his blogging may be akin to the average person's thoughts on how social media could play a role in a possible future lawsuit or criminal case—negligible, at best. The possibilities, however, are endless. Social media usage has formed the basis for lawsuits and criminal prosecutions. For example, a former prosecutor now faces felony charges due to an allegedly threatening rant he posted on Facebook about his former employer,[29] and an NBA referee recently sued the Associated Press and a sports writer for defamation, claiming that the writer's Twitter message harmed "his professional reputation" as a referee and "led to a disciplinary investigation by the NBA."[30] Moreover, printouts of electronic files from social media websites—especially blog and social networking websites—are increasingly relevant to many areas of litigation, ranging from criminal

---

[25] *See id.*; *see also* Jenna Wortham, *Campaigns Use Social Media to Lure Younger Voters*, N.Y.TIMES.COM (Oct. 7, 2012), http://www.nytimes.com/2012/10/08/technology/campaigns-use-social-media-to-lure-younger-voters.html?amp&_r=0.

[26] Catherine Clifford, *What You Can Learn About Social Media from Big Bird*, ENTREPRENEUR.COM (Oct. 8, 2012, 4:50 PM EST), http://www.nbcnews.com/id/49334469#.UZPxVrvLi9s.

[27] *Id.*

[28] *See* Stoppelenburg, *supra* note 1.

[29] Louis Hansen, *Ex-Norfolk Prosecutor Charged over Facebook Posts*, PILOTONLINE.COM (July 27, 2012), http://hamptonroads.com.nyud.net/2012/07/exnorfolk-prosecutor-charged-after-facebook-post.

[30] Associated Press, *Bill Spooner Sues AP Writer over Tweet*, ESPN (Mar. 15, 2011, 6:30 PM), http://sports.espn.go.com/nba/news/story?id=6218678.

cases[31] to personal injury cases[32] and even employment discrimination.[33] Attorneys frequently seek relevant social media content in discovery, and the content is often subject to a civil litigant's common law duty to preserve evidence relevant to a foreseeable lawsuit.[34] One should expect social media evidence to be offered in any litigation that involves the state of mind, intent, or motives of the parties. Jurors, attorneys, and even judges may use social media in conjunction with a case.[35]

In short, lawyers and judges who lament the explosion of social media use and the evidentiary challenges social media presents when offered as evidence need to, in the vernacular of any teenaged Facebook user, just get over it. This Article is intended to help them to do just that. Here, we focus on the authentication of social media evidence at civil and criminal trials.[36] Part I discusses the case law to date. In Part II, we discuss the factors governing the authentication of social media evidence. Part III provides a checklist to assist lawyers and judges in analyzing authentication issues relating to social media.

The focus of this Article is the authentication of social media evidence, rather than the broader subject of its overall admissibility. The oft-cited

---

[31] *See generally, e.g.*, State v. Gurney, No. CR-2009-4017, 2010 WL 3830832 (Me. Super. Ct. July 12, 2010) (order denying motions to suppress evidence, including evidence contained on the defendant's Facebook account).

[32] *See generally, e.g.*, Romano v. Steelcase Inc., 907 N.Y.S.2d 650 (N.Y. Sup. Ct. 2010) (order in personal injury case granting defendant's motion for access to plaintiff's Facebook and MySpace accounts).

[33] *See generally, e.g.*, Equal Emp't Opportunity Comm'n v. Simply Storage Mgmt., LLC, 270 F.R.D. 430 (S.D. Ind. 2010) (order ruling on discovery issues, including whether the plaintiffs had to produce their MySpace and Facebook profiles).

[34] *See, e.g.*, Victor Stanley, Inc. v. Creative Pipe, Inc., 269 F.R.D. 497, 521 (D. Md. 2010) (order granting in part and denying in part plaintiff's motion for sanctions against defendant for spoliation of electronically stored evidence) ("The common law imposes the obligation to preserve evidence from the moment that litigation is reasonably anticipated.").

[35] *See generally, e.g.*, Veremis v. Gratiot Place, LLC, No. 07-63269-NI-3, 2010 WL 6826665 (Mich. Cir. Ct. Dec. 29, 2010) (order denying defendant's motion for judgment notwithstanding the verdict or in the alternative a new trail where the defendant argued that one of the jurors had Facebook "friended" the plaintiffs during the trial).

[36] Our analysis will focus on the Federal Rules of Evidence, but most states have identical or similar requirements in their rules of evidence. References to "Rule" refer to the Federal Rules of Evidence unless otherwise noted.

case *Lorraine v. Markel American Insurance Co.*[37] identifies and discusses all of the issues a court may need to consider in determining admissibility of digital evidence, which include relevance, authenticity, hearsay, the original writing rule, and probative value as compared with possible unfair prejudice.[38] While there are multiple evidentiary issues that affect the admissibility of any electronic evidence, the greatest challenge is how to authenticate digital evidence. That is where we will focus.[39]

This Article focuses on Federal Rule of Evidence 901, which deals with authentication,[40] as well as Federal Rules of Evidence 104(a) and 104(b)—rules that are rarely discussed yet are inextricably intertwined with Rule 901 and greatly impact the authentication of social media evidence.[41] In a nutshell, Rule 901(a) establishes the requirement of authentication or identification as a condition precedent to the admissibility of nontestimonial evidence.[42] Rule 901(b) identifies ten nonexclusive examples of how authentication can be accomplished, many of which are tailor-made for use in authenticating social media evidence.[43] Rule 104(a) works in tandem with Rule 901(a) because it establishes the responsibility of the trial judge to make preliminary determinations regarding the admissibility of evidence.[44] Authenticity is one of those preliminary determinations.[45] Rule 104(b), perhaps the most enigmatic evidence rule, can be especially important in the process of authenticating social media and other digital evidence. Rule 104(b), often referred to as the "conditional relevance rule," applies during the authentication

---

[37] 241 F.R.D. 534 (D. Md. 2007).

[38] *Lorraine*, 241 F.R.D. at 538.

[39] *See id.* at 541-62 (discussing authenticating electronically stored information); Paul W. Grimm et al., *Back to the Future:* Lorraine v. Markel American Insurance Co. *and New Findings on the Admissibility of Electronically Stored Information*, 42 AKRON L. REV. 357, 366-96 (2009) (offering a broader analysis of authentication).

[40] *See* FED. R. EVID. 901.

[41] *See* FED. R. EVID. 104(a)-(b).

[42] *See* FED. R. EVID. 901(a).

[43] *See* FED. R. EVID. 901(b).

[44] *See* Grimm et al., *supra* note 39, at 363-64.

[45] *See* FED. R. EVID. 901 advisory committee's note to subdivision (a).

process when there is a dispute of fact regarding whether an exhibit is authentic—such as when the proponent of the evidence offers facts to establish authenticity that would be sufficient to persuade a reasonable jury by a preponderance of the evidence that the exhibit is authentic, but at the same time, the party seeking to exclude the evidence offers other evidence that could persuade a reasonable jury that the exhibit is not authentic.[46] When this situation occurs, the trial judge cannot determine authentication as a preliminary matter under Rule 104(a) because there is a genuine dispute of fact that must be resolved before a final determination may be made.[47] For example, an exhibit determined to be inauthentic is irrelevant because an inauthentic document has no tendency whatsoever to make a material fact to the litigation more or less probable, and therefore, that exhibit should be excluded.[48] Rule 104(b) allocates to the ultimate fact finder—the jury in all nonbench trials—the responsibility to resolve disputes of fact, which include genuine factual disputes regarding the authenticity of digital evidence.[49]

This Article examines the dynamic between Rules 104(a), 104(b), and 901 as they relate to the authentication of social media evidence. Courts that have decided issues regarding authenticity of social media have not demonstrated sufficient appreciation of these rules and their operation. Of most concern, 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 and not because the party opposing introduction of the evidence introduced other evidence to raise a genuine dispute about authenticity. Finally, this Article considers the rare case to date where the opponent of the evidence showed—through facts rather than conjecture—that the evidence may be inauthentic, resulting in the issue being given to the jury for ultimate resolution without any discussion of Rule 104(b)—the very rule which allows the jury to do so.

---

[46] *See* Grimm et al., *supra* note 39, at 364-66; *see also* FED. R. EVID. 104(b).

[47] *See* FED. R. EVID. 104 advisory committee's note to subdivision (b).

[48] *See* FED. R. EVID. 401 (defining relevant evidence); *see* FED. R. EVID. 402 ("Irrelevant evidence is not admissible.").

[49] *See* FED. R. EVID. 104 advisory committee's note to subdivision (b).

I. Existing Case Law (Clear as Mud)

At present, the cases that address the authentication and admissibility of social media evidence—typically photographs and postings on MySpace and Facebook pages—unfortunately arrive at widely disparate outcomes. One line of cases sets an unnecessarily high bar for the admissibility of social media evidence by not admitting the exhibit unless the court definitively determines that the evidence is authentic. Another line of cases takes a different tact, determining the admissibility of social media evidence based on whether there was sufficient evidence of authenticity for a reasonable jury to conclude that the evidence was authentic.

Perhaps the most comprehensive case in the first line is *Griffin v. State*,[50] involving a homicide. In *Griffin*, the State offered printouts from the defendant's girlfriend's MySpace profile, on which the statement "FREE BOOZY [defendant's nickname]!!!! JUST REMEMBER SNITCHES GET STITCHES!! U KNOW WHO YOU ARE!!" appeared, to show that the girlfriend, Ms. Barber, had threatened another State witness prior to trial by posting that warning on her profile.[51] Outside the jury's presence, the State only offered testimony from its lead investigator in an "attempt[] to authenticate the pages, as belonging to Ms. Barber."[52] The investigator testified that he knew it was the girlfriend's page "'[t]hrough the photograph of her and Boozy on the front, through the reference to Boozy, [] the reference [to] the children, and [] her birth date indicated on the [printout].'"[53] Counsel for the defense objected to the evidence "because the State could not sufficiently establish a 'connection' between the profile and posting and Ms. Barber."[54] The trial court admitted the printouts.[55] The defendant was convicted and he appealed.[56]

---

[50] 19 A.3d 415 (Md. 2011).

[51] *Griffin*, 19 A.3d at 418 (quoting Ms. Barber's MySpace profile) (internal quotation marks omitted).

[52] *Id.*

[53] *Id.* (alterations in original) (quoting Sergeant Cook's testimony).

[54] *Id.*

[55] *Id.* at 417, 419.

[56] *Id.* at 417.

On appeal, the defendant alleged that the printouts were inadmissible because they were not properly authenticated.[57] The Maryland Court of Special Appeals noted the lack of Maryland precedent and "scant case law from other jurisdictions" regarding the authentication of social media evidence and, specifically, the "authentication of a printout from a MySpace or Facebook profile."[58] The court also noted that, in many jurisdictions, chat logs may be authenticated by either party to the conversation[59] or through circumstantial evidence and context such as special code words or phrases unique to those engaging in the communication.[60] Observing that "social networking profiles contain information posted by someone with the correct user name and password,"[61] the court acknowledged the differences between a printout of a "pseudonymous social networking profile" and "real time" instant messages between site members and recognized the "concern that someone other than the alleged author may have accessed the account and posted the message in question."[62] Nonetheless, the court regarded "decisions as to authentication of evidence from chat rooms, instant messages, text messages, and other electronic communications . . . instructive to the extent that they address the matter of authentication of pseudonymous electronic messages based on content and context."[63] The court referenced the "inherent nature" of social networking websites as encouraging users to individualize their profile by posting various forms of identifying personal information such as "profile pictures or descriptions of . . . physical appearances, personal background information, and lifestyles."[64] The court analyzed the content and context of the posting at issue and found that the circumstantial evidence of the user's birthdate, a photo-

---

[57] *Id.*

[58] Griffin v. State, 995 A.2d 791, 799, 804 (Md. Ct. Spec. App. 2010), *rev'd*, 19 A.3d 415 (Md. 2011).

[59] *See, e.g.*, FED. R. EVID. 901(b)(1) (stating that testimony by a witness with knowledge is sufficient to satisfy the authentication requirement).

[60] *Griffin*, 995 A.2d at 805 (quoting State v. Bell, 882 N.E.2d 502, 512 (Ohio Ct. Com. Pl. 2008)); *see, e.g.*, FED. R. EVID. 901(b)(4) (stating that distinctive characteristics may satisfy the authentication requirement).

[61] *Griffin*, 995 A.2d at 805.

[62] *Id.* at 805-06 (internal quotation marks omitted).

[63] *Id.* at 806.

[64] *Id.*

graph of the user with the defendant "in an embrace," multiple references to the defendant's nickname, and a reference to the user's children sufficient to authenticate the printout and therefore admit the document into evidence.[65]

The Court of Appeals reversed and remanded,[66] holding that

> the picture of Ms. Barber, coupled with her birth date and location, were not sufficient "distinctive characteristics" on a MySpace profile to authenticate its printout [pursuant to Md. Rule 5-901, which is materially similar to Federal Rule of Evidence 901], given the prospect that someone other than Ms. Barber could have not only created the site, but also posted the "snitches get stitches" comment.[67]

Quoting *Lorraine v. Markel American Insurance Co.*,[68] the court stated that "the 'requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims,' to insure trustworthiness."[69] The court continued, "[A]uthenticating electronically stored information presents a myriad of concerns because 'technology changes so rapidly[,]' . . . is 'often new to many judges,'" and "requires greater scrutiny of 'the foundational requirements' than letters or other paper records, to bolster reliability."[70] The court observed that "[t]he identity of who generated the profile may be confounding, because 'a person observing the online profile of a user with whom the observer is unacquainted has no idea whether the profile is legitimate,'"[71] and with "relative ease," a person "can create a fictitious account and masquerade under another person's name or can gain access to another's account by obtaining the user's username and password."[72]

---

[65] *Id.* at 797, 806.

[66] *Griffin*, 19 A.3d at 418.

[67] *Id.* at 424.

[68] 241 F.R.D. 534 (D. Md. 2007).

[69] *Griffin*, 19 A.3d at 423 (quoting *Lorraine*, 241 F.R.D. at 541-44).

[70] *Id.* (quoting *Lorraine*, 241 F.R.D. at 543-44).

[71] *Id.* at 421 (quoting Nathan Petrashek, *The Fourth Amendment and the Brave New World of Online Social Networking*, 93 MARQ. L. REV. 1495, 1499 n.16 (2010)).

[72] *Id.* (citing David Hector Montes, *Living Our Lives Online: The Privacy Implications of Online Social Networking*, 5 ISJLP 507, 508 (2009)).

Considering "[t]he potential for abuse and manipulation of a social networking site by someone other than its purported creator and/or user," the court concluded that a printout from a social media site "requires a greater degree of authentication than merely identifying the date of birth of the creator and her visage in a photograph on the site" to determine that the person whose birthday is listed and whose photograph appears on the site is both the creator of the site and the person who wrote the posting.[73] The court identified proper means to authenticate printouts of postings on social media sites as follows: (1) "ask the purported creator if she indeed created the profile and also if she added the posting in question"; (2) "search the computer of the person who allegedly created the profile and posting and examine the computer's internet history and hard drive to determine whether that computer was used to originate the social networking profile and posting in question"; and (3) "obtain information directly from the social networking website that links the establishment of the profile to the person who allegedly created it and also links the posting sought to be introduced to the person who initiated it."[74]

The dissent stated that, given the investigator's testimony and the website's contents, "a reasonable juror could conclude . . . that the redacted printed pages of the MySpace profile contained information posted by Ms. Barber," and "'a document is properly authenticated if a reasonable juror could find in favor of authenticity.'"[75] Judge Harrell, writing for the dissent, noted that "'[i]n a jury trial, the judge need not be personally satisfied, by even a preponderance of the evidence, that the proffered item is authentic; the judge must find the authentication requirement met, if a reasonable jury could find the evidence to be what its proponent claims it to be.'"[76] He further observed that, while the majority concerned itself with the possibility that "someone other than Ms. Barber could access or create the account and post the threatening message," the facts on the record "suggest[ed] no motive to do so," and

---

[73] *Id.* at 423-24.

[74] *Id.* at 427-28.

[75] *Id.* at 429 (Harrell, J., dissenting) (emphasis omitted) (quoting United States v. Gagliardi, 506 F.3d 140, 151 (2d Cir. 2007)).

[76] *Id.* at 429 n.2 (quoting 6A LYNN MCLAIN, MARYLAND EVIDENCE: STATE AND FEDERAL § 901:1 (2d ed. 2001)).

therefore, "[t]he potentialities that are of concern to the Majority Opinion are fit subjects for cross-examination or rebuttal testimony and go properly to the weight the fact-finder may give the print-outs."[77]

Relying on *Griffin*, the court in *Commonwealth v. Wallick*[78] held that a photograph is insufficient to authenticate a MySpace page because "[t]he fact that there are photographs of [an individual] on [a] particular webpage does nothing to indicate who created or maintained the page. . . . [T]hey merely offer evidence that the person who did maintain the MySpace page had access to photographs of Defendant."[79] The court concluded that the photographs offered by the Commonwealth "from [Defendant's] alleged MySpace page . . . for purposes of authenticating the MySpace page"[80] were not relevant and therefore were inadmissible.[81]

Similarly, in *Commonwealth v. Williams*,[82] a witness testified that the defendant's brother had the MySpace screen name "doit4it" and had a photo of himself on his MySpace page.[83] The witness said that the defendant's brother—using the screen name "doit4it"—contacted her through four instant messages on her MySpace page to tell her "not to testify against the defendant or to claim a lack of memory about the events at her apartment the night of the murder" with which the defendant was charged.[84] Over the defendant's objection, the trial court admitted the witness's testimony about the messages, although it did not admit printouts of the MySpace page.[85]

The appellate court analogized the MySpace messages to a phone call, stating that "a witness's testimony that he or she has received an incoming call from a person claiming to be 'A,' without more, is insufficient evidence to admit the call as a conversation with 'A.'"[86] Noting that the

---

[77] *Id.* at 429-30.

[78] No. CP-67-CR-5884-2010 (Pa. Ct. Com. Pl. Oct. 2011).

[79] *Wallick*, No. CP-67-CR-5884-2010, slip. op. at 10-11.

[80] *Id.* at 9.

[81] *Id.* at 11.

[82] 926 N.E.2d 1162 (Mass. 2010).

[83] *Williams*, 926 N.E.2d at 1172.

[84] *Id.* at 1165, 1172.

[85] *Id.* at 1171 & n.9.

[86] *Id.* at 1172 (citing Commonwealth v. Hartford, 194 N.E.2d 401 (Mass. 1963)).

State did not offer any evidence about "how secure such a Web page is, who can access a MySpace Web page, whether codes are needed for such access, etc.," the court held that the trial court should not have admitted testimony about the messages because the State failed to lay an adequate foundation to authenticate the MySpace messages.[87] The court concluded that "while the foundational testimony established that the messages were sent by someone with access to [the defendant's brother's] MySpace Web page, it did not identify the person who actually sent the communication."[88] The court added that there also was no "expert testimony that no one other than [the defendant's brother] could communicate from that Web page."[89]

Likewise, in *People v. Beckley*,[90] Beckley's girlfriend testified that she associated with gang members.[91] To rebut this testimony, the prosecution offered into evidence a photograph of the girlfriend displaying a gang hand signal; a detective "testified that he downloaded the photograph from Beckley's home page on the internet website MySpace."[92] Beckley and his codefendants objected that the photograph "had not been authenticated," but the trial court admitted the evidence.[93] The jury returned a guilty verdict.[94]

On appeal, the California Court of Appeal held that "the prosecution's failure to authenticate a photograph . . . downloaded from [an] internet web site[] should have barred [the photograph's] admission."[95] The appellate court reasoned that "the record does not contain . . . evidence sufficient to sustain a finding that it is the photograph that the prosecution claims it is, namely, an accurate depiction of [the girlfriend] actually flashing a gang sign" even though appellants "conceded that the face in the MySpace photograph was [the girlfriend's]."[96] The court noted that

---

[87] *Id.* at 1172-73.

[88] *Id.*

[89] *Id.* at 1173.

[90] 110 Cal. Rptr. 3d 362 (Ct. App. 2010).

[91] *Beckley*, 110 Cal. Rptr. 3d at 365.

[92] *Id.* at 365-66.

[93] *Id.* at 366.

[94] *Id.* at 364.

[95] *Id.*

[96] *Id.* at 366.

"no expert testified that the picture was not a 'composite' or 'faked' photograph," and "digital photographs can be changed to produce false images."[97] Nonetheless, the *Beckley* court concluded that the admission of the evidence was harmless error.[98]

The Connecticut Appellate Court reached a similar conclusion in *State v. Eleck*.[99] There, the defendant offered into evidence printouts of Facebook messages he allegedly received from a State witness.[100] Through his own testimony to authenticate the printouts, the defendant showed that (1) "he downloaded and printed the exchange of messages directly from his own computer"; (2) "he recognized the user name, 'Simone Danielle,' as belonging to [the State witness]"; (3) "the 'Simone Danielle' profile contained photographs and other entries identifying [the State witness] as the holder of that account"; and (4) "when [the defendant] logged in to his Facebook account after the previous day's testimony, user 'Simone Danielle' had removed him from her list of Facebook 'friends.'"[101] The State witness claimed that, although the messages did come from her account, her account was hacked, and she was unable to access it for some time.[102] The trial court ruled that the messages were inadmissible; the defendant did not provide enough circumstantial evidence to prove who sent the Facebook messages, such that the messages lacked a sufficient foundation for authentication.[103] The appellate court affirmed[104] and explained,

---

[97] *Id.*; *see also* People v. Lenihan, 911 N.Y.S.2d 588, 591-93 (N.Y. Sup. Ct. 2010) (affirming trial court's ruling that defendant could not use photographs printed from MySpace to cross-examine two witnesses because, "[i]n light of the ability to 'photo shop,' edit photographs on the computer, defendant could not authenticate the photographs," and "[d]efendant did not know who took these photographs or posted them on 'Myspace'").

[98] *Beckley*, 110 Cal. Rptr. 3d at 364. *But see* United States v. Phaknikone, 605 F.3d 1099, 1101-06 (11th Cir. 2010) (affirming trial court's admission of photographs from a MySpace page, which the court admitted after "the government laid the foundation for the MySpace evidence by showing the photographs, profile page, and subscriber report to [a witness who knew Phaknikone], who identified Phaknikone as the person pictured" and "through the testimony of an employee of MySpace").

[99] 23 A.3d 818, 821-25 (Conn. App. Ct. 2011).

[100] *Eleck*, 23 A.3d at 820.

[101] *Id.* at 820-21.

[102] *Id.* at 820.

[103] *See id.*

[104] *Id.* at 824-25.

> The need for authentication arises in this context because an electronic communication, such as a Facebook message, an e-mail or a cell phone text message, could be generated by someone other than the named sender. This is true even with respect to accounts requiring a unique user name and password, given that account holders frequently remain logged in to their accounts while leaving their computers and cell phones unattended. Additionally, passwords and website security are subject to compromise by hackers. Consequently, proving only that a message came from a particular account, without further authenticating evidence, has been held to be inadequate proof of authorship.[105]

The court further explained that "[a]n electronic document may continue to be authenticated by traditional means such as the direct testimony of the purported author or circumstantial evidence of 'distinctive characteristics' in the document that identify the author."[106]

These cases follow earlier decisions that revealed courts' skepticism about website contents and their reluctance to admit printouts from the Internet. For example, in *St. Clair v. Johnny's Oyster & Shrimp, Inc.*,[107] the plaintiff offered a printout from the U.S. Coast Guard's online vessel database to support the plaintiff's claim that the defendant owned the vessel involved in the accident with plaintiff.[108] The defendant moved for dismissal, arguing the plaintiff's evidence was insufficient to show that the defendant owned the vessel.[109] The court granted the motion, stating,

> Plaintiff's electronic "evidence" is totally insufficient to withstand Defendant's Motion to Dismiss. While some look to the Internet as an innovative

---

[105] *Id.* at 822.

[106] *Id.* at 823; *see also* United States v. Jackson, 208 F.3d 633, 637-38 (7th Cir. 2000) (affirming the trial court's exclusion of evidence defendant offered in the form of postings from the websites of white supremacist groups in which the groups "gloat about the Jackson case [and] take credit for the [acts for which Jackson was indicted]"; reasoning in part that the defendant failed to lay an appropriate foundation to authenticate the printouts because she did not demonstrate that the postings "actually were posted by the groups, as opposed to being slipped onto the groups' web sites by Jackson herself, who was a skilled computer user").

[107] 76 F. Supp. 2d 773 (S.D. Tex. 1999) (order conditionally denying defendant's motion to dismiss).

[108] *St. Clair*, 76 F. Supp. 2d at 774.

[109] *Id.*

> vehicle for communication, the Court continues to warily and wearily view it largely as one large catalyst for rumor, innuendo, and misinformation. So as to not mince words, the Court reiterates that this so-called Web provides no way of verifying the authenticity of the alleged contentions that Plaintiff wishes to rely upon in his Response to Defendant's Motion. There is no way Plaintiff can overcome the presumption that the information he discovered on the Internet is inherently untrustworthy. Anyone can put anything on the Internet. No web-site is monitored for accuracy and *nothing* contained therein is under oath or even subject to independent verification absent underlying documentation. Moreover, the Court holds no illusions that hackers can adulterate the content on *any* web-site from *any* location at *any* time. For these reasons, any evidence procured off the Internet is adequate for almost nothing, even under the most liberal interpretation of the hearsay exception rules found in Fed. R. [Evid.] 807.[110]

In the other line of cases, as noted, courts more appropriately evaluated whether there was sufficient evidence of authenticity for a reasonable jury to conclude that the evidence was authentic in order to determine the admissibility of social media evidence.

One example is *Tienda v. State*.[111] At Tienda's trial on murder charges, the State offered into evidence several MySpace pages from three MySpace accounts allegedly belonging to Tienda.[112] The victim's sister, who directed the State to the pages, was the "sponsoring witness for these MySpace accounts," and a detective testified about typical gang usage of social media.[113] Each account stated that it was "created by a 'Ron Mr. T'" or Tienda's well-known nickname, "'Smiley Face,'" and that the account owner lived in Dallas, or "'D TOWN,'" where Tienda lived.[114] The accounts were registered to e-mail addresses with Tienda's name or nickname in them.[115] One account included a heading reading "'RIP [the victim]'" above a link to the song that was played at the victim's funeral.[116] The accounts linked to photographs of someone who "at least resembled" Tienda; instant messages between the account owner

---

[110] *Id.* at 774-75.

[111] 358 S.W.3d 633 (Tex. Crim. App. 2012).

[112] *Tienda*, 358 S.W.3d at 634-35.

[113] *Id.* at 635-36.

[114] *Id.* at 634-35.

[115] *Id.* at 635.

[116] *Id.*

and others referenced details surrounding the murder in question and mentioned that the account owner was placed on electronic monitoring.[117] Tienda repeatedly objected, and his counsel "elicited testimony regarding the ease with which a person could create a MySpace page in someone else's name and then send messages, purportedly written by the person reflected in the profile picture, without their approval" as well as testimony that the detective did not know how MySpace accounts were created.[118] Nonetheless, the trial court admitted the evidence, which the State referenced repeatedly in closing argument.[119] Tienda was convicted of murder.[120]

Tienda appealed, contending that it was error for the trial court to admit the MySpace evidence.[121] Relying on the Maryland Court of Special Appeals' opinion in *Griffin v. State*,[122] the intermediate appellate court concluded that the Texas trial court did not err in admitting the evidence.[123] The court of criminal appeals recognized that the Maryland Court of Appeals reversed *Griffin*,[124] and it noted,

> That an email on its face purports to come from a certain person's email address, that the respondent in an internet chat room dialogue purports to identify himself, or that a text message emanates from a cell phone number assigned to the purported author—none of these circumstances, without more, has typically been regarded as sufficient to support a finding of authenticity.[125]

The Court of Criminal Appeals of Texas nonetheless affirmed the intermediate appellate court, reasoning that "there [were] far more circumstantial indicia of authenticity in [*Tienda*] than in *Griffin*."[126]

---

[117] *Id.* at 635-36.

[118] *Id.* at 636.

[119] *Id.* at 634, 636.

[120] *Id.* at 636.

[121] *Id.* at 637.

[122] Griffin v. State, 995 A.2d 791, 799 (Md. Ct. Spec. App. 2010), *rev'd*, 19 A.3d 415 (Md. 2011).

[123] *Tienda*, 358 S.W.3d at 637 & n.7.

[124] *Id.* (citing Griffin v. State, 19 A.3d 415 (Md. 2011)).

[125] *Id.* at 641-42.

[126] *Id.* at 647.

Relying on *Lorraine v. Markel American Insurance Co.*,[127] the court stated that, "as with the authentication of any kind of proffered evidence, the best or most appropriate method for authenticating electronic evidence will often depend upon the nature of the evidence and the circumstances of the particular case."[128] The court concluded that there was "ample circumstantial evidence—taken as a whole with all of the individual, particular details considered in combination—to support a finding that the MySpace pages belonged to the appellant and that he created and maintained them."[129] Thus, the Court of Criminal Appeals of Texas concluded that the trial court did not abuse its discretion in admitting the pages.[130] The court stated that whether Tienda's MySpace page had been fabricated was an "alternate scenario whose *likelihood and weight the jury was entitled to assess*."[131]

In *State v. Assi*,[132] after noting that "[t]he trial court need not 'determine whether the evidence is authentic, but only whether evidence exists from which the jury could reasonably conclude that the evidence is authentic,'"[133] the appellate court concluded that "the State presented sufficient evidence at trial from which the *jury could reasonably conclude* [that] Defendant [Assi] was the subject of the MySpace page associated with the username profile 'Flaco.'"[134] At Assi's trial for attempted second-degree murder of a former gang member, the trial court admitted a detective's testimony about Assi's MySpace page and "photographs of [Assi] taken from his MySpace page."[135] The photos showed guns, Assi "posing with guns," and Assi "'throwing up gang signs.'"[136] Following a guilty verdict, Assi appealed, arguing that the MySpace photos

---

[127] 241 F.R.D. 534 (D. Md. 2007).

[128] *Tienda*, 358 S.W.3d at 639.

[129] *Id.* at 645.

[130] *Id.* at 647.

[131] *Id.* at 646 (emphasis added).

[132] No. 1 CA-CR 10-0900, 2012 WL 3580488 (Ariz. Ct. App. Aug. 21, 2012).

[133] *Assi*, 2012 WL 3580488, at *3 (quoting State v. Damper, 225 P.3d 1148, 1152 (Ariz. Ct. App. 2010)).

[134] *Id.* (emphasis added).

[135] *Id.* at *2.

[136] *Id.* at *3.

lacked a proper foundation.[137] The appellate court catalogued the evidence offered to authenticate the MySpace page as Assi's:

> Defendant was known to gang unit officers as Flaco and as a member of PBS. Defendant was the only documented PBS member in police gang records who went by the nickname "Flaco," and two other gang members who were in the Nissan at the time of the shooting . . . testified that Defendant was a member of PBS and went by the nickname Flaco. When Defendant was arrested, he admitted to being a member of PBS and that his nickname was Flaco. Defendant's father also testified that Defendant had a MySpace page and he had seen the photographs in Exhibits 20, 21, and 22 on Defendant's MySpace page.[138]

The court also stated that, because "[t]he State introduced the MySpace information for identification purposes," there was a sufficient foundation that the page was actually created by Assi.[139]

Similarly, in *People v. Valdez*,[140] the trial court admitted MySpace printouts to "(1) corroborat[e] a victim's statement to investigators shortly after the first shooting that the victim recognized Valdez from the MySpace site and (2) as foundation for [the prosecution's gang expert's] . . . testimony" that Valdez was a gang member.[141] The jury found Valdez guilty on various counts,[142] and Valdez appealed, arguing, *inter alia*, that the court should not have admitted the MySpace printouts because they were not authenticated.[143] The appellate court observed that Valdez's photo appeared as the "owner of the [MySpace] page," postings on the page referred to him by his first name, his sister referred to him as her brother, and personal details in postings by the owner and others "matched what the police otherwise knew of Valdez's interests."[144] The court stated that, "[a]lthough Valdez was free to argue otherwise to the jury, *a reasonable trier of fact could conclude* from the posting of

---

[137] *Id.* at *2-3.

[138] *Id.* at *3.

[139] *Id.* at *4.

[140] 135 Cal. Rptr. 3d 628 (Ct. App. 2011).

[141] *Valdez*, 135 Cal. Rptr. 3d at 632.

[142] *Id.* at 630.

[143] *Id.* at 632.

[144] *Id.* at 633.

personal photographs, communications, and other details that the MySpace page belonged to him."[145] Thus, noting that there only has to be "'*a sufficient showing of authenticity of the writing to permit the trier of fact to find that it is authentic*,'"[146] the appellate court concluded that "the prosecution met its initial burden to support its claim the MySpace site belonged to Valdez, and that the photographs and other content at the page were not falsified but accurately depicted what they purported to show."[147] Additionally, the court stated that "the trial court could conclude that particular items on the page, including a photograph of Valdez forming a gang signal with his right hand, met the threshold required for the jury to determine their authenticity" because "[t]he contents of a document may authenticate it," and other "consistent, mutually-reinforcing content on the page helped authenticate the photograph and writings."[148]

The appellate court distinguished *People v. Beckley*,[149] in which the court found a website photograph to be insufficiently authenticated because "'[a]nyone can put anything on the Internet.'"[150] The *Valdez* court noted that in the case before it—unlike *Beckley*—there was "evidence of the password requirement for posting and deleting content" and "pervasive consistency of the content of the page, filled with personal photographs, communications, and other details tending together to identify and show owner-management of a page devoted to gang-related interests."[151] Additionally, the court reasoned that, "unlike other authority on which Valdez relie[d], nothing suggested he had a personal enemy with a motive to implicate Valdez in future gang crimes by creating an entire site or individual postings on it."[152]

---

[145] *Id.* (emphasis added).

[146] *Id.* at 632-33 (emphasis added) (quoting CAL. EVID. CODE § 1400 (West, Westlaw through 2012 Reg. Sess.)).

[147] *Id.*

[148] *Id.* at 633-34.

[149] 110 Cal. Rptr. 3d 362 (Ct. App. 2010); *see supra* text accompanying notes 91-98.

[150] *Valdez*, 135 Cal. Rptr. 3d at 634 (alteration in original) (quoting *Beckley*, 110 Cal. Rptr. 3d at 367).

[151] *Id.*

[152] *Id.*

In *People v. Clevenstine*,[153] the State offered into evidence a computer disk containing instant messages exchanged on MySpace between the defendant and his victims whom he allegedly raped.[154] The defendant objected, alleging that the evidence "had not been properly authenticated."[155] The trial court admitted the evidence, the jury returned a guilty finding, and the defendant appealed.[156] The appellate court affirmed, holding that there was "ample authentication for admission of this evidence."[157] The appellate court noted that

> both victims testified that they had engaged in instant messaging about sexual activities with defendant through the social networking site MySpace, an investigator from the computer crime unit of the State Police related that he had retrieved such conversations from the hard drive of the computer used by the victims, a legal compliance officer for MySpace explained that the messages on the computer disk had been exchanged by users of accounts created by defendant and the victims, and defendant's wife recalled the sexually explicit conversations she viewed in defendant's MySpace account while on their computer.[158]

The court acknowledged "it was possible that someone else accessed his MySpace account and sent messages under his user name" but determined that the trial court "properly concluded that, under the facts of this case, the likelihood of such a scenario presented *a factual issue for the jury*."[159] Other cases in which the courts have admitted evidence for the jury to determine its authenticity include *Manuel v. State*[160] and *In re T.T.*[161]

---

[153] 891 N.Y.S.2d 511 (N.Y. App. Div. 2009).

[154] *Clevenstine*, 891 N.Y.S.2d at 513-14.

[155] *Id.* at 514.

[156] *Id.* at 513-14.

[157] *Id.* at 514.

[158] *Id.*

[159] *Id.* (emphasis added).

[160] 357 S.W.3d 66, 75, 79-82 (Tex. Ct. App. 2011) (relying on FED. R. EVID. 901(b)(4) and the reply-letter doctrine to conclude that the trial court properly admitted electronic communications that Manuel allegedly sent via MySpace and Facebook because "a *reasonable fact finder could find* that [Manuel] sent the electronic communications attributed to him by the State and depicted in the challenged exhibits" (emphasis added)).

[161] 228 S.W.3d 312, 321-22 (Tex. Ct. App. 2007) (admitting a MySpace webpage as evidence against a father in termination of parental rights case after the father

II. Determining the Authenticity of Social Media Evidence

Broadly speaking, the cases that address the admissibility of social media evidence tend to fall into two categories. In the first category, courts expressed skepticism about admitting social media evidence[162] or a website printout[163] because the proponent failed to introduce evidence that affirmatively disproved the *possibility* that someone other than the alleged creator of the evidence created or manipulated it.[164] Simply put, the possibility that the evidence may have been created by someone other than its putative creator—even in the absence of any evidence that in fact this happened—appears to have been sufficient for these courts to exclude the evidence.[165] In contrast, in the second category of cases, the courts

---

"admitted that he had a webpage on 'myspace.com'" but "claimed not to know about the contents of the webpage"; reasoning that "[t]here was *sufficient evidence for the jury reasonably to conclude that [the father] set up the webpage*" because (1) the man who the father alleged created the page testified that "he did not set up and knew nothing about any webpage that [the father] had on 'myspace.com,'" (2) the mother testified that the father "had been unfaithful to her," and (3) the contents of the page included a photograph of the father, identified him as single, and included "the statement, 'I don't want kids'" (emphasis added)).

[162] *See generally* United States v. Jackson, 208 F.3d 633 (7th Cir. 2000); State v. Eleck, 23 A.3d 818 (Conn. App. Ct. 2011); Commonwealth v. Wallick, No. CP-67-CR-5884-2010 (Pa. Ct. Com. Pl. Oct. 2011); People v. Beckley, 110 Cal. Rptr. 3d 362 (Ct. App. 2010); Griffin v. State, 995 A.2d 791 (Md. Ct. Spec. App. 2010), *rev'd*, 19 A.3d 415 (Md. 2011); Commonwealth v. Williams, 926 N.E.2d 1162 (Mass. 2010); People v. Lenihan, 911 N.Y.S.2d 588 (N.Y. Sup. Ct. 2010).

[163] *See* St. Clair v. Johnny's Oyster & Shrimp, Inc., 76 F. Supp. 2d 773 (S.D. Tex. 1999) (order conditionally denying defendant's motion to dismiss).

[164] Curiously, in *United States v. Jackson*, although the court ultimately concluded that Jackson did not sufficiently authenticate the social media evidence she offered because she failed to show that the postings "actually were posted by the groups, as opposed to being slipped onto the groups' web sites by Jackson herself, who was a skilled computer user," the court also scoffed at the Government's argument that "Jackson concocted these documents and posted them on the supremacists' web sites in an attempt to cover up her crimes"—calling it a "novel theory" under which "defense evidence should be excluded whenever the prosecution pronounces it phony." 208 F.3d 633, 637-38 (7th Cir. 2000). Moreover, the court acknowledged that "[s]orting truth from fiction, of course, is for the jury." *Id.* at 637.

[165] *See* State v. Eleck, 23 A.3d 818, 822-25 (Conn. App. Ct. 2011) (printout of instant message from defendant's Facebook page not properly authenticated where there was no assurance that defendant's account was not hacked); Commonwealth v.

concluded that all the proponent had to do to authenticate social media evidence was to introduce sufficient facts—generally by any of the methods identified by Rule 901(b) (and state evidence rules equivalents) to persuade a reasonable juror that the evidence was created by the person who the proponent alleged created the evidence.[166] Once the proponent produces sufficient evidence to convince a reasonable juror that the social media evidence is authentic, the burden of production shifts to the party objecting to the introduction of the evidence as inauthentic to prove facts demonstrating that the putative creator did not create the evidence.[167] If this is done, assuming that a reasonable juror could find for either the proponent of the evidence or for the party objecting to the evidence, it is appropriate for the trial judge to admit the evidence conditionally and to allow the jury to determine whether to accept or reject the evidence. The approach adopted by the second category of cases is better reasoned, as it affords appropriate deference to the interplay between the evidence rules that govern the admissibility of social media evidence: Rule 104(a) and (b),[168] Rule 901,[169] and Rule 401.[170]

The cases that approach the authentication of social media evidence as a determination based on whether there is sufficient evidence for a reasonable jury to conclude that the evidence is authentic are not introducing a new concept. Rather, courts historically considered admissibility of all documentary evidence on a continuum, in which clearly authentic evidence is admitted, clearly inauthentic evidence is excluded,

---

Williams, 926 N.E.2d 1162, 1171-73 (Mass. 2010) (message not properly authenticated, even though it came from purported sender's MySpace page, because "there is no testimony (from [the recipient] or another) regarding how secure such a Web page is, who can access a MySpace Web page, whether codes are needed for such access, etc.," and also no testimony circumstantially to "identify the person who actually sent the communication").

[166] *See generally* State v. Assi, No. 1 CA-CR 10-0900, 2012 WL 3580488 (Ariz. Ct. App. Aug. 21, 2012); People v. Valdez, 135 Cal. Rptr. 3d 628 (Ct. App. 2011); People v. Clevenstine, 891 N.Y.S.2d 511 (N.Y. App. Div. 2009); Tienda v. State, 358 S.W.3d 633 (Tex. Crim. App. 2012); Manuel v. State, 357 S.W.3d 66 (Tex. Ct. App. 2011); *In re* T.T., 228 S.W.3d 312 (Tex. Ct. App. 2007).

[167] *See Tienda*, 358 S.W.3d at 642-47 (where the defendant was unable to disprove evidence of his MySpace profiles).

[168] FED. R. EVID. 104(a)-(b) (preliminary rulings on admissibility of evidence).

[169] FED. R. EVID. 901 (authentication).

[170] FED. R. EVID. 401 (relevance).

and everything in between is conditionally relevant and admitted for the jury to determine its authenticity.[171] The United States District Court for the District of Maryland outlined this approach for electronic evidence in *Lorraine v. Markel American Insurance Co.*[172] There, the court comprehensively discussed "the evidentiary issues associated with the admissibility of electronically generated and stored evidence," including the judge-jury relationship addressed by Rule 104 and authentication under Rules 901 and 902[173] in an analysis that the *Griffin v. State* court acknowledged but did not apply to authentication of social media site contents.[174] The *Lorraine* court noted that the authentication requirement "'as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.'"[175] It explained that "[t]his is not a particularly high barrier to overcome," as "[a] party seeking to admit an exhibit need only make a prima facie showing that it is what he or she claims it to be,"[176] and "'[t]he court need not find that the evidence is necessarily what the proponent claims, but only that there is sufficient evidence that the *jury* might ultimately do so.'"[177] Indeed, the "requirement of authentication or identification is the paradigm of a preliminary question."[178]

In the vast majority of cases, when the proponent of documentary or similar evidence—whether digital or hard copy—offers the exhibit into evidence, there either is no authenticity objection at all or a formalistic objection that the foundation offered was inadequate because of an asserted failure to produce evidence that would fit within one of the methods of authentication illustrated in Rule 901(b) or Rule 902. Seldom does the objecting party offer a competing version of facts that would

---

[171] *See* Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 538-39 (D. Md. 2007).

[172] 241 F.R.D. 534 (D. Md. 2007).

[173] *Lorraine*, 241 F.R.D. at 537-54.

[174] 19 A.3d 415, 422-24, 427-28 (Md. 2011).

[175] 241 F.R.D. at 541-42 (quoting FED. R. EVID. 901(a)).

[176] *Lorraine*, 241 F.R.D. at 542 (citing 5 JACK B. WEINSTEIN & MARGARET A. BERGER, WEINSTEIN'S FEDERAL EVIDENCE § 901.02[3] (Joseph M. McLaughlin ed., 2d ed. 1997)).

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

[178] 1 JACK B. WEINSTEIN & MARGARET A. BERGER, WEINSTEIN'S FEDERAL EVIDENCE § 104.30[3] (Joseph M. McLaughlin ed., 2d ed. 2012).

rebut those offered by the proponent to show that the exhibit is what the proponent contends it is. When all that the objecting party offers is speculation or conjecture about who, other than the putative creator, "could" have created the evidence, such questions are properly left to the jury in determining how much weight, if any, to give to the evidence—provided that the trial judge is convinced that the proponent has met the relatively low threshold required by Rule 901(a) of producing facts that would be sufficient for a reasonable jury to conclude that the evidence was created by the putative creator. In these circumstances, it is the trial judge's decision whether the evidence is authentic pursuant to Rule 104(a).

Only in the comparatively less frequent case where the proponent of the evidence proves facts sufficient to justify a jury's conclusion that the evidence is authentic, and the opponent proves facts that also would justify a reasonable jury in reaching the opposite conclusion does the judge not have the final say about the admissibility of the evidence. In such an instance, the court is faced with a conditional relevance issue under Rule 104(b). When a conditional relevance issue arises, the proper action for the trial judge to take is to conditionally admit the evidence and instruct the jurors that if they agree with the proponent, they may consider the evidence, giving it the weight they think it deserves. If they side with the opponent, however, they should not consider the evidence. When there is plausible evidence of both authenticity and inauthenticity, the trial judge should *not* exclude the evidence. *State v. Eleck*[179] illustrates the frequent misunderstanding of this confusing rule.

In *Eleck*, the defendant offered into evidence printed Facebook messages between the defendant and a State witness.[180] The proponent testified he had downloaded and printed the exhibit.[181] The messages in question came from an account owned by the State witness based on the facts that the defendant "recognized the user name . . . as belonging to [the State witness]," the account "contained photographs and other entries identifying [the State witness] as the holder of that account," and the account owner "removed [the defendant] from her list of Facebook

---

[179] 23 A.3d 818 (Conn. App. Ct. 2011).

[180] *Eleck*, 23 A.3d at 820.

[181] *Id.* at 821.

'friends'" after she testified that she had not communicated with him.[182] The opponent provided the State witness's testimony that her account was hacked, and she was unable to access her account for some time.[183] The case presents an instance where there was plausible evidence supporting either authentication or a failure to authenticate.[184] Thus, the evidence should have been admitted conditionally for the jury to determine its relevance.[185] The court excluded it, however, reasoning that the defendant failed to provide enough circumstantial evidence of who sent the Facebook messages to overcome the possibility that they "could be generated by someone other than the named sender."[186] This was not warranted given the state of the evidence at trial.

A trial judge should admit the evidence if there is plausible evidence of authenticity produced by the proponent of the evidence and only speculation or conjecture—not facts—by the opponent of the evidence about how, or by whom, it "might" have been created. Too many courts that considered admissibility of social media evidence completely overlooked this important distinction and, in doing so, made questionable rulings excluding evidence that should be admitted. A concrete understanding of Federal Rules of Evidence 104(a) and (b) is necessary to help in the determination of whether social media evidence is admissible and to avoid the unwarranted rulings discussed above.

Rules 104(a) and (b) state, in relevant part:

> (a) In General. The court must decide any preliminary question about whether a witness is qualified, a privilege exists, or evidence is admissible. In so deciding, the court is not bound by evidence rules, except those on privilege.
>
> (b) Relevance That Depends on a Fact. When the relevance of evidence depends on whether a fact exists, proof must be introduced sufficient to support a finding that the fact does exist. The court may admit the proposed evidence on the condition that the proof be introduced later.[187]

---

[182] *Id.* at 820-21.

[183] *Id.* at 820.

[184] *See id.* at 820-21.

[185] *See* FED. R. EVID. 104(b).

[186] *Eleck*, 23 A.3d at 822, 824.

[187] FED. R. EVID. 104(a)-(b).

The authenticity of evidence, including social media evidence, is governed by Rule 901 and "viewed as a subset of relevancy, because 'evidence cannot have a tendency to make the existence of a disputed fact more or less likely if the evidence is not that which its proponent claims.'"[188] When the trial judge is confronted by plausible evidence of both authenticity and inauthenticity, authenticating and admitting social media evidence or electronic evidence generally "calls for a factual determination by the jury."[189] Rule 104(b) governs, and the court must engage in a two-step process.[190] First, the "'[trial] court must determine whether its proponent has offered a satisfactory foundation from which the jury could reasonably find that the evidence is authentic.'"[191] If the judge finds that the evidence is clearly authentic, or clearly inauthentic, and determines that a reasonable jury could not find to the contrary, "the judge withdraws the matter from [the jury's] consideration."[192] However, "[i]f after all the evidence on the issue is in, pro and con, the jury could reasonably conclude that fulfillment of the condition is not established, the issue is for them."[193] That is, if the judge determines that a jury could reasonably find the evidence to be authentic, the evidence goes to the jury to "'ultimately resolve[] whether evidence admitted . . . is that which the proponent claims.'"[194]

Under Rule 104(a), the judge makes a preliminary determination of the admissibility of conditionally relevant evidence based on whether a reasonable fact finder could find the evidence to be what it purports to be by a preponderance of the evidence.[195] This standard applies in civil

---

[188] Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 539 (D. Md. 2007) (quoting United States v. Branch, 970 F.2d 1368, 1370 (4th Cir. 1992)).

[189] *Id.*

[190] *See id.* at 539-40; *see also* FED. R. EVID. 901 advisory committee's note to subdivision (a). ("Authentication and identification represent a special aspect of relevancy. . . . This requirement of showing authenticity or identity 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).").

[191] *Lorraine*, 241 F.R.D. at 539 (quoting *Branch*, 970 F.2d at 1370).

[192] FED. R. EVID. 104 advisory committee's note to subdivision (b).

[193] *Id.*

[194] *Lorraine*, 241 F.R.D. at 539-40 (quoting *Branch*, 970 F.2d at 1370-71).

[195] 1 STEPHEN A. SALTZBURG ET AL., FEDERAL RULES OF EVIDENCE MANUAL § 104.02[9] (8th ed. 2002) ("[T]he Supreme Court has, in several cases, held that the

and criminal cases alike.[196] In *Bourjaily v. United States*,[197] the Supreme Court "implied that the preponderance standard should be the governing standard for all preliminary questions decided under Rule 104(a),"[198] and in *Daubert v. Merrell Dow Pharmaceuticals*,[199] the Supreme Court "relied on Rule 104 and *Bourjaily*" to hold that "the proponent of expert testimony has the burden of establishing its reliability under Rule 702 by a preponderance of the evidence."[200] Additionally, "[l]ower [c]ourts have applied the preponderance standard to an array of competency questions."[201] Importantly, the Advisory Committee Notes state that "the preponderance standard applies to the Court's rulings under Rule 104(a)."[202]

A litigant may authenticate social media evidence or electronically stored information (ESI) by use of Rules 901 and 902. The *Lorraine* court observed that Rule 901(b) provides a nonexclusive list of methods of authenticating ESI and that courts have recognized five of the methods listed in Rule 901(b) as being particularly appropriate for authenticating digital evidence.[203] While many of the cases involve digital evidence from Internet sites other than social media sites, the methods approved by those cases apply with equal force to social media evidence.[204]

---

moving party has the burden of proving admissibility requirements under Rule 104(a) by a preponderance of the evidence. Where the objection goes to conditional relevance, the proponent must show that a reasonable juror could believe the preliminary fact by a preponderance of the evidence.").

[196] 1 MICHAEL H. GRAHAM, HANDBOOK OF FEDERAL EVIDENCE § 104.1 (6th ed. 2006) (citing Bourjaily v. United States, 483 U.S. 171, 173-77 (1987)) ("In reaching a determination pursuant to Rule 104(a) on a question of admissibility for the court alone whether that be in a criminal or a civil case, the court should apply the standard for the burden of persuasion applicable generally in civil cases of more probably true than not true.").

[197] 483 U.S. 171 (1987).

[198] SALTZBURG ET AL., *supra* note 195 (citing *Bourjaily*, 483 U.S. at 175).

[199] 509 U.S. 579 (1993).

[200] SALTZBURG ET AL., *supra* note 195 (citing *Daubert*, 509 U.S. 579).

[201] *Id.*

[202] *Id.*; *see also* FED. R. EVID. 702 advisory committee's note to 2000 amendments.

[203] Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 544-49 (D. Md. 2007).

[204] *See id.* at 554-59 (discussing the authentication of e-mail, internet website postings, chat room content, and computer records and data evidence).

Pursuant to 901(b)(1), courts have assessed the authenticity of ESI using the testimony of a witness with "personal knowledge of how that type of exhibit is routinely made"[205] who provides "factual specificity" about how the ESI "is created, acquired, maintained, and preserved without alteration or change" or about how it is produced via "a system or process that does so."[206] Under Rule 901(b)(1), it is not sufficient for a witness to provide "boilerplate, conclusory statements that simply parrot the elements of the business record exception to the hearsay rule . . . or public record exception."[207] Courts have approved the comparison of ESI known to be authentic with ESI of questionable authenticity pursuant to Rule 901(b)(3), and they have considered circumstances and distinctive characteristics of the ESI—for example, hash values and metadata—pursuant to Rule 901(b)(4).[208] Additionally, pursuant to 901(b)(7), courts have determined the authenticity of ESI that comes from public records based on whether the proponent has made a showing that "'the office from which the records were taken is the legal custodian of the records.'"[209] Finally, pursuant to Rule 901(b)(9), courts have accepted "proof that [the records] were produced by a system or process capable of producing a reliable result" to determine the authenticity of ESI.[210]

The *Lorraine* court further noted that Rule 902 provides for self-authentication (sometimes with an accompanying certificate signed by a custodian) of certain enumerated documents such as, *inter alia*, public documents, official publications, trade inscriptions, and certified domestic records of regularly conducted activity.[211] An example of self-authentication under Rule 902[212] is *U.S. Equal Employment Opportunity Commis-*

---

[205] *Id.* at 545 (citing 5 JACK B. WEINSTEIN & MARGARET A. BERGER, WEINSTEIN'S FEDERAL EVIDENCE § 901.03[2] (Joseph M. McLaughlin ed., 2d ed. 1997)).

[206] *Id.*

[207] *Id.* at 545-46.

[208] *See id.* at 546-48.

[209] *Id.* at 548 (quoting 5 JACK B. WEINSTEIN & MARGARET A. BERGER, WEINSTEIN'S FEDERAL EVIDENCE § 901.10[2] (Joseph M. McLaughlin ed., 2d ed. 1997)).

[210] *Id.*

[211] *Id.* at 549-51.

[212] *See* FED. R. EVID. 902(5).

sion v. E.I. DuPont de Nemours & Co.,[213] where the court concluded that "a printout of a table from the website of the United States Census Bureau," which "contain[ed] the internet domain address from which the table was printed, and the date on which it was printed," was admissible because it was self-authenticating.[214] However, the *Lorraine* court cautioned that the opposing party still may challenge the authenticity of the document—in which case the "exhibit and the evidence challenging its authenticity goes to the jury, which ultimately determines whether it is authentic."[215] Judicial notice under Rule 201 also could be useful in authenticating ESI.[216]

With regard to website postings specifically, the *Lorraine* court noted that one concern is whether "the organization hosting the website actually posted the statements or authorized their posting."[217] It said that, "'[i]n applying [the authentication standard] to website evidence, there are three questions that must be answered, explicitly or implicitly: (1) What was actually on the website? (2) Does the exhibit or testimony accurately reflect it? (3) If so, is it attributable to the owner of the site?'"[218] Other

---

[213] No. Civ.A. 03-1605, 2004 WL 2347559 (E.D. La. Oct. 18, 2004) (order denying motion in limine to exclude website printout exhibit).

[214] *E.I. DuPont*, 2004 WL 2347559, at *1-2; *see also* Williams v. Long, 585 F. Supp. 2d 679, 688 n.4, 689 (D. Md. 2008) (noting that information posted on the Internet "by a qualifying public authority" is a publication for purposes of Rule 902(5), such that it is self-authenticating, and "[a] proponent of ESI could use the URL, date, and/or official title on a printed webpage to show that the information was from a public authority's website, and therefore, self-authenticating"; concluding that "[t]he printed webpage from the Maryland Judiciary Case Search website is self-authenticating under Rule 902(5)" because it is a government publication, the page refers to the "Maryland Judiciary" and the "District Court of Maryland," and "the URL on the top of the printed webpage identifies that the results are in fact from the website"; also concluding that "[t]he printed webpage from the Employment Standards Service website could also be considered a self-authenticating 'official publication,'" because it is "hosted by a subdivision of a state agency . . . [,] the URL on the webpage identifies the correct website, and the agency's name is printed preceding the search results").

[215] *Lorraine*, 241 F.R.D. at 551 (citing FED. R. EVID. 902 advisory committee's notes).

[216] *Id.* at 553.

[217] *Id.* at 555.

[218] *Id.* (alterations in original) (quoting Gregory P. Joseph, *Internet and Email Evidence*, 13 PRAC. LITIGATOR 45, Mar. 2002, *reprinted in* 5 STEPHEN A. SALTZBURG ET AL., FEDERAL RULES OF EVIDENCE MANUAL, pt. 4, at 21 (9th ed. 2006)).

factors relevant to the admissibility of website postings as evidence, and which counsel should consider when deciding how to build a foundation and authenticate the evidence, include

> [t]he length of time the data was posted on the site; whether others report having seen it; whether it remains on the website for the court to verify; whether the data is of a type ordinarily posted on that website or websites of similar entities (e.g. financial information from corporations); whether the owner of the site has elsewhere published the same data, in whole or in part; whether others have published the same data, in whole or in part; whether the data has been republished by others who identify the source of the data as the website in question?[219]

The *Lorraine* court further stated that the "authentication rules most likely to apply, singly or in combination," to website postings are the five that courts have applied to ESI—Rules 901(b)(1) (testimony of a witness with personal knowledge), 901(b)(3) (comparison with an authenticated document), 901(b)(4) (distinctive characteristics), 901(b)(7) (evidence about public records), and 901(b)(9) (evidence about a process or system) —as well as Rule 902(5) (official publications).[220]

Additionally, courts have relied on Rule 901(b) specifically for determining the admissibility of evidence from the Internet, which is equally applicable to authenticating social media evidence. In *Telewizja Polska USA, Inc. v. Echostar Satellite Corp.*,[221] the defendant offered printouts from the plaintiff's website as it appeared years earlier.[222] To authenticate the printouts, the defendant offered an affidavit from the administrative director for the Internet Archive Company, the company that retrieved the historic website images,[223] "verifying that the Internet

---

[219] *Id.* at 555-56 (quoting Gregory P. Joseph, *Internet and Email Evidence*, 13 PRAC. LITIGATOR 45, Mar. 2002, *reprinted in* 5 STEPHEN A. SALTZBURG ET AL., FEDERAL RULES OF EVIDENCE MANUAL, pt. 4, at 22 (9th ed. 2006)).

[220] *Id.* at 556; *see* FED. R. EVID. 901(b); FED. R. EVID. 902(5).

[221] No. 02 C 3293, 2004 WL 2367740 (N.D. Ill. Oct. 15, 2004) (order ruling on plaintiff's seventeen motions in limine and defendant's thirty-eight motions in limine).

[222] *Telewizja Polska*, 2004 WL 2367740, at *5.

[223] St. Luke's Cataract & Laser Inst. v. Sanderson, No 8:06-CV-223-T-MSS, 2006 WL 1320242, at *1 (M.D. Fla. May 12, 2006) (order denying plaintiff's motion to admit Internet Archive website printouts) (discussing *Telewizja* at length); *Telewizja Polska*, 2004 WL 2367740, at *6.

Archive Company retrieved copies of the website as it appeared on the dates in question from its electronic archives."[224] The plaintiff objected to the evidence as not properly authenticated.[225] The court rejected that argument, reasoning,

> Federal Rule of Evidence 901 "requires only a prima facie showing of genuineness and *leaves it to the jury to decide the true authenticity and probative value of the evidence*." Admittedly, the Internet Archive does not fit neatly into any of the non-exhaustive examples listed in Rule 901; the Internet Archive is a relatively new source for archiving websites. Nevertheless, Plaintiff has presented no evidence that the Internet Archive is unreliable or biased. And Plaintiff has neither denied that the exhibit represents the contents of its website on the dates in question, nor come forward with its own evidence challenging the veracity of the exhibit.[226]

On that basis, the court concluded that the affidavit was "sufficient to satisfy Rule 901's threshold requirement for admissibility."[227]

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 (even if not from a live witness)—including documents, whether electronic or hard copy—on a continuum. That is, clearly authentic evidence is admitted, clearly inauthentic evidence is excluded, and everything in between is conditionally relevant and admitted for the jury to make the final determination as to authenticity. Given the state of the case law as it currently exists regarding the authentication of social media evidence and the certainty that this type of evidence will continue to be offered in civil and criminal cases throughout the country in state and federal court, it is helpful to distill some rules of reason. Such rules will hopefully facilitate lawyers

---

[224] *Telewizja Polska*, 2004 WL 2367740, at *6.

[225] *Id.*

[226] *Id.* (emphasis added) (citation omitted) (quoting United States v. Harvey, 117 F.3d 1044, 1049 (7th Cir. 1997)).

[227] *Id.*; *see also* Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1153-54 (C.D. Cal. 2002) (order granting plaintiff's motion for preliminary injunction) (admitting internet images over defendant's objection because the accompanying affidavit from the individual responsible for printing the internet images, "in combination with circumstantial indicia of authenticity (such as the dates and web addresses), *would support a reasonable juror in the belief* that the documents are what Perfect 10 says they are" (emphasis added)).

and judges in reaching principled and predictable decisions regarding how social media evidence should be authenticated. It serves no interest for the law to remain in its current inconsistent and unpredictable state. 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.

III. Checklist for Authentication

The following rules of reason should help practitioners better prepare to introduce social media evidence successfully at trial.

A. Mind Your Ps

There is an old saying that "Prior Preparation Prevents Poor Performance." Most unsuccessful attempts to authenticate social media or other digital evidence result from self-inflicted injuries caused by the failure to plan in advance of trial. In civil cases, the time to plan for introduction of social media evidence is during discovery when, for example, there is time to ask witnesses questions during a deposition that will establish the methods of authentication identified in Rules 901(b) and 902. In criminal cases, where there is far less discovery, plan how you will authenticate the evidence as soon as you first obtain it. Prior planning will alert you to when you need to call a live witness to authenticate social media evidence and will permit you time to issue a subpoena to get the needed witness to trial or, in a civil case, to take their deposition so that if they are unavailable for trial, their testimony is admissible under Rule 804(b)(1) as prior testimony of an unavailable declarant.

B. Do Your Homework

As previously discussed, courts have reached widely divergent and inconsistent rulings regarding the admissibility of social media evidence. Expect this to continue until a national consensus has developed. In the meantime, be prepared by researching whether the judge or court presiding over your case has issued any opinions regarding the admissibility of social media evidence. Adapt your approach to authentication in light of any prior rulings. If you are urging the court to change its prior

views, you should file a motion in limine well before trial to try to get an advance ruling. If the court does not agree with your approach, you have time to choose a method you are confident the court will accept.

C. Sometimes (But Not Often) It Helps to Be Lazy

Never rule out the possibility that your adversaries will stipulate to the authenticity of social media evidence you want to introduce, and do not be afraid to ask. If they agree, get it in writing. Often they will agree because they want stipulations from you as well. If they will not stipulate, you then have advance notice that you will get an objection and should prepare accordingly. Similarly, in civil cases, if you gained access to the social media evidence from your adversary in response to a document production request, most courts then recognize that there is a presumption of authenticity that applies to evidence obtained in discovery from an adversary.[228] Also, in civil cases, do not overlook Federal Rule of Civil Procedure 36,[229] which governs requests for admission of genuineness and authenticity of documents. Recall that if you file a request for admission, and your opponent fails to deny within thirty days, the requests are conclusively admitted for purposes of your litigation.[230] Rule 36 requests are woefully underused and perfect to authenticate evidence.

D. Remember the Interplay Between Rules 104(a) and (b) and "Conditional Relevance"

Before any trial where you plan to introduce social media evidence, re-read Rule 104(a) and (b).[231] If you are aware of any facts that your

---

[228] Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 552 (D. Md. 2007) (citing Indianapolis Minority Contractors Ass'n v. Wiley, No. IP 94-1175-C-T/G, 1998 WL 19888026, at *6 (S.D. Ind. May 13, 1998) ("The act of production is an implicit authentication of documents produced.")).

[229] *See* FED. R. CIV. P. 36.

[230] *See* FED. R. CIV. P. 36(a)(3) ("A matter is admitted unless, within 30 days after being served, the party to whom the request is directed serves on the requesting party a written answer or objection addressed to the matter and signed by the party or its attorney.").

[231] *See* FED. R. EVID. 104.

adversary will attempt to prove to rebut the evidence you intend to offer to authenticate your social media evidence, carefully consider whether you can argue that it is insufficient to convince a reasonable jury that your evidence is not authentic. If you conclude that the judge is likely to find that the evidence would be sufficient to persuade a reasonable jury that your evidence is not authentic, be prepared to argue that the evidence supporting authenticity is sufficient to persuade a reasonable juror that it is authentic. In this scenario, the judge must admit the exhibit conditionally and instruct the jurors that if they accept your version of the facts, they may consider the evidence and give it the weight that it deserves; if not, they must not consider it. Remember that the judge may not be familiar with the interplay between Rule 104(a) and (b). Consider gathering research to cite to support your argument that, if your opponent offers evidence of inauthenticity, the jury needs to resolve the conflict, and exclusion of the social media evidence by the judge is improper. If the judge rules against you, make sure to make an appropriate proffer pursuant to Rule 103 to preserve the issue for appellate review.[232]

E. Choose Wisely

As far in advance of trial as possible, and for each distinct type of social media evidence you intend to introduce, carefully plan the method you want to use to authenticate each exhibit. If possible, be prepared to authenticate more than one way. To pick the best way, review the methods listed in Rule 901(b).[233] Of them, the most helpful for social media evidence are as follows:

1. Rule 901(b)(1)—Someone with Personal Knowledge

This rule allows a witness with personal knowledge to authenticate evidence.[234] If you are introducing a screen shot from a Facebook page, call as a witness the person who created and maintains the page, and ask the witness if she made or authorized the posting. In a civil case, you can establish this foundation by deposing the owner.

---

[232] *See* FED. R. EVID. 103.

[233] *See* FED. R. EVID. 901(b).

[234] *See* FED. R. EVID. 901(b)(1).

2. Rule 901(b)(3)—Use of an Expert or Comparison by the Fact Finder

A computer forensic expert can frequently authenticate the maker of social media content.[235] Obviously, you will need to retain the proper expert and ensure that he or she has enough time and information to make the identification. Advance planning is essential, and be mindful of the potentially substantial cost. If the social media evidence is critical to the success of your case, however, the cost is worth it. Less elegantly, Rule 901(b)(3) also allows the fact finder (usually the jury) to authenticate social media evidence when shown an example of a posting that is known to have been made by the person that you contend authored the posting by comparing it to a posting of unknown authenticity.[236] While this method is allowed by the rule, it is risky to use because you never know how the jurors will respond, and you will not be able to obtain any feedback from them as to how they came out on the issue until you receive a final verdict and attempt to figure out whether they saw things the way you wanted.

3. Rule 901(b)(4)—Distinctive Circumstances or Characteristics

This is one of the most successful methods used to authenticate all evidence, including social media evidence.[237] Recall the old saying, "If it looks like a duck, waddles like a duck, and quacks like a duck, it must be a duck." Make an inventory of all of the circumstances and characteristics that apply to the social media exhibit that add up to a showing that, more likely than not, it was authored by the person that you contend authored it. Consider the content, whether the post replied to an earlier

---

[235] *See* FED. R. EVID. 901(b)(3) (allowing an expert witness to compare an "authenticated specimen" to the offered evidence).

[236] *See id.* (allowing the trier of fact to compare an "authenticated specimen" to the offered evidence).

[237] *See generally* FED. R. EVID. 901(b)(4) (allowing the "[t]he appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances" to support the assertion that offered evidence is what it is proclaimed to be).

inquiry or posting, any distinguishing language, abbreviations, slang, punctuation, use of emoticons,[238] nicknames, content that was uniquely known by the person you claim is the author, Internet address, date, and any other factors that are unique to the person that you claim authored it. If you use this approach, make sure you do research to find any cases from the court that will try the case (or the appropriate appellate court having jurisdiction over that court) that discuss what is or is not sufficient similarity or circumstances to permit authentication by this method. Adjust your approach accordingly.

4. Rule 901(b)(9)—System or Process Producing Reliable Results

This is one of the most useful ways to authenticate social media evidence,[239] but it requires a witness who has personal knowledge under Rule 602[240] to explain how the social media evidence was created or, alternatively, is an expert qualified under Rule 702[241] who can provide opinion testimony. Plan in advance by making sure that the witness is available to testify at trial or is deposed pre-trial in civil cases. If the witness is unavailable at trial, the deposition will be admissible under Rule 804(b)(1).[242]

5. Rule 902(5)—Official Publications

Although not likely to be a useful method to authenticate social media evidence such as a nongovernmental social media website like Facebook or Myspace, it is possible that this authentication method could be used

---

[238] An emoticon is "a group of keyboard characters . . . that typically represents a facial expression or suggests an attitude or emotion and that is used especially in computerized communications." Definition of *Emoticon*, MERRIAM-WEBSTER, http://www.merriam-webster.com/dictionary/emoticon (last visited June 2, 2013). For example, using a colon and parenthesis :) will convert to a smiley face ☺ emoticon.

[239] *See generally* FED. R. EVID. 901(b)(9) (allowing offered evidence that was produced by a process or system to be authenticated by evidence "describing [the] process or system and showing that it produces an accurate result").

[240] *See* FED. R. EVID. 602.

[241] *See* FED. R. EVID. 702.

[242] *See* FED. R. EVID. 804(b)(1).

if there is an interactive website sponsored by a government agency.[243] For example, in *Williams v. Long*,[244] the plaintiffs attempted to conditionally certify a collective action under the Fair Labor Standards Act and submitted as evidence printed webpages from the website of the Employment Standards Service of the Division of Labor and Industry in the Maryland Department of Labor, Licensing and Regulation.[245] If found to be "authentic and considered for their substantive truth," these printouts suggested that "there [were] other claimants who might desire to join the [p]laintiffs' suit."[246] The court addressed the applicability of Rule 902(5) to website postings specifically, stating that "[a] proponent of ESI could use the URL, date, and/or official title on a printed webpage to show that the information was from a public authority's website, and therefore, self-authenticating."[247] Holding that the webpage printouts were a self-authenticating "official publication" under Rule 902(5), the court recognized that the "public authority's selection of the posted information for publication on its website will act as the necessary 'seal of approval.'"[248] Keep in mind that the United States Government is considering use of social media sources to better communicate with the public. If so, state and local governments will likely follow, if they are not already.[249]

6. Rule 902(6)—Newspapers and Periodicals

Although traditionally used to authenticate hard copies of newspapers or magazines, because of the distinctive features of most newspaper

---

[243] *See* FED. R. EVID. 902(5) (stating that official publications by public authorities are self-authenticating).

[244] 585 F. Supp. 2d 679 (D. Md. 2008).

[245] *Long*, 585 F. Supp. 2d at 681-82.

[246] *Id.* at 685 (citing Pls.' Exs. 1, 3).

[247] *Id.* at 689.

[248] *Id.*

[249] *See* Presidential Memorandum—Building a 21st Century Digital Government, 77 Fed. Reg. 32391, 32391 (The White House, Office of Press Sec'y, May 23, 2012), *available at* http://www.whitehouse.gov/the-press-office/2012/05/23/presidential-memorandum-building-21st-century-digital-government (directing government agencies to "use emerging technologies to serve the public as effectively as possible").

mastheads and magazine covers, traditional news media sources are increasingly going digital. Many programs and reporters have Twitter sites. If the social media evidence includes a newspaper or periodical-sponsored Twitter posting, consider Rule 902(6).[250] If accepted by the court, this rule allows the newspaper or periodical posting to be self-authenticated, eliminating the need for a sponsoring witness.[251]

Conclusion

Given the ubiquitous use of digital devices to communicate on social media sites, there is little chance that such evidence will cease to be highly relevant in either criminal or civil cases. This is particularly so whenever motive, state of mind, intent, interpersonal interactions, physical health, and conduct occurring outside of public observation are at issue. 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. Nowhere is this uncertain state more evident than in the near total absence in any of the reported cases of any recognition or application of the two evidence rules most important to making the correct ruling—Rules 104(a) and (b).

Hopefully, this Article can shed some light on the nature of the confusion and offer useful suggestions on how to approach the authentication of social media evidence. It is a near certainty that the public appetite for use of social media sites is unlikely to abate, and it is essential for courts and lawyers to do a better job in offering and admitting this evidence. We hope that reading this Article will be their first step toward this goal.

---

[250] *See* FED. R. EVID. 902(6) ("Printed material purporting to be a newspaper or periodical" is self-authenticating.).

[251] *Id.*