Volume 61 | Issue 2 Article 3

6-1-2016

#Guilty? Sublet v. State and the Authentication of Social Media Evidence in Criminal Proceedings

Elizabeth A. Flanagan

#GUILTY? *SUBLET v. STATE* AND THE AUTHENTICATION OF SOCIAL MEDIA EVIDENCE IN CRIMINAL PROCEEDINGS

ELIZABETH A. FLANAGAN*

"[W]ith social networks and other tools on the Internet, all of these 500 million people have a way to say what they're thinking and have their voice be heard."[1]

I. THE COURTROOM MEETS THE CHAT ROOM: AN INTRODUCTION TO THE USE OF SOCIAL MEDIA IN LITIGATION

The above quotation, from Facebook founder and CEO, Mark Zuckerberg, reflects the dynamic nature of social media in today's society: over half a billion people worldwide can express themselves to a potentially unlimited audience through social media networks.[2] This quote also demonstrates an undisputed fact: social media is everywhere.[3] In fact, the Pew Internet Project calculated that, as of January 2014, 74% of online adults have used a social networking site.[4] An estimated 71% of online American adults use Facebook, making it the most popular social media site in the

* J.D. Candidate, 2017, Villanova University Charles Widger School of Law; M.S.W. 2014, University of Pennsylvania; B.A. 2010, University of Pennsylvania. This Note is dedicated to my family and friends who have supported me in everything I have done throughout my life. I would like to thank all those who provided feedback and input in writing this Note, especially the staff of the *Villanova Law Review*. I would particularly like to thank Matt Kaiser, Kristen Ashe, and Carina Meleca for their thoughtful edits and valuable advice throughout this entire process.

1. Ki Mae Heussner, *Facebook CEO Mark Zuckerberg Talks to Diane Sawyer as Website Gets 500-Millionth Member*, ABC NEWS (July 21, 2010), http://abcnews.go.com/WN/zuckerberg-calls-movie-fiction-disputes-signing-contract-giving/story?id=11217015 [https://perma.cc/23UX-L2BQ] (quoting Mark Zuckerberg and discussing social media's broad reach) (internal quotation marks omitted).

2. *See id.* (identifying number of Facebook users worldwide); *see also* Andrew B. Delaney & Darren A. Heitner, *Made for Each Other Social Media and Litigation*, N.Y. ST. B.J., Feb. 2013, at 10, 11–12 (providing social media statistics as of time of publication). Delaney and Heitner state that the most popular social networking site, Facebook, has over one billion users, half of whom will log in on any given day. *See id.* at 11 (discussing users' Facebook activity worldwide).

3. *See* Delaney & Heitner, *supra* note 2, at 11 (explaining prevalence of social media in society). Delaney and Heitner note that almost half of Americans use some sort of social media, and these numbers are quickly rising. *See id.* (describing popularity of social media among Americans).

4. *See Social Networking Fact Sheet*, PEW RES. CTR., www.pewinternet.org/fact-sheets/social-networking-fact-sheet [https://perma.cc/8NTM-YANK] (last updated Sept. 2014) (providing statistics regarding social media usage worldwide). The Pew Research Center "conducts public opinion polling, demographic research, media content analysis, and other empirical social science research." *See id.* (describing purpose).

United States.[5] Additionally, over 23% of online adults in the United States use at least one of the other three most popular social media sites: Twitter, LinkedIn, and Instagram.[6] With the ever-increasing ease of access to social media, users are able to instantly share personal information with a potentially limitless audience at the tap of a button.[7]

As social media has become more ubiquitous, its use in litigation has become a topic of great debate.[8] One particular issue in this debate is how social media evidence can be authenticated.[9] Courts in multiple juris-

5. *See id.* (discussing Facebook usage and popularity in United States); *see also* Zoe Rosenthal, Note, *"Sharing" with the Court: The Discoverability of Private Social Media Accounts in Civil Litigation*, 25 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 227, 229 (2014) (commenting on rapid growth in Facebook usage since creation in 2004). Rosenthal notes that, as of the time of her writing, Facebook comprised one in every five Internet page views in the United States. *See id.*

6. *See Social Networking Fact Sheet*, *supra* note 4 (discussing Americans' usage of various social networking sites). According to this study, 23% of online adults in the United States use Twitter, 26% use Instagram, and 28% use LinkedIn. *See id.*

7. *See* Breanne M. Democko, Comment, *Social Media and the Rules on Authentication*, 43 U. TOL. L. REV. 367, 376 (2012) (noting social networking sites, specifically Facebook, have added "functions and applications [ ] allow[ing] users to communicate in" variety of different ways). Democko notes here that social media surpassed e-mail in 2009 as the preferred form of electronic communication worldwide. *See id.* at 367 (illustrating popularity of social media as new way of communicating with others). Further, social media users access their accounts not only through their computers but also through their cell phones, creating an unprecedented ease of access to social media accounts. *See id.* (describing ways in which many individuals access their social media accounts).

8. *See generally* Delaney & Heitner, *supra* note 2 (relating social media to existing rules of evidence); Democko, *supra* note 7 (discussing developments in social media and its use in litigation). Courts have "consistently rejected" litigants' arguments that social media content is protected under a "user's right to privacy" because the user is sharing the content with others, even if they are only part of a select group of "friends." *See* Margaret DiBianca, *Managing Clients' Social-Media Evidence*, DEL. LAW., Fall 2014, at 26, 27 (describing current debate regarding social media content and privacy).

9. *See* Democko, *supra* note 7, at 388–89 (discussing courts' varying responses to social media evidence). Democko notes that, when courts "face[ ] issues of authentication, some courts appear uncomfortable and highly skeptical" because of the ease with which social media could be tampered with, while other courts readily equate "social networking sites to other forms of Internet-based communications[,]" which allows these courts to rely on more established precedent in their decisions. *See id.* (describing legal ambiguity courts face when addressing authentication of social media); *see also, e.g.*, Parker v. State, 85 A.3d 682, 683 (Del. 2014) (discussing standard of authentication required for social media evidence); Fawcett v. Altieri, 960 N.Y.S.2d 592, 595 (Sup. Ct. 2013) (describing two-prong analysis required to compel discovery of social media accounts).

In *Parker*, the Delaware Supreme Court held that authentication of social media evidence could be accomplished if the proponent presented sufficient evidence that a reasonable juror could find that the post was what the proponent claimed it to be. *See Parker*, 85 A.3d at 687–88 (detailing standard for trial judge to apply when litigant "seeks to introduce social media evidence" and has offered evidence to authenticate it).

In *Fawcett*, a New York Supreme Court described a two-pronged analysis for determining whether a social media post was discoverable: first, whether the con-

dictions have recently begun to address the evidentiary requirements for social media, seeking to craft a workable standard for authentication.[10]

In *Sublet v. State*,[11] the Maryland Court of Appeals decided three consolidated cases addressing the authentication of messages and posts made via Facebook and Twitter and developed a vague outline of the ways in which a party can authenticate social media evidence.[12] The court relied on Maryland Rule 5-901, which is based on Rule 901(a) of the Federal Rules of Evidence.[13] Under the federal rule, in order to authenticate an

---

tent was "material and necessary" to the litigation and second, whether compelling production would violate the privacy rights of the account holder. *See Fawcett*, 960 N.Y.S.2d at 595 (internal quotation marks omitted) (describing test after "survey[ing] [ ] cases dealing with the production of social media accounts[ ] in both the criminal and civil contexts"). For a detailed discussion of *Fawcett* and *Parker*, see *infra* notes 28 and 49, respectively.

10. *See, e.g.*, State v. Eleck, 23 A.3d 818, 822 (Conn. App. Ct.) (describing methods for social media authentication), *cert. granted mem. in part by* 30 A.3d 2 (Conn. 2011), *and aff'd on other grounds by* 100 A.3d 817 (Conn. 2014); *Parker*, 85 A.2d at 683 (discussing various approaches to social media authentication); Griffin v. State, 19 A.3d 415, 424 (Md. 2011) (suggesting greater scrutiny may be required for social media authentication "because of the heightened possibility for manipulation by other than the true user or poster"). For further discussion of *Griffin*, *Eleck*, and *Parker*, see *infra* notes 33–38 and accompanying text, note 60, and note 49, respectively.

Because of concerns that social media evidence could have been tampered with by another party and because of courts' general unfamiliarity with social media, "some courts [ ] apply an extraneously high standard of authentication," which may lead to the inevitable exclusion of crucial evidence. *See* Democko, *supra* note 7, at 369 ("Since social media has become the preferred method of communication, applying such a high standard to authenticate electronic evidence would inevitably exclude a mass quantity of crucial evidence."). For a further discussion, see Josh Gilliland, *The Admissibility of Social Media Evidence*, ABA, http://apps.americanbar.org/litigation/litigationnews/trial_skills/030413-tips-admissibility-ESI.html [https://perma.cc/8FJ4-KRSG] (last visited Mar. 28, 2016) ("The Rules of Evidence do not update like an app whenever a new smartphone or electronic device is released. For that reason, courts apply the evidence rules similarly to all evidence, including social media."); Steven Goode, *The Admissibility of Electronic Evidence*, 29 REV. LITIG. 1 (2009) (discussing application of authentication rules to social media evidence); Elana Harris, *Authenticating Social Media Evidence (Part II of V): Federal Rules of Evidence 901(b)(1)*, PAGEVAULT (Sept. 14, 2015), https://www.page-vault.com/authenticate-webpage-2/ [https://perma.cc/YW2M-WE6B] (suggesting three questions to consider in attempting to authenticate social media evidence: "1. When, where and how was the evidence collected? . . . 2. Who collected the evidence? . . . 3. How was the evidence preserved?"); David I. Schoen, *The Authentication of Social Media Postings*, ABA (May 17, 2011), https://apps.americanbar.org/litigation/committees/trialevidence/articles/051711-authentication-social-media.html [https://perma.cc/V25B-LSG3] (discussing evidentiary implications of increased prevalence of social media in litigation).

11. 113 A.3d 695 (Md. 2015).

12. *See id.* at 698 (utilizing reasonable juror standard for authentication of social media evidence). *See infra* notes 70–105 and accompanying text for facts and reasoning of *Sublet*.

13. *See id.* at 697–98 (discussing relevant Maryland rule and application to case at issue). MARYLAND RULE 5-901(a) reads, "The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evi-

item of evidence, "the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is."[14] In each of the three cases decided by the *Sublet* court, the court relied on a variety of circumstantial evidence in authenticating the social media evidence at issue.[15]

This Note discusses the vague standard outlined in *Sublet* and points to a need for further clarification of authentication standards for social media posts.[16] Part II provides background information regarding the use of social media in litigation.[17] Part III discusses the facts and holding of *Sublet*.[18] Part IV analyzes the *Sublet* majority's decision-making process as well as the dissent's critique of it.[19] Part V provides a critical analysis of the court's reasoning in *Sublet*.[20] Finally, Part VI highlights the impact of *Sublet* and recommends a clearer standard for authentication that effectively balances the value of social media evidence against the myriad concerns regarding authorship.[21]

II. EVIDENCE GOES VIRAL: SOCIAL MEDIA'S EXPANDED USE IN LITIGATION BEFORE *SUBLET*

In 2009, social media surpassed e-mail as the preferred use of online communication worldwide.[22] As of 2013, an estimated 500,000 people logged into Facebook, the most popular social media site, every day.[23] With social media's increased prevalence, litigants increasingly attempt to

dence sufficient to support a finding that the matter in question is what its proponent claims." MD. R. 5-901(a).

14. *See* FED. R. EVID. 901(a) (providing general federal rule of evidence regarding authentication).

15. *See generally Sublet*, 113 A.3d 695 (using circumstantial evidence in each case to determine authenticity of social media evidence). For further discussion of the standards used in *Sublet*, see *infra* notes 106–21 and accompanying text.

16. *See infra* notes 111–18 and accompanying text for a discussion of the *Sublet* court's standard. *See infra* notes 119–25 for a discussion of problems with the court's current standard.

17. For a complete discussion of cases and research relating to the issue addressed in *Sublet*, see *infra* notes 22–69 and accompanying text.

18. For a complete discussion of the facts of the three consolidated cases considered in *Sublet*, see *infra* notes 70–105 and accompanying text.

19. For analysis of the *Sublet* court's reasoning, see *infra* notes 106–21 and accompanying text.

20. For a critical analysis of the issues surrounding social media authentication, see *infra* notes 122–37 and accompanying text.

21. For discussion of the impact of *Sublet* on future litigation, see *infra* notes 138–48 and accompanying text.

22. *See* Democko, *supra* note 7, at 367 (noting worldwide prevalence of social networking and blogging websites).

23. *See* Delaney & Heitner, *supra* note 2, at 11 (discussing rapid growth of social media use). Delaney and Heitner note that almost half of the United States' population used social media in 2013. *See id.* At the time the article was written, "Facebook report[ed] that it ha[d] more than one billion users who log[ged] in at least once per month, half of whom will log in to Facebook any given day." *Id.* (footnote omitted). The authors also discuss LinkedIn and Twitter, noting that

introduce information from these accounts as evidence in both civil and criminal trials.[24] The growing use of social media in litigation has created a broad debate among courts over how best to address issues of discoverability, admissibility, and authentication standards for social media evidence.[25]

A. *Keeping Your Selfies to Yourself: The Debate over Privacy Settings and Discoverability*

Courts consistently allow discovery of social media evidence, even those posts the account holder assumes are protected by privacy settings.[26] Moreover, they regularly hold that discoverability of social media evidence

---

these sites, like Facebook, have reported rapid growth in membership since their creation. *See id.* at 11–12.

24. *See* Delaney & Heitner, *supra* note 2, at 14–15 (discussing benefits and issues social media creates for litigation process); Jonathan D. Frieden & Leigh M. Murray, *The Admissibility of Electronic Evidence Under the Federal Rules of Evidence*, 17 RICH. J.L. & TECH. 5, *1 (discussing importance of proper authentication of social media). Delaney and Heitner note that much of the information that can easily be gathered from social media accounts would have only been available through the use of a private investigator in years past. *See* Delaney & Heitner, *supra* note 2, at 11 (identifying how social media has changed landscape of litigation process). Advances in technology and social media have led to an evolution in the available forms of communication, creating unique challenges for both litigants and judges. *See* Democko, *supra* note 7, at 368 ("Technology continues to rapidly evolve into increasingly complex portals of communication, and courts are left to interpret the evidentiary questions resulting from each advance.").

25. *See also* Parker v. State, 85 A.3d 682, 683 (Del. 2014) (presenting varying approaches to social media authentication). *Compare* Griffin v. State, 19 A.3d 415, 427 (Md. 2011) (suggesting higher standard of authentication required for social media than other evidence because of high potential for fabrication), *with* Tienda v. State, 358 S.W.3d 633, 647 (Tex. Crim. App. 2012) (requiring "sufficient circumstantial evidence to support a finding that the exhibits were what they purported to be"). Some courts disagree as to whether new rules should be adopted for discoverability, admissibility, and authentication. *See, e.g.*, *id.*; *see also* Democko, *supra* note 7, at 369–71 (acknowledging advocates' desires to amend Federal Rules of Evidence to specifically address electronic evidence; however rebutting such change because "social networking sites pose the same concerns as and are fundamentally similar to other forms of Internet-based communications, which most courts have authenticated using the same standard and mechanisms as traditional forms of evidence").

26. *See* DiBianca, *supra* note 8, at 27 (asserting parties in litigation are entitled to discovery of social media content, regardless of privacy settings imposed by user). Litigants argue that they should have "privacy protections" over their social media content because, taking Facebook as an example, they only allow certain people, i.e., "friends," the ability to view their social media accounts and messages. *See id.* (internal quotation marks omitted). Courts regularly reject this argument, finding that, because the user has shared his or her profile with at least one other person, it is inherently no longer private and therefore is subject to discovery. *See id.* ("[C]ourts find that 'private' is not necessarily the same as 'not public.' By sharing content with others, even in limited numbers, the user has lost his or her right to keep such information 'private.'"). For a discussion of the privacy aspect, see generally Allyson Haynes Stuart, *Finding Privacy in a Sea of Social Media and Other E-Discovery*, 12 NW. J. TECH. & INTELL. PROP. 149 (2014).

should be governed by the standard evidentiary rules regarding discovery.[27] Consequently, courts apply a two-pronged analysis to determine whether evidence may be discovered from a particular social media account. The party seeking to admit the evidence must demonstrate first that the content is material and necessary to its case, and then show that any violation of the account holder's right to privacy is outweighed by the probative value of the content.[28]

B. *Admissibility of Social Media Is Trending in Litigation*

After satisfying the two-pronged test necessary for discovery, the party seeking to admit social media evidence must then properly authenticate evidence from that account in order to make it admissible in court.[29] Be-

27. *See* Steven S. Gensler, *Special Rules for Social Media Discovery?*, 65 ARK. L. REV. 7, 16–17 (2012) (discussing court's use of standard discovery rules to order plaintiffs to produce social media messages in EEOC v. Simply Storage Mgmt. LLC, 270 F.R.D. 430 (S.D. Ind. 2010)). The court in *Simply Storage* noted that "remarkably few published decisions provide guidance on the issues presented here." *See Simply Storage*, 270 F.R.D. at 434 (finding social media discovery likely to be frequent issue in litigation and noting, "[d]iscovery of [social networking sites] requires the application of basic discovery principles in a novel context"). Commentators have generally agreed with the use of current federal and state discovery rules to deal with social media evidence. *See, e.g.*, Gensler, *supra*, at 10 ("Not only do I think social-media discovery fits easily into the existing discovery scheme, I think judges have, for the most part, already figured out how to fit it in."); Rosenthal, *supra* note 5, at 261 (arguing need to apply standard evidentiary rules to social media discovery).

28. *See* Fawcett v. Altieri, 960 N.Y.S.2d 592, 595 (Sup. Ct. 2013) (discussing two-pronged analysis regarding discoverability of social media evidence).

In *Fawcett*, two personal injury defendants requested discovery of the plaintiff's social media accounts, including accounts on Facebook, MySpace, Friendster, Flickr, and other websites; the plaintiffs objected to the discovery of such information, arguing that the accounts were both private and irrelevant to the litigation at issue. *See id.* at 594–95 (describing discovery request and response). The court agreed with the plaintiffs, finding that the defendants' request for discovery was a fishing expedition and that they intended to undertake it in the hopes that something relevant would be discovered. *Id.* at 597. ("There must be a clear factual predicate in order to compel the production of social media records from the defendants or authorizations for the production of that material from certain social media providers."). The court held that this was not a sufficient basis to compel discovery of social media posts and denied the defendants' request. *See id.* ("The party requesting the discovery of an adversary's restricted social media accounts should first demonstrate a good faith basis to make the request.").

29. *See* Delaney & Heitner, *supra* note 2, at 14 (discussing authentication process of social media evidence after such evidence has been discovered). While no rules specifically address social media authentication, courts have typically applied FEDERAL RULE OF EVIDENCE 901(a) to social media evidence. *See id.* (explaining e-discovery processing firm's report on how courts have relied on FEDERAL RULE OF EVIDENCE 901(a) to determine whether social media evidence was properly authenticated). Besides using Rule 901(a), courts have also relied on FEDERAL RULE OF EVIDENCE 901(b)(4), which states that electronically stored information can be authenticated with circumstantial evidence that reflects the "contents, substance, internal patterns, or other distinctive characteristics" of the evidence. *See id.* (describing how "[a] party can authenticate electronically stored information").

cause of the unique nature of social media, no bright-line rule currently exists for authentication.[30]

1. *Which Standard to Sign up for?: The Maryland and Texas Approaches*

Since 2011, several courts have dealt with the issue of social media authentication differently; however, two particular standards have emerged as the most prominent: the Maryland Approach and the Texas Approach.[31]

In 2011, the Maryland Court of Appeals laid out what some commentators and courts have classified as a "high standard" for authenticating social media evidence in *Griffin v. State*.[32] In *Griffin*, the prosecution "sought to introduce [the defendant's] girlfriend's . . . MySpace profile to demonstrate that, prior to trial, [the girlfriend] had allegedly threatened another witness called by the State."[33] The prosecution presented "a MySpace profile in the name of 'Sistasouljah,'" which not only contained the alleged threat, but also identifying information such as the profile owner's birthday, location, and a picture of the defendant and his girlfriend together.[34] The State attempted to authenticate the MySpace profile and messages as the girlfriend's using the lead investigator from the case.[35]

The appellate court ruled these efforts insufficient, emphasizing the ease with which an individual can both make a MySpace profile in another

30. *See id.* at 14 (noting lack of "hard and fast rules" for authenticating social media evidence); *see also* Paul W. Grimm, Lisa Yurwit Bergstrom & Melissa M. O'Toole–Loureiro, *Authentication of Social Media Evidence*, 36 AM. J. TRIAL ADVOC. 433, 441 (2013) ("At present, the cases that address the authentication and admissibility evidence of social media evidence . . . unfortunately arrive at widely disparate outcomes.").

31. *See* Griffin v. State, 19 A.3d 415, 427–28 (Md. 2011) (articulating "Maryland" standard for authentication); Tienda v. State, 358 S.W.3d 633, 647 (Tex. Crim. App. 2012) (setting out "Texas" standard for authentication); *see also, e.g.*, State v. Eleck, 23 A.3d 818, 822 (Conn. App. Ct.) (describing standard similar to *Griffin* court's for social media authentication), *cert. granted mem. in part by* 30 A.3d 2 (Conn. 2011), *and aff'd on other grounds by* 100 A.3d 817 (Conn. 2014); Parker v. State, 85 A.3d 682, 686–88 (Del. 2014) (separating past cases into "Maryland approach" and "Texas approach"). *See infra* notes 35–38 and accompanying text for details regarding the Maryland standard for authentication and notes 39–42 and accompanying text for details regarding the Texas standard for authentication.

32. 19 A.3d 415 (Md. 2011); *see also Parker*, 85 A.3d at 686 (describing Maryland Approach as "[t]he higher standard for social media authentication"); Grimm et al., *supra* note 30, at 441 (describing Maryland Approach as setting "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"). *But see* Wendy Angus-Anderson, Brief, *Authenticity and Admissibility of Social Media Website Printouts*, 14 DUKE L. & TECH. REV. 33, 44–46 (2015) (arguing Maryland and Texas Approaches can be reconciled).

33. *See Griffin*, 19 A.3d at 418 (explaining case background).

34. *See id.* (providing factual background of social media evidence sought to be admitted into court).

35. *See id.* at 418–19 (explaining Maryland's authentication method and providing investigator's testimony at trial).

person's name as well as access another party's MySpace profile.[36] The court noted as an initial matter that authentication requires that the proponent produce evidence sufficient to demonstrate that the item is what the proponent claims it to be.[37] Although the court proffered a non-exhaustive list of other ways the prosecution could have authenticated the social media evidence, its analysis suggests a belief that social media evidence should be held to a higher standard of authentication than other evidence.[38]

The following year, the Texas Court of Criminal Appeals took a less restrictive approach to authenticating social media evidence in *Tienda v. State*.[39] In *Tienda*, the prosecution introduced evidence from three MySpace profile pages allegedly belonging to the defendant, who was convicted of murder in a gang-related shootout.[40] Defense counsel argued that, because of the ease with which a person could create a MySpace profile in someone else's name, as well as the fact that any reference to case-specific facts were not facts solely within the defendant's knowledge, the evidence should not have been admitted.[41] The court found that courts "need not be persuaded that the proffered evidence is authentic"; instead, the court only needs "to decide . . . whether the proponent of the evidence has supplied facts that are sufficient to support a reasonable jury determination that the evidence he has proffered is authentic."[42]

Thus, even if there is "the possibility that someone other than the alleged creator of the evidence created or manipulated" the proffered social media evidence, as long as there is "sufficient evidence of authenticity" such that "a reasonable jury [could] conclude that the evidence was au-

36. *See id.* at 423–24 (describing court's reasoning and deciding girlfriend's personal information were not "sufficient distinctive characteristics . . . to authenticate its printout"). The court highlighted its concerns that "someone other than [the girlfriend] could have not only created the [Myspace profile], but also posted the [post in question]." *Id.* at 424. The court created a standard where social media evidence could not be admitted "unless the court definitively determine[d] that the evidence [wa]s authentic." Grimm et al., *supra* note 30, at 441.

37. *See Griffin*, 19 A.3d at 423 (explaining procedure for authentication under FEDERAL RULE OF EVIDENCE 901(a) and MARYLAND RULE 5-901(b)(4)).

38. *See id.* at 427–28 (listing three methods of authenticating social media evidence: (1) getting creator to testify whether he or she created profile and posted message; (2) searching computer's internet history and hard drive "to determine whether that computer was used to originate the social networking profile and posting in question"; or (3) "obtain[ing] 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").

39. 358 S.W.3d 633 (Tex. Crim. App. 2012).

40. *Id.* at 634 (providing background of case).

41. *Id.* at 636 (explaining defendant's claims against admitting social media evidence).

42. *Id.* at 638 (describing court's standard for authentication of social media evidence).

thentic," then the proffered evidence meets the authentication burden.[43] This standard is significantly less restrictive and allows for authentication of a greater proportion of social media evidence than the *Griffin* standard.[44]

2. *Texas's Standard Gets the Most Likes*

As more and more courts have begun to encounter evidentiary issues about social media, many courts, including federal courts, have decided to adopt the Texas Approach, as opposed to the Maryland Approach.[45] For example, in 2014, two cases—*Parker v. State*[46] and *United States v. Vayner*[47]—adopted the Texas Approach espoused in *Tienda* over the Maryland Approach in *Griffin*.[48]

In *Parker v. State*, the Delaware Supreme Court put aside the threat that "social media evidence could be falsified" and relied on Rule 901 of the Delaware Rules of Evidence to determine such evidence's authenticity and admissibility in trial.[49] Similar to *Tienda*, the court held that the trial judge "may admit the social media post when there is evidence 'sufficient

---

43. *See* Grimm et al., *supra* note 30, at 441, 455.

44. *See* Angus-Anderson, *supra* note 32, at 37–38.

The "Maryland Approach [ ] [is] skeptical of social media evidence, finding the odds too great that someone other than the alleged author of the evidence was the actual creator" and therefore sets the bar high for attorneys to authenticate the evidence. *Id.* The Texas Approach is "seen as more lenient" and transfers the burden of production "to the objecting party to demonstrate that the evidence was created or manipulated by a third party." *Id.*

45. *See id.* at 38, 41 & n.74 (listing many more cases that follow Texas Approach than Maryland Approach).

46. 85 A.3d 682 (Del. 2014).

47. 769 F.3d 125 (2d Cir. 2014).

48. For a further discussion of *Parker*, see *infra* notes 49–50 and accompanying text, and for a further discussion of *Vayner*, see *infra* notes 51–53.

49. *See Parker*, 85 A.3d at 687 (explaining reason for adopting Texas Approach).

In *Parker*, the defendant was charged with second-degree assault and terroristic threatening for an altercation with a friend regarding a mutual love interest. *See id.* at 683. Delaware attempted to introduce Facebook posts allegedly authored by Parker after the altercation stating, among other things, "#caughtthatbit[*]h," and other statements referring to her own role in the altercation. *See id.* at 684 (providing content of Facebook entries). The prosecutor presented evidence from the profile, as well as testimony from the other party to the altercation, to authenticate the posts. *See id.* (describing authentication evidence, which included "[Parker's] picture, the name 'Tiffanni Parker,' and a time stamp for each entry, stating that they were posted on [the day of the altercation]. . . . The State used testimony from Brown [the other party to the altercation], as well as circumstantial evidence, to authenticate the Facebook entries"). Parker was convicted of second-degree assault, and on appeal, the Delaware Supreme Court upheld the conviction, rejecting the defendant's claim that the Facebook posts had not been properly authenticated. *See id.* at 684, 688.

to support a finding' by a reasonable juror that the proffered evidence is what its proponent claims it to be."[50]

Relying on Rule 901 of the Federal Rules of Evidence, the Second Circuit utilized the same reasonable juror standard articulated in *Tienda* and *Parker* to rule on an issue of social media authentication in *United States v. Vayner*.[51] Similar to the *Tienda* court, the *Vayner* court recognized that social media evidence could not be authenticated absent a finding that the proffering party had presented sufficient evidence such that a reasonable juror could conclude that the post in question was what its proponent claimed it to be.[52] Consequently, the Second Circuit declined to admit posts from a social media page into evidence because sufficient evidence had not been presented to support ownership of the account or authorship of the posts at issue.[53]

3. *Social Media Gets Caught in World Wide Web of Circumstantial Evidence*

Because every social media post is unique, courts have not developed a consistent set of rules regarding authentication of social media evidence.[54] Courts rely on various sources of circumstantial evidence presented by litigants who seek to authenticate particular social media ac-

50. *See id.* at 688 (stating standard and finding evidence provided for authentication "sufficient for the trial court to find that a reasonable juror could determine that the proffered evidence was authentic").

51. *See Vayner*, 769 F.3d at 132–33 (utilizing reasonable juror standard to determine authentication of VK.com profile). The *Vayner* court applied the Federal Rules of Evidence to social media authentication, requiring "evidence sufficient to support a finding that the item is what the proponent claims it is." *See id.* at 132. (quoting FED. R. EVID. 901(a)) (internal quotation marks omitted). *See infra* note 53 for details of *Vayner* court's analysis.

52. *See id.* at 132–33 (holding social media evidence not properly authenticated). The court found that the prosecution did not meet its burden of demonstrating authenticity, finding the prosecution's reliance on the personal information in the defendant's profile insufficient, as other parties knew all of that information and could have falsely created a profile in the defendant's name. *See id.* at 132 ("[T]he information contained on the VK page allegedly tying the page to [the defendant] was also known by [the witness] and likely others, some of whom may have had reasons to create a profile page falsely attributed to the defendant.").

53. *See id.* at 128–29, 131–32 (describing prosecution's attempts to authenticate VK page). Here, the prosecution argued that because information about the defendant appeared on the VK page, including his name, photograph, and some details about his life, it sufficiently indicated that the page belonged to the defendant. *See id.* However, the court rejected this argument, finding such evidence insufficient for authentication. *See id.* at 132 ("[C]ontrary to the government's argument, the mere fact that a page with [the defendant's] name and photograph happened to exist on the Internet at the time of [the witness's] testimony does not permit a reasonable conclusion that this page was created by the defendant or on his behalf.").

54. *See generally* Grimm et al., *supra* note 30 (addressing disparity in authentication standards used by courts).

counts and communications.[55] Parties typically offer testimony by the recipient of a particular message as evidence of the message's authenticity.[56]

55. *See* State v. Eleck, 23 A.3d 818, 822 (Conn. App. Ct.) (describing several ways in which litigant may successfully authenticate social media post), *cert. granted mem. in part by* 30 A.3d 2 (Conn. 2011), *and aff'd on other grounds by* 100 A.3d 817 (Conn. 2014).

The ways in which the litigant may authenticate include the following:

> (1) A witness with personal knowledge may testify that the offered evidence is what its proponent claims it to be. . . . (3) The trier of fact or an expert witness can authenticate a contested item of evidence by comparing it with preauthenticated specimens. . . . (4) The distinctive characteristics of an object, writing or other communication, when considered in conjunction with the surrounding circumstances, may provide sufficient circumstantial evidence of authenticity.

Id. (alterations in original) (internal quotations omitted). The court suggested that a combination of these factors may provide sufficient evidence of authenticity. *See id.*

56. *See* Commonwealth v. Williams, 926 N.E.2d 1162, 1171–72 (Mass. 2010) (finding testimony of recipient of Facebook messages insufficient for authentication); Smith v. State, 136 So. 3d 424, 431, 436 (Miss. 2014) (same); Campbell v. State, 382 S.W.3d 545, 551 (Tex. Ct. App. 2012) (holding testimony from recipient of Facebook messages sufficient for authentication).

In *Smith*, the defendant was convicted of capital murder of his wife's seventeen-month-old child. *See Smith*, 136 So. 3d at 426. Mississippi sought to introduce two Facebook messages allegedly from the defendant to his wife that purported to discuss the defendant's problems with the child: "[I] feel my temper building and [I] know [I] will hurt someone . . . ." *See id.* at 430 (alterations in original) (internal quotations omitted). To authenticate the messages, the defendant's wife testified that he would send her messages on Facebook and that these particular messages were sent by the defendant. *See id.* at 430–31. The Supreme Court of Mississippi held that "the State failed to provide evidence sufficient to support a finding that the Facebook messages from Smith were what the State claimed." *See id.* at 434. In so holding, the court noted that the defendant's wife did not testify as to how she knew that the defendant actually authored the Facebook messages and that, because there was no testimony regarding the security of or access to the defendant's Facebook account and no information in the messages that was known only to the defendant, the messages had not been properly authenticated. *See id.* at 434–35.

Similarly, in *Williams*, the defendant was convicted of first-degree murder, partly due to evidence presented of MySpace messages allegedly sent by the defendant's brother to one of the State's witnesses, urging the witness not to testify against the defendant or to claim a lack of memory about the events that occurred on the night of the murder. *See Williams*, 926 N.E.2d at 1165, 1171–72. The court found the messages inadmissible due to lack of authentication because the State's only evidence for authentication was one witness's testimony that the messages were sent by the defendant's brother. *See id.* at 1172–73 (noting testimony "established that the messages were sent by someone with access to Williams's MySpace Web page, [but] it did not identify the person who actually sent the communication").

In *Campbell*, the defendant was convicted of aggravated assault with a deadly weapon, and during the trial, Texas presented Facebook messages allegedly sent to the victim by the defendant as evidence. *See Campbell*, 382 S.W.3d at 546, 548. The only evidence Texas presented for authentication was the victim's testimony that she received the messages from the defendant a few days after the assault, did not send them to herself, and did not have access to the defendant's Facebook account after the incident. *See id.* at 550. The defendant argued that this evidence was

While this testimony supports a claim of authorship, a majority of courts have held that, absent some additional evidence, mere testimony from the recipient of messages is not sufficient for authentication.[57] Because social media accounts can be accessed by anyone who has the account's username and password, authorship of particular posts can be difficult to prove.[58] In some cases, a party may authenticate social media evidence either through particular testimony that confirms information in a post or message known only to a small number of people, or through the actions of the alleged author that confirm the information in the posts or messages.[59]

---

insufficient to demonstrate that the messages were in fact from his Facebook account. *See id.* at 547 (providing defendant's assertion that "there is no evidence that the messages are in fact from [defendant's] Facebook account"). Here, the court held that the victim's testimony was sufficient to authenticate the Facebook messages, finding that "there was prima facie evidence such that a reasonable jury could have found that the Facebook messages were created by [the defendant]." *See id.* at 553.

57. *See, e.g.*, *Williams*, 926 N.E.2d at 1172 (holding testimony by witness relating to authorship of messages was not enough evidence to support authentication); *Smith*, 136 So. 3d at 434 (finding testimony by message recipient insufficient for authentication). The *Williams* court analogized the MySpace post at issue to a telephone call, explaining that "a witness's testimony that he or she has received an incoming call from a person claiming to be 'A,' without more, [would be] insufficient evidence to admit the call as a conversation with 'A.'" *See Williams*, 926 N.E.2d at 1172. The court noted that additional testimony regarding page security and accessibility was necessary to authenticate the messages. *See id.* (describing additional information needed to authenticate MySpace page, including "how secure such a Web page is, who can access a MySpace Web page, whether codes are needed for such access, etc.").

58. *See Campbell*, 382 S.W.3d at 550 (noting electronic communications are particularly susceptible to fabrication and manipulation). In *Campbell*, the court noted two particular concerns associated with authenticating social media evidence: first, because any person could establish a profile under any name, the person viewing a profile would have no way of knowing for certain whether the profile was legitimate; and second, because Facebook accounts can be accessed by anyone with the account's username and password, a person viewing communications from a particular account cannot be certain that the author is the actual owner of the profile. *See id.* (explaining court's skepticism regarding social media evidence).

59. *See, e.g.*, State v. Eleck, 23 A.3d 818, 822 (Conn. App. Ct.) (holding prima facie showing of authenticity may be made through use of surrounding circumstances), *cert. granted mem. in part by* 30 A.3d 2 (Conn. 2011), *and aff'd on other grounds by* 100 A.3d 817 (Conn. 2014); Commonwealth v. Foster F., 20 N.E.3d 967, 971 (Mass. App. Ct. 2014); Boyd v. State, 175 So. 3d 1, 5–6 (Miss. 2015) (finding defendant's actions that confirmed content of Facebook messages sufficient to authenticate messages). In *Foster F.*, the defendant allegedly sent messages to three girls and, in the course of those messages, set up a plan to meet them in a particular location on a particular date to play a "'dating game.'" *See Foster F.*, 20 N.E.3d at 970. The defendant met the girls in that location on that date, and while attempting to play this game, the defendant allegedly sexually assaulted one of the girls. *See id.* The court found that, because these actions provided sufficient circumstances confirming the content of the messages, the posts were properly authenticated and were thus admissible. *See id.* at 971 (finding "[t]he judge could

Because social media communications must originate from a specific account, personal information from a particular account profile, such as photographs, location information, and personal details, can be a useful tool for litigants attempting to authenticate messages or posts originating from that account.[60] Courts differ in their willingness to accept personal

have concluded, based on the proffered evidence, that it was the juvenile who authored the Facebook messages to the victim").

Similarly, in *Boyd*, the defendant was convicted of sending sexually suggestive Facebook messages to a minor. *See Boyd*, 175 So. 3d at 7. The defendant argued "'[t]he Facebook messages did not contain any personal identifying information' and that '[w]ith nothing more to properly authenticate' the trial court should have excluded the Facebook messages from evidence." *See id.* at 5 (alterations in original). The court allowed the messages to be admitted over the defendant's objection because the defendant was carrying a cell phone that had the same six digits as the creator of the Facebook message claimed to have and "was arrested at the time and meeting place arranged in text messages originating" from that cell phone. *See id.* at 6 ("We find the Facebook messages were properly admitted considering the circumstances laid out [ ].").

60. *See* Nicholas O. McCann, *Tips for Authenticating Social Media Evidence,* 100 ILL. B.J. 482, 484 (2012) (noting courts vary in allowing authentication based on "unique identifying characteristics" of profile in question); *see also* Moore v. State, 763 S.E.2d 670, 674 (Ga. 2014) (allowing authentication of Facebook profile via pictures, hometown, cell phone number, use of nickname, and personal details on profile); Burgess v. State, 742 S.E.2d 464, 467 (Ga. 2013) (finding pictures, nicknames, age, and location on MySpace profile sufficient for authentication of account). *But see Eleck*, 23 A.3d at 821 (holding username and profile picture insufficient to authenticate Facebook profile).

In *Burgess*, the defendant was convicted on several charges for his involvement in a drive-by shooting. *See Burgess*, 742 S.E.2d at 466 (providing disposition of court). At trial, the prosecution introduced evidence from a MySpace profile allegedly belonging to the defendant and attempted to authenticate the profile using the username, age, hometown of the user, personal information about the user, and photographs of the defendant on the page. *See id.* at 467 (describing evidence presented for authentication). The court held that this evidence was sufficient to authenticate the MySpace page as belonging to the defendant. *See id.* at 467 ("In this case, there was sufficient circumstantial evidence to authenticate the printout from the MySpace profile page.").

Similarly, in *Moore,* the defense challenged the prosecution's attempt to use evidence from a Facebook profile allegedly belonging to the defendant based on lack of authentication. *See Moore*, 763 S.E.2d at 672–74 (providing factual background and noting Appellant's objection that "the Facebook page was not properly authenticated and there was insufficient evidence to prove that Appellant actually made the comments on the page"). The court held that the profile had been properly authenticated through testimony that confirmed the picture on the page was of the defendant, the hometown listed was the defendant's, the cell phone number listed on the page was the defendant's, the name on the profile was the defendant's nickname, and the page contained details about the defendant's life that were not public knowledge. *See id.*

Conversely, the court in *Eleck* found that information taken from a Facebook profile was insufficient for authentication. *See Eleck*, 23 A.3d at 825. In *Eleck*, the defendant was convicted of assault in the first degree by means of a dangerous instrument. *See id.* at 819. During trial, the defendant offered evidence of messages purportedly sent to him by the victim from her Facebook account in an attempt to impeach her credibility. *See id.* at 820 (summarizing introduction of Facebook messages allegedly sent by victim to defendant after the altercation at issue). The defendant attempted to authenticate the messages by testifying that

profile information as ample evidence of authentication.[61] However, if the opposing party does not claim that multiple parties have access to a particular profile, personal information from that profile may suffice to authenticate communications from that profile.[62]

---

the username was one that he recognized as belonging to the victim, that the profile contained photographs and other entries identifying the victim as the owner of the account, and that she had removed him as a friend the day after he testified to this effect. *See id.* at 821. The court found that this was insufficient evidence because the defendant had not demonstrated that the messages were in fact written by the victim. *See id.* at 824 (noting victim's testimony denying authorship of messages; finding defendant failed to "advance other foundational proof to authenticate that the proffered messages did, in fact, come from [the victim] and not simply from [victim's] Facebook account"). The court gave weight to the victim's testimony that her account had been hacked, noting that this "highlight[ed] the general lack of security" of Facebook accounts. *See id.* at 824 (finding victim's testimony "highlights the general lack of security . . . and raises an issue as to whether a third party may have sent the messages via [victim's] account").

61. *Compare* Dering v. State, 465 S.W.3d 668, 672 (Tex. Ct. App. 2015) (holding names and photos from Facebook profile were insufficient basis for authentication), *and Eleck*, 23 A.3d at 822 (finding information taken from witness's Facebook profile insufficient to authenticate messages sent from that account), *with Moore*, 763 S.E.2d at 674 (finding personal information and photographs of defendant on Facebook profile sufficient for authentication). *See supra* note 60 for detailed facts of *Eleck* and *Moore*.

In *Dering*, the defendant sought to transfer venue from its current location because he felt he "could not obtain a fair and impartial trial" as evidenced by the multitude of Facebook posts from third parties, none of whom testified in the case. *See Dering*, 465 S.W.3d at 670 (internal quotation marks omitted). Moreover, the posts were neither made on the defendant's account nor made by the defendant. *See id.* Wanting to stay in the current venue, "[t]he State objected to the admission of the Facebook posts because they were not properly authenticated." *See id.* The court agreed with Texas, finding that no evidence had been presented to support the claim that the posts were actually written by the purported author. *See id.* at 672 ("There was no evidence of the authenticity of who the purported author was of any of the Facebook posts. All that [the defendant] offered in terms of authenticity were the names and photos as shown on the accounts of the owner and posters. Without more, this evidence is insufficient to support a finding of authenticity."). The *Dering* court held that the posts at issue were not properly authenticated because the defendant failed to present circumstantial evidence that the posts were actually created by the alleged authors. *See id.* (describing circumstantial evidence presented and finding it "insufficient to support a finding of authenticity").

Similarly, the *Eleck* court emphasized a need for additional circumstantial evidence beyond the personal information on the profile at issue. *See Eleck*, 23 A.3d at 823 ("An electronic document may . . . be authenticated by traditional means such as . . . circumstantial evidence of 'distinctive characteristics' in the document that identify the author."). In contrast, the *Moore* court found the amount of personal information on the defendant's profile, as well as the presence of details that were not public knowledge, sufficient circumstantial evidence to authenticate the social media evidence. *See Moore*, 763 S.E.2d at 674 ("Based on this direct and circumstantial evidence, we find that the Facebook page was properly authenticated.").

62. *See Moore*, 763 S.E.2d at 674 (holding defendant's nickname, location, photographs, and biographical information sufficient to authenticate Facebook profile without considering profile security as a factor weighing against authentication); Wilson v. State, 30 N.E.3d 1264, 1269 (Ind. Ct. App. 2015) (allowing authentication based on circumstantial evidence and not addressing profile security

C. *To Share or Not to Share: Authentication Concerns Based on Ease of Access*

Authentication of any message or post on a social media account is complicated by the ease with which anyone can access the account.[63] Social media evidence presents two separate concerns regarding authentication: first, anyone can make a profile under a fictitious name, and second, a person can access another's profile simply by attaining the profile's username and password.[64] In either instance, a viewer cannot be sure whether the profile is legitimate or even who actually authored a particular post.[65] These concerns are enhanced by the fact that many users will

concerns). *But see Eleck*, 23 A.3d at 824 (emphasizing general lack of security of Facebook accounts).

The *Moore* court relied on the wealth of personal information on the defendant's profile to confirm authentication. *See Moore*, 763 S.E.2d at 674 (finding testimony confirming "that the picture on the Facebook page was of [defendant] and [ ] that [defendant's] hometown was Gary, Indiana, as listed on the page[,]" among other information, such as defendant's nickname, "structure and style of the comments posted on the page," and cell phone number, which were all on Facebook page, were sufficient to authenticate social media evidence). In *Moore*, the court did not consider profile security as a factor weighing against authentication, as the objecting party did not present evidence suggesting shared access to the profile. *See generally id.* (finding sufficient evidence for authentication of social media evidence without addressing skepticism for security of social media account).

In *Wilson*, the court did not consider security concerns regarding social media accounts and found the defendant's Twitter profile was authentic based on a witness's testimony regarding her communications with the defendant via Twitter, as well as the photos posted from the account and references to gangs with whom the defendant was known to be affiliated. *See Wilson*, 30 N.E.3d at 1268–69 ("[T]aken together, the witness testimony identifying the Twitter account as belonging to [the defendant] and the content posted on the account . . . are more than sufficient to authenticate the Twitter posts . . . ."). In comparison, in *Eleck*, because the alleged author of the posts testified that her Facebook account had been hacked, the court required that the defendant counter her testimony with evidence supporting his claim that, despite the possibility that others had accessed the account, a reasonable juror could still conclude that the alleged author created the posts at issue. *See Eleck*, 23 A.3d at 824 (finding testimony that account had been hacked "highlights the general lack of security of the medium and raises an issue as to whether a third party may have sent the messages via [the witness's] account").

63. *See Campbell*, 382 S.W.3d at 550 (noting electronic communications are particularly susceptible to fabrication and manipulation). For additional discussion of *Campbell*, see *supra* note 56. The *Campbell* court emphasized that "the fact that an electronic communication on its face purports to originate from a certain person's social networking account is generally insufficient standing alone to authenticate that person as the author of the communication." *See id.* at 549.

64. *See id.* (discussing twofold concern regarding authentication of Facebook posts).

65. The court in *Campbell* recognized that electronic forms of communication may be especially susceptible to manipulation and falsification. *See id.* at 549–50 ("However, in evaluating whether an electronic communication has been sufficiently linked to the purported author, we recognize that electronic communications are susceptible to fabrication and manipulation."). Concerns about third parties either creating profiles under fictitious identities or sending communications through another person's account therefore create significant authentication concerns. *See id.* at 550.

store their account passwords either on their computers or through cell phone apps, which allows third parties to access social media accounts simply by having control of the account holder's cell phone or computer.[66]

Because profiles can easily be fabricated or accessed by multiple people, parties seeking to admit social media evidence who do not sufficiently demonstrate the *actual* authorship of a proffered post will not meet the burden of authentication.[67] Some courts require parties to present expert testimony demonstrating profile security and how easily a person could either create an account or access another person's account.[68] Courts

66. *See Social Networking Fact Sheet*, *supra* note 4 (finding 40% of cell phone users access social network via phones). According to this study, as of 2012, an estimated 28% of cell phone users reported typically accessing their social media accounts on their phones at least once per day. *See id.*; *see also Eleck*, 23 A.3d at 822 ("[A]ccount holders frequently remain logged in to their accounts while leaving their computers and cell phones unattended."). The *Eleck* court acknowledged cell phone access to social media increased the potential for a third party to access another person's social media account. *See id.* (noting practice of remaining logged in to social media accounts subjects "passwords and website security . . . . to compromise by hackers").

67. *See* United States v. Vayner, 769 F.3d 125, 132 (2d Cir. 2014) (holding social media posts not properly authenticated because of sufficient possibility someone else could have authored posts). In *Vayner*, at issue were posts allegedly made by the defendant on VK.com, which is described to the court as the Russian equivalent of Facebook. *See id.* at 128. The only evidence presented by the prosecution was that an agent had viewed the page online and that it contained information related to the defendant. *See id.* at 129. The court found that, because no additional evidence was presented that suggested the defendant had authored the posts at issue, the posts were not properly authenticated. *See id.* at 131–32 ("The government did not provide a sufficient basis on which to conclude that the proffered printout was what the government claimed it to be . . . and there was thus insufficient evidence to authenticate the VK page and to permit its consideration by the jury."). The court recognized the possibility that someone else could have authored the posts in the defendant's name. *See id.* at 132 ("[T]here was no evidence that [the defendant] himself had created the page or was responsible for its contents."). Because nothing other than the defendant's name and photograph on the profile page suggested that he was the author of the posts, the court held that the government failed to meets its burden to support a reasonable conclusion that the posts were authored by the defendant. *See id.* ("[C]ontrary to the government's argument, the mere fact that a page with [the defendant's] name and photograph happened to exist on the Internet at the time of [the agent's] testimony does not permit a reasonable conclusion that this page was created by the defendant or on his behalf.").

68. *See, e.g.*, Commonwealth v. Williams, 926 N.E.2d 1162, 1173 (Mass. 2010) (holding MySpace profile was not properly authenticated because no testimony was presented regarding profile security). For detailed facts of *Williams*, see *supra* note 56.

In *Williams*, the proffering party presented no witness testimony regarding "how secure such a [MySpace] Web page is, who can access a Myspace Web page, whether codes are needed for such access, etc." *See id.* at 1172. Witnesses testified that messages were sent from the defendant's MySpace page, but they did not identify the actual sender of the messages. *See id.* at 1172–73. Absent such a showing, the court found that the messages had not been properly authenticated. *See id.* at 1173 ("Here, while the foundational testimony established that the messages were sent by someone with access to [the defendant's] MySpace Web page, it did

often indicate a need for specific testimony establishing that a particular social media account could not possibly have been accessed by anyone other than the account holder in order to sufficiently show that the account holder actually authored the communications at issue.[69]

III. #NOFILTER: SHARING ON SOCIAL MEDIA CONTRIBUTED TO CRIMINAL CONVICTIONS IN *SUBLET*

In *Sublet*, the Maryland Court of Appeals reviewed three cases raising the issue of social media authentication.[70] The court held that authentication of social media evidence requires proof from which a reasonable juror could find that the evidence was what the proponent claimed it to be.[71] As a result, the court declined to authenticate the Facebook posts at issue in *Sublet v. State* and affirmed the authentication of both the Twitter messages at issue in *Harris v. State* and the Facebook messages at issue in *Monge–Martinez v. State*, thus upholding the convictions of all three defendants.[72]

A. Sublet v. State

The Anne Arundel County Circuit Court convicted the petitioner, Albert Sublet (Sublet), of two counts of second-degree assault and sentenced him to ten years imprisonment for his involvement in an altercation with Chrishell Parker (Parker).[73] Sublet claimed that Parker instigated the al-

---

not identify the person who actually sent the communication. Nor was there expert testimony that no one other than [the defendant] could communicate from that Web page.").

69. *See id.* The *Williams* court held the proffered MySpace messages inadmissible based on a failure to present evidence showing that no one else could possibly have accessed the profile to send the messages. *See id.* ("Testimony regarding the contents of the [Myspace] messages should not have been admitted.").

70. *See* Sublet v. State, 113 A.3d 695, 697–708 (Md. 2015) (consolidating Sublet v. State, 2014 Md. LEXIS 370 (Ct. Spec. App. 2014) (unpublished table decision), Harris v. State, 99 A.3d 778 (Md. Ct. Spec. App. 2014) (unpublished table decision), and Monge–Martinez v. State, 99 A.3d 778 (Md. Ct. Spec. App. 2014) (unpublished table decision) into this appeal).

71. *See id.* at 718 (announcing court's authentication standard). In analyzing the facts of each case, the court relied on the Maryland rule for authentication of evidence, which states, "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." MD. R. 5-901(a). This rule is based off of the federal evidentiary rule governing authentication, which states, "To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is." FED. R. EVID. 901(a).

72. *See Sublet*, 113 A.3d at 719–22 (discussing court's decision in *Sublet*, *Harris*, and *Monge–Martinez*).

73. *See id.* at 701 (describing disposition of lower court). Sublet was initially charged "with three counts of first degree assault, second degree assault and reckless endangerment, as well as with one count of carrying a deadly weapon with intent to injure." *Id.* at 698.

tercation and sought to introduce into evidence four printed pages allegedly from Parker's Facebook page that supported this contention.[74] On the fourth page of the document, a post from "Cece Parker," admittedly Parker's account, stated, among other things, that "her [boyfriend—allegedly, Sublet] is a dead man walkn."[75] Parker, while admitting that she had authored the other entries in the document posted by "Cece Parker," denied having authored this particular statement.[76] Parker also explained that because she shared her username and password with other people, it was possible someone else could have posted this message from her account.[77]

The trial court sustained Maryland's objection to admission of the Facebook conversation based on its findings that Parker's password was not a secret, that another person could have presumably accessed her account and posted from it, and that Sublet's attorney did not present any expert testimony disputing Parker's explanation.[78] The Maryland Court of Appeals agreed with the trial court's assessment that the document had not been properly authenticated and affirmed Sublet's conviction.[79] In

74. *See id.* at 698–99. The Facebook post at issue involved a conversation between seven different Facebook users and consisted of comments to a status initially posted on the public Facebook profile of one of the conversation's participants. *See id.* at 699–700.

75. *See id.* at 700–01 (describing Parker's testimony regarding Facebook conversation). Parker did not dispute the authenticity of the first three pages of the document, but she testified that she had not written the entries on the last page—which contained the threat at issue—and "did not understand where they came from." *Id.* at 701.

76. *See id.* at 700–01 (providing Parker's testimony). When Sublet's attorney questioned Parker about the post that read, "[H]er bf is a dead man walkn," the prosecution objected, arguing that this particular post had not been properly authenticated. *See id.* at 700.

77. *See id.* at 701 (noting prosecution's challenges to authentication of Facebook posts). Parker admitted ownership of the Facebook account belonging to Cece Parker but noted that she shared her password with other people, including at least one of the other participants in the conversation at issue. *See id.* ("Parker explained that she '[gave] her logout name and password to other people' . . . ." (first alteration in original)).

78. *See id.* (noting trial court's reasoning in declining to authenticate Facebook posts). The trial court found that, because Parker's testimony cast doubt regarding authorship of the particular post, the defense failed to provide sufficient evidence for authentication. *See id.* ("The trial judge [ ] sustained the State's objection to admission of [the Facebook posts], based upon three findings: that Ms. Parker's password was not a secret, that other people could and had presumably accessed and changed or inserted information on Ms. Parker's Facebook page, thereby attributing it to her, and that Ms. Parker's explanation was not disputed by expert testimony . . . .").

79. *See id.* at 718–19 (affirming Sublet's conviction). The court of appeals noted that, "when a witness denies having personal knowledge of the creation of the item to be authenticated, that denial necessarily undercuts the notion of authenticity." *Id.* at 723 (internal quotation marks omitted). The court also found that "Sublet's argument that Ms. Parker's credibility was for the jury to determine misses the mark, because her denial of authenticity of the page undermined its admissibility." *Id.* at 719.

reaching its decision, the court noted that Sublet had not presented sufficient evidence such that a reasonable juror could have found the pages to be authentic.[80]

B. Harris v. State

The issue in *Harris v. State* stemmed from an attempt to introduce evidence from the defendant's Twitter account.[81] In *Harris*, a fight broke out at a local high school, and James, a student at the school, punched petitioner Tavares Harris's (Harris) friend, Keon.[82] Harris then allegedly planned to shoot Jared, a friend of James's, in retaliation.[83] The next day, Jared and another party were both shot and injured, allegedly by Harris.[84] Harris was convicted and sentenced to twenty years in prison for first-degree assault and the use of a handgun in the commission of a crime of violence.[85]

At Harris's trial, Maryland sought to introduce private, direct Twitter messages and public tweets obtained from two cell phones "recovered from Harris's person."[86] The direct Twitter messages showed a conversation between the users "OMGitsLOCO" and "TheyLovingTc."[87] A friend of Harris's testified that Harris was the owner of the Twitter handle "TheyLovingTc."[88] The direct messages sent by "TheyLovingTc" included

80. *See id.* at 718–19 (providing list of reasons court considered when declining to authenticate).

81. *See id.* at 702 (providing principal issue of *Harris*).

82. *See id.* (describing initial altercation). The four parties involved in the fight were Harris and his friend Keon on one side, Jared and his friend James on the other, and the fight allegedly broke out because Jared planned to rob Keon. *See id.*

83. *See id.* (introducing social media evidence at issue). Harris's alleged plan to shoot Jared C. was discovered after the shooting through an analysis of private messages and public tweets sent via Harris's Twitter account. *See id.* (noting Maryland's use of expert witness to testify to "analysis and interpretation of digital evidence recovered during the investigation" (internal quotation marks omitted)).

84. *See id.* (describing shooting for which Harris was convicted).

85. *See id.* at 706 (discussing trial court's decision in *Harris*). Harris was initially charged with "two counts of attempted first degree murder, two counts of attempted second degree murder, two counts of assault in the first degree, two counts of use of a handgun in the commission of a felony and one count of conspiracy to commit murder." *Id.* at 702.

86. *See id.* at 703 (describing social media evidence presented). The direct messages were recovered from an iPhone seized in the course of a police search of Harris's bedroom, and the public tweets were found on an Android phone seized from Harris's person. *See id.* at 702–03.

87. *See id.* at 703 (discussing content of conversation via two Twitter accounts). The iPhone was identified as belonging to Foulke, a friend of Harris's, who was found to be the owner of the Twitter handle, "OMGitsLOCO." *See id.* at 703, 705.

88. *See id.* at 705 (detailing process by which State demonstrated ownership of relevant Twitter accounts). Witness testimony, as well as the profile picture for the account, sufficiently proved that Harris was the owner of the account with the Twitter handle, "TheyLovingTc." *See id.* at 706.

a statement expressing a desire to "avenge keon" and another stating, "[T]ell them bitch ass n[****]s to come to the farm cuz I don't feel safe shooting them right by the police station unless we got the car."[89] Public tweets, posted by "TheyLovingTc" and accompanied by a profile picture identified as belonging to Harris, included statements such as "Sh[*]t finna get real tomorrow" and "F[*]ck Probation im all in tomorrow."[90] According to the timestamps on both the private messages and the public tweets, the communications were sent the night before the shooting occurred.[91]

The trial court found that Maryland had successfully authenticated both the private messages and public tweets.[92] First, Maryland called a police detective who testified that he used forensic software to identify the cell phones from which the private messages were sent.[93] Next, a friend of Harris's testified that Harris owned the Twitter handle "TheyLovingTc," thus independently verifying the account.[94] The trial court found the testimony of these two witnesses sufficient to authenticate the private

89. *See id.* at 703–04 (second alteration in original) (providing content of private messages recovered from cell phones). The messages also contained reference to a shooting and noted a desire to exact revenge. *See id.* ("[T]hey should have neva f[*]cked wit Y2C bra it's game ova[.]").

90. *See id.* at 705–06 (discussing profile evidence linking tweets to defendant). The trial judge found the defendant's profile picture, which appeared next to the tweets, and Harris's username, which matched the username in the private messages, combined with the fact that the tweets "contained content that would only have been created by a few people," was sufficient for authenticating the social media evidence. *See id.* at 706 (internal quotation marks omitted).

91. *See id.* at 705 (presenting timestamps of communications). The timestamps on each communication at issue indicated that they were sent on May 17, 2012, and the shooting occurred on May 18, 2012. *See id.* at 702, 705. The timestamp on the public tweets indicated they were posted within an hour of the already authenticated private messages. *Id.*

92. *See id.* at 706 (explaining trial court's ruling on defendant's authentication objection). *See supra* notes 86–91 and accompanying text for a discussion of the circumstantial evidence the trial court relied on in allowing the messages and posts to be admitted over the defendant's objection.

93. *See id.* at 705 (detailing technical evidence State presented for authentication). The detective testified that through the use of special forensic software, he was able to compile the conversations and determine that the direct messages sent from the iPhone were authored by "OMGitsLOCO" and that the iPhone received messages from "TheyLovingTc." *See id.* Detective Grimes was able to perform a full forensic examination of the iPhone, which included accessing the phone's "contacts, the call logs, . . . images, . . . videos, [and] Twitter chats . . . ." *See id.* (first, second, and third alterations in original) (internal quotation marks omitted).

94. *See id.* (discussing independent witness verification of posts). Jahmil, a friend of Harris's, testified based on personal knowledge that Harris owned the Twitter handle, "TheyLovingTc." *See id.* at 705–06. The court found that this was sufficient independent verification of the account. *See id.* at 706 (holding evidence properly authenticated).

messages.[95] The trial judge then concluded that the public tweets were also properly authenticated, because they were authored at the same time as the direct messages and contained information that only a few people could have known.[96] The court of appeals affirmed the trial court's decision, finding that there were sufficient distinctive characteristics from which the trial judge could have determined that a reasonable juror could find the direct messages and tweets authentic.[97]

C. Monge–Martinez v. State

In the third case, *Monge–Martinez v. State*, petitioner Carlos Alberto Monge–Martinez (Monge–Martinez) was convicted and sentenced to thirteen years in prison for second-degree assault and openly carrying a dangerous weapon with the intent to injure.[98] The incident involved an altercation between Monge–Martinez and his former girlfriend, Dorothy Ana Santa Maria (Santa Maria), which resulted in Santa Maria being stabbed.[99] At trial, Maryland attempted to introduce private Facebook messages allegedly sent to Santa Maria by Monge–Martinez.[100] The messages were sent from a profile user named Carlos Monge on the same day as the altercation, and in the messages, the sender apologized to Santa Maria, asked her for forgiveness, reproached her for deceiving him, and expressed his love for her.[101] Monge–Martinez's attorney objected to the admission of these messages based on a lack of proper authentication.[102]

---

95. *See id.* at 704 ("The trial judge determined that [the private messages] were properly authenticated, because, along with the proffer of Detective Grimes's testimony, there was independent verification of the Twitter account . . . .").

96. *See id.* at 706 (describing circumstantial evidence used to authenticate public tweets).

97. *See id.* at 722 (stating court of appeals' holding).

98. *See id.* at 708 (providing trial court's disposition in *Monge–Martinez*). Monge–Martinez was charged with "attempted second degree murder and two counts each of first degree assault, second degree assault and reckless endangerment . . . ." *Id.* at 707.

99. *See id.* at 707 (providing details of altercation at issue in *Monge–Martinez*). The prosecution claimed that Monge–Martinez "intentionally instigated the fight," while Monge–Martinez argued that "he was defending himself from Ms. Santa Maria." *See id.*

100. *See id.* (introducing evidence presented by Maryland). Maryland attempted to use these messages to show that Monge–Martinez expressed remorse for his actions, which would counter his claim of self-defense. *See id.*

101. *See id.* (describing content of Facebook messages at issue). Maryland presented printed out copies of three messages: the first asked for forgiveness, the second included a statement by the author that he or she "no longer want[ed] to live with this," and the third expressed love for Santa Maria but also claimed that she deceived the author. *See id.* (internal quotation marks omitted). The timestamps of the messages indicated that they were sent on the afternoon of April 23, 2012, the same day that the altercation at issue occurred. *See id.* at 707, 721.

102. *See id.* at 707 (stating defense's objections to admission of Facebook messages). The defense argued that the messages were not properly authenticated because nothing in them referred specifically to the altercation at issue. *See id.* ("Monge–Martinez's attorney objected to [the messages'] admission on the basis

The court of appeals upheld Monge–Martinez's conviction, finding that the State presented sufficient circumstantial evidence to authenticate the Facebook messages.[103] The court of appeals agreed with the trial court in finding that Santa Maria's testimony, the timestamps of the messages, the fact that the messages were written in Monge–Martinez's native language of Spanish, and the allusions in the messages to the stabbing, sufficiently met the threshold of required circumstantial evidence for authentication.[104] Notably, the court found that the authenticity inquiry was context-specific and that there was no requirement that biographical information be present on the Facebook profile in order to authenticate the messages.[105]

IV. AUTHENTICATION STANDARD GETS STATUS UPDATE IN *SUBLET*

In *Sublet*, the Court of Appeals of Maryland attempted to clarify the standard for authentication of social media evidence that the same court elucidated in *Griffin*.[106] In both *Sublet* and *Griffin*, the court applied the

that 'the State will not be able to show any evidence that's referring to the incident on the 23rd.' ").

103. *See id.* at 722 (holding trial court did not err in admitting Facebook messages in *Monge–Martinez*). The court of appeals held that social media authentication depends on the trial judge finding sufficient proof from which a reasonable juror could find the evidence to be what its proponent claims it to be. *See id.* ("We hold that, in order to authenticate evidence derived from a social networking website, the trial judge must determine that there is proof from which a reasonable juror could find that the evidence is what the proponent claims it to be.").

104. *See id.* at 721 (discussing evidence presented by State in *Monge–Martinez* in order to authenticate Facebook messages). The trial court noted that the messages possessed sufficient distinctive characteristics for authentication. *See id.* at 721–22 ("The various communications from Monge–Martinez, together with the limited number of people knowledgeable of the incident as well as the use of Spanish in each message was sufficient evidence upon which the trial judge could rely to authenticate the Facebook messages.").

105. *See id.* at 721 ("The lack of biographical information . . . does not, by itself, prevent authentication, because the inquiry is context-specific; what may be present, yet insufficient, in one case may not be required in another situation."); *see also, e.g.*, United States v. Vayner, 769 F.3d 125, 132–33 (2d Cir. 2014) (finding biographical information present on profile page insufficient to authenticate because information was known to many others and requiring more context-specific information linking defendant to profile page).

106. *See Sublet*, 113 A.3d at 698 ("We shall hold that, in order to authenticate evidence derived from a social networking website, the trial judge must determine that there is proof from which a reasonable juror could find that the evidence is what the proponent claims it to be."); *see also* Griffin v. State, 19 A.3d 415, 423 (Md. 2011) ("[T]he 'requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims,' to insure trustworthiness." (quoting Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 541–42 (D. Md. 2007))).

In *Griffin*, the court of appeals considered social media authentication as an issue of first impression. *Griffin*, 19 A.3d at 422 ("[N]either we nor our appellate brethren heretofore has considered [MARYLAND RULE 5-901's] application to authenticate pages printed from a social networking site."). The *Griffin* court required that the proffering party present evidence of sufficient distinctive

existing Maryland Rules of Evidence, noting that, while the rules do not explicitly define authentication standards for social media, they provide the basis by which all evidence should be authenticated.[107]

Although the court affirmed the trial courts' determinations in all three cases, three of seven judges dissented in the case of the first defendant, Sublet.[108] The dissent found the majority's holding, which upheld the exclusion of social media evidence, to be inconsistent with the other two cases, which each upheld the admission of social media evidence.[109] The dissent contended that the majority's holding led to the creation of a murky rule that could not be applied with consistency in the future.[110]

---

characteristics to demonstrate that the evidence at issue was actually created by the person alleged to have created it. *See id.* at 424 (noting need for "greater degree of authentication than merely identifying the date of birth of the creator and her . . . photograph on the site" because of the "potential for abuse and manipulation of a social networking site by someone other than its purported creator and/or user"). Since *Griffin*, the use of social media in litigation has increased. *Sublet*, 113 A.3d at 713 ("In the period since *Griffin* had been decided, cases in which authentication of social networking websites and postings has been addressed have proliferated.").

107. *See Sublet*, 113 A.3d at 719–22 (applying MD. R. 5-901 to cases); *see also Griffin*, 19 A.3d at 427 (providing three non-exclusive ways of authenticating social media evidence based on MARYLAND'S RULE 5-901). Neither the state nor the federal rule for authentication specifically addresses social media, but each provides a general basis for the authentication of all evidence. *See* MD. R. 5-901; *see also* FED. R. EVID. 901. Commentators argue that the existing evidentiary rules provide a sufficient basis for authentication and that no new rules are necessary to address social media authentication. *See, e.g.*, Democko, *supra* note 7, at 405 (arguing education of judges and attorneys is more effective than attempting to craft new evidentiary rule); Rosenthal, *supra* note 5, at 261 (noting current evidentiary rules regarding discovery of evidence sufficient to handle discovery of social media evidence as well).

108. *See Sublet*, 113 A.3d at 722 (announcing dissenting judges).

109. *See id.* at 722–23 (Adkins, J., dissenting in part) (disagreeing with majority's application of reasonable juror standard as applied to consolidated case, *Sublet v. State*, 2014 Md. LEXIS 370 (Ct. Spec. App. 2014) (unpublished table decision)). In disagreeing with the majority's holding for the *Sublet* case, the dissent referred to the "relatively low threshold for admissibility" and authentication the court adopted in *Harris* and argued that the amount of circumstantial evidence presented in *Sublet* should have been sufficient to meet that threshold. *See id.* at 723. The dissent found unpersuasive Parker's claims that, although she authored the posts on the first three pages, she was not responsible for the posts on the final page. *See id.* at 724 ("If we step back and put ourselves in the jury box, can we say that we would be unreasonable if we concluded that not only did Ms. Parker author the posts under her profile that appear on page one, but that she continued the conversation as shown on page four of the print-out?").

110. *See id.* at 725 (arguing *Sublet* ruling created unclear standard). Based on the context and content of the messages, the dissent posited that, not only would it be reasonable for a juror to conclude that Parker was the author, "it would be the unusual juror who would *not* draw that conclusion." *See id.* at 724.

The dissent compared the facts of *Sublet* to the Delaware Supreme Court's holding in *Parker v. State*, 85 A.3d 682 (Del. 2014). *See id.* at 724–45 (analyzing *Parker* court's discussion of authentication). They argued that the *Parker* court's holding was more appropriate in relation to the case at issue, especially because the "evidence supporting authentication of the Facebook entries in [*Sublet*] [wa]s stronger than in *Parker*." *See id.* at 725. The dissent, in comparing the two cases,

A. *Court's Timeline Shows Use of Past Cases to Inform* Sublet *Decision*

The *Sublet* court began its analysis by recognizing the unique challenges presented by social media authentication.[111] Unlike other sources of evidence, authorship of social media posts can be complicated by a number of factors relating to the anonymity and ease of access of social media sites.[112] Authentication of social media thus links inextricably with an analysis of the actual ownership of a profile and the ease with which parties other than the actual owner can access a particular account.[113]

The *Sublet* court next referred to its holding four years prior in *Griffin*, noting that the Maryland Court of Appeals grappled with social media authentication for the first time in that case.[114] The *Sublet* court noted that, while *Griffin* provided a foundation for its future jurisprudence, the issue

---

claimed that the majority's decision in *Sublet* set the bar for authentication too high and "muddled" the court's traditional "reasonable juror" standard. *See id.*

> [T]he Majority set bad precedent in holding that a trial judge can establish such a high bar for authentication as the court did in the *Sublet* case. The Majority muddled our "reasonable juror" standard by refusing to accept Facebook posts as authenticated, based on an undisputed admission by the witness that she made posts referring to the fight at the party in a Facebook conversation with friends the day after the party, but denying the posts *on the same topic* occurring shortly thereafter.

Id.

111. *See id.* at 710–11 (majority opinion) (discussing authentication of writings and noting unique challenges of social media). The *Sublet* court began by noting that authentication, for many types of written evidence, is accomplished through determining authorship. *See id.* at 710 ("The most straightforward approach to authenticating a writing is to ask an individual with personal knowledge about the document whether the matter was what it purported to be."). With social media, however, such analysis becomes especially challenging. *See id.* at 711 ("[T]raditional opportunities for authentication are reduced by the lack of handwriting, the absence of a physical location of the document and the inherent anonymity provided by posting on websites.").

112. *See id.* (discussing anonymity and ease of access to social media accounts). The court discussed the process by which a social media profile is created, noting that, although a person must provide biographical information in order to create a profile, "there doesn't appear to be a way to validate such information before a page can be created." *See id.* (internal quotation marks omitted) (noting court's concern of inability to validate creator of profile). Further, owners of social media profiles frequently, as in *Sublet*, share their login and password information with other people, which adds another layer of complication when trying to assess the authenticity of a profile or post. *See id.* at 701, 712 (presenting Parker's claim in *Sublet* that her password was known by others).

113. *See id.* at 712 (finding authentication of social media complicated by inability to confirm identity of profile's creator and ease with which accounts can be accessed by others); *see also* Griffin v. State, 19 A.3d 415, 421 (Md. 2011) ("[A]nyone 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 . . . ."). The *Sublet* court noted that authentication depends on whether a profile was actually "created by its purported owner" and on whether any other person has gained access to the profile. *See Sublet*, 113 A.3d at 712.

114. *See Griffin*, 19 A.3d at 422 ("[N]either we nor our appellate brethren heretofore has considered [MARYLAND RULE 5-901's] application to authenticate

of authentication of social media was an open one that requires further analysis.[115] The court next turned to *Vayner* for guidance.[116] In *Vayner*, the Second Circuit found that social media authentication depends on a context-specific analysis of whether, based on distinctive characteristics and the surrounding circumstances, sufficient proof existed such that a reasonable juror could find the item in question to be authentic.[117] The *Sublet* court drew from the *Vayner* ruling, emphasizing the distinctive characteristics—or lack thereof—in the social media evidence in each of the cases before it.[118]

B. *Dissent Tags Majority's Holding as a #Fail*

While all seven judges joined in the majority opinion with respect to *Harris* and *Monge–Martinez*, three of the judges dissented from the majority in *Sublet*, finding the majority's application of the reasonable juror standard in the *Sublet* case to be inconsistent with the court's analysis in the

---

pages printed from a social networking site."). For a description of the facts and holding in *Griffin*, see *supra* notes 33–38 and accompanying text.

Although the *Griffin* court found the information in its case to be insufficient for authenticating the social media evidence, the court identified three potential, non-exclusive means of social media authentication. *See id.* at 427–28 (listing possible methods for authenticating social media evidence). For a list of the *Griffin* court's means for authentication, see *supra* note 38.

115. *See Sublet*, 113 A.3d at 713 (noting increase in use of social media in litigation since *Griffin*). The *Sublet* court tasked itself to "discern a standard for authentication of social networking evidence" in the wake of *Griffin*. *See id.* at 714.

116. *See id.* ("[W]e find succor in the standard articulated by the United States Court of Appeals for the Second Circuit in *United States v. Vayner*, which, on facts analogous to those in *Griffin*, reached a similar conclusion." (citation omitted)). The *Sublet* court subsequently used the *Vayner* ruling as a guide in its development of an updated standard for social media authentication. *See id.*

117. *See id.* at 715 ("[T]his requirement is satisfied if sufficient proof has been introduced so that a reasonable juror could find in favor of authenticity or identification. Thereafter, the jury ultimately is left to make the determination as to whether the evidence is, in fact, what its proponent claims." (citation omitted) (quoting United States v. Vayner, 769 F.3d 125, 129–30 (2d Cir. 2014)) (internal quotation marks omitted)).

In *Vayner*, the Second Circuit found that the government failed to properly authenticate evidence from VK.com, described as the Russian equivalent of Facebook. *See Vayner*, 769 F.3d at 127 (announcing court's holding). The court declined to speculate as to what evidence would have been sufficient for authentication in this case, emphasizing that the authentication of social media is highly context-specific and can draw from a variety of sources. *See id.* at 133 ("We express no view on what kind of evidence *would* have been sufficient to authenticate the VK page . . . . [A]s with any piece of evidence whose authenticity is in question, the 'type and quantum' of evidence necessary to authenticate a web page will always depend on context."). For more discussion on *Vayner*, see *supra* notes 51–53 and accompanying text.

118. *See Sublet*, 113 A.3d at 718–22 (detailing distinctive characteristics provided for authentication in each of the cases at issue). *See supra* notes 70–105 and accompanying text for details regarding circumstantial evidence used to authenticate posts in each case.

other cases.[119] The dissenting judges felt that the majority's decision with respect to *Sublet* created bad precedent, arguing that the appellant, Sublet, did present sufficient evidence to meet the relatively low threshold requirement suggested by both the court's holding in *Harris* and by the Second Circuit in *Vayner*.[120] Stressing the likelihood that social media's use in litigation will continue to become more prevalent in the future, the dissent predicted that the *Sublet* holding would create a vague standard that courts would struggle to apply with consistency in the future.[121]

---

119. *See Sublet*, 113 A.3d at 724 (Adkins, J., dissenting in part) (arguing reasonable juror would have found Parker authored the last page of social media evidence). The dissent noted that, although Parker eventually denied having authored the final page of the four pages allegedly taken from her Facebook profile, she initially admitted to having "said" the content written in the posts, "without qualifying" that her response referred only to "the first three pages" of the document. *See id.* at 723 (identifying contradictory evidence to suggest social media profile was properly authenticated). Further, the dissent argued sufficient distinctive characteristics existed in *Sublet* such that a reasonable juror could have found Parker authored the posts on the fourth page of the document. *See id.* at 723–24 ("I submit that the circumstantial evidence in *Sublet* . . . was [ ] sufficient to pass the preliminary, low threshold test necessary to authenticate the Facebook conversation."). The dissent found that the similarity in content between the pages necessarily led to the conclusion that the final page had also been authored by Parker and that it would be only an unusual juror who would reach the opposite conclusion. *See id.* at 724 ("The Majority misses the mark by ignoring that the contents and substance of the entries on page four relate directly to the entries on pages one through three. . . . If we step back and put ourselves in the jury box, can we say that we would be unreasonable if we concluded that not only did Ms. Parker author the posts under her profile that appear on page one, but that she continued the conversation as shown on page four of the print-out?").

120. *See id.* at 723–25 (noting apparent inconsistencies in majority's ruling). The dissent referenced the *Vayner* standard, noting that "the bar for authentication of evidence is not particularly high." *Id.* at 723 (quoting *Vayner*, 769 F.3d at 130) (internal quotations omitted). Comparing the circumstantial evidence in *Sublet* to that in *Harris*, the dissent argued that the circumstantial evidence in *Sublet* was sufficient to overcome the low threshold. *See id.* at 723 (arguing circumstantial evidence in *Sublet* should suffice for authentication). The dissent also referenced *Parker v. State*, 85 A.3d 682 (Del. 2014), in which the Delaware Supreme Court found that circumstantial evidence presented to authenticate Facebook posts was sufficient because the substance of the post referenced the altercation at issue, the post was created the day after the altercation at issue, and a witness "testified that she viewed Parker's post through a mutual friend. . . . [and subsequently] . . . shared the post and published it on her own Facebook page." *See Sublet*, 113 A.3d at 724–25 (quoting *Parker*, 85 A.3d at 688) (internal quotation marks omitted). The Delaware court held that the circumstantial evidence and testimony were sufficient for the trial court to find that a "reasonable juror could determine that the proffered evidence was authentic." *See Parker*, 85 A.3d at 688. The *Sublet* dissent felt that the majority ignored *Parker* in holding that the posts in *Sublet* had not properly been authenticated, stating that more evidence had been presented in *Sublet* for authentication than in *Parker*. *See Sublet*, 113 A.3d at 725 (Adkins, J., dissenting in part) ("The evidence supporting authentication of the Facebook entries in [*Sublet*] is stronger than in *Parker*.").

121. *See Sublet*, 113 A.3d at 725 (arguing majority's holding set bad precedent in allowing high bar for authentication). The dissent agreed with the court's adoption of the reasonable juror standard and the use of circumstantial evidence for social media authentication; however, the dissent felt that the standard was blurred

V. *SUBLET* COURT'S DECISION UNLIKELY TO GET FOLLOWERS

Courts in the future will likely struggle to apply the rule set forth in *Sublet*.[122] While the court's use of a context-specific, reasonable juror standard creates an effective baseline for social media authentication, the court failed to provide effective guidance regarding the types and quantity of circumstantial evidence that is sufficient for authentication.[123] Courts faced with issues of social media authentication in the future should continue to rely on the existing rules of evidence, just as the *Sublet* court did.[124] As technology continues to develop and more social media authentication issues appear in courts, a clearer articulation of the appropriate circumstantial evidence that would authenticate social media evidence is needed to prevent the types of contrasting holdings illustrated in *Sublet*.[125]

---

by the court's holding in *Sublet*, stating that, if the court wants its standard to be used effectively in future litigation, it should have developed a clearer standard. *See id.* ("We would enunciate a clearer standard and advance the law more profitably if we affirmed the trial court rulings in *Harris* and *Monge–Martinez*, but reversed the trial court in *Sublet*.").

122. *See id.* at 698 (majority opinion) (articulating reasonable juror standard for social media authentication). In *Sublet*, the court's holdings relied on circumstantial evidence to determine authenticity of evidence. *See id.* at 718–22. However, the application of the standard to the *Sublet* case appears internally inconsistent, as the standard for authentication required in *Sublet* exceeded that which was required in both *Harris* and *Monge–Martinez*. *See id.* at 723 (Adkins, J., dissenting in part) (discussing low threshold for authentication relied on for *Harris* and *Monge–Martinez* and arguing *Sublet* evidence was properly authenticated based on this standard).

123. *See id.* at 718–22 (drawing on evidence of content, style of messages, external circumstances, and other factors in ruling on authentication). Here, by using a reasonable juror standard, which is consistent with both MARYLAND RULE 5-901 and FEDERAL RULE OF EVIDENCE 901, the court recognizes that social media evidence presents a vast array of authentication concerns. *See id.* at 712 ("Authentication of social networking communications and postings has been and continues to be a significant issue."). However, as noted in the dissent, the standard applied in *Sublet* appears to differ from that applied in both *Harris* and *Monge–Martinez*. *See id.* at 723 (Adkins, J., dissenting in part) ("I . . . think the Majority fails, in its disposition of the *Sublet* case, to adhere to the relatively low threshold for admissibility that it adopts and applies to authentication issues in *Harris*.").

124. *See Parker*, 85 A.3d at 687 ("Although we are mindful of the concern that social media evidence could be falsified, the existing Rules of Evidence provide an appropriate framework for determining admissibility."). The *Parker* court noted that the ultimate determination of authenticity should be for the jury and that therefore the trial judge's role should be to determine whether there is enough evidence to support a finding by a reasonable juror that the evidence is what the proponent claims it to be. *See id.* at 687–88 (noting social media evidence "should be subject to the same authentication requirements under the DELAWARE RULES OF EVIDENCE RULE 901(b) as any other evidence" and may be authenticated with any available form of verification, "including witness testimony, corroborative circumstances, distinctive characteristics, or descriptions and explanations of the technical process or system that generated the evidence in question").

125. *See* Jonathan L. Moore, *Time for an Upgrade: Amending the Federal Rules of Evidence to Address the Challenges of Electronically Stored Information in Civil Litigation*, 50 JURIMETRICS J. 147, 161–62 (2010) (noting courts vary in type and amount of

A. *Social Media Authentication Should Reject Friend Request from New Rule of Evidence*

While some scholars argue that social media evidence requires a special evidentiary rule because of its unique characteristics, development of such a rule would be both "unnecessary" and unduly confusing.[126] Any special rule that involves a trial judge acting as a gatekeeper for evidence would likely utilize a reasonableness standard, particularly when addressing the authentication of evidence.[127] Moreover, because every social me-

---

circumstantial evidence required for authentication). Moore notes that some courts allow electronically stored information to be authenticated with information on printed out sheets alone, while others "remain wary of the potential for fraud and therefore require parties to present elaborate evidence demonstrating the integrity of a computerized storage system." *See id.* at 162.

126. *See* Democko, *supra* note 7, at 370, 402 (noting heightened standard of authentication for social media would take away jury's ability to determine strength of evidence for itself); *see also* Griffin v. State, 19 A.3d 415, 429–30 (Md. 2011) (Harrell, J., dissenting) (emphasizing need to apply reasonable juror standard to authentication and allow jurors to decide for themselves whether evidence is properly authenticated).

Democko further notes that authentication of evidence should be determined on a case-by-case basis and that a bright-line rule specifically addressing social media would be insufficient. *See id.* at 404 ("Since technology is always changing and the facts or circumstances surrounding each case can differ significantly, a per se authentication rule would be inadequate to address all forms of electronic evidence offered."). In *Vayner*, the Second Circuit noted that social media evidence must be based on the particular circumstances of the case, refusing to speculate as to what evidence would have been sufficient in that case for authentication. *See* United States v. Vayner, 769 F.3d 125, 133 (2d Cir. 2014) (advocating for individualized authentication of social media evidence). The Second Circuit's ruling suggests any rule that states with greater specificity the requirements for social media authentication would be an unhelpful and inappropriate standard. *See id.* ("We express no view on what kind of evidence *would* have been sufficient to authenticate the [Russian Facebook] page and warrant its consideration by the jury. Evidence may be authenticated in many ways, and as with any piece of evidence whose authenticity is in question, the 'type and quantum' of evidence necessary to authenticate a web page will always depend on context."). *But see* Moore, *supra* note 125, at 183 (suggesting "technology-specific amendment" to Rules of Evidence would promote consistency in authentication).

127. *See, e.g.*, Parker v. State, 85 A.3d 682, 687–88 (Del. 2014) (adopting *Tienda* reasonable juror standard for social media authentication); Tienda v. State, 358 S.W.3d 633, 638 (Tex. Crim. App. 2012) (utilizing reasonable juror standard for authentication).

The court in *Parker* debated the merits of each of the prior standards and found that the *Tienda* standard better aligned with the existing rules of evidence. *See Parker*, 85 A.3d at 687–88. In so finding, the court addressed some of the unique issues associated with social media evidence, including the ease at which a profile or post could be falsified and held that the use of a reasonable juror standard best dealt with these issues. *See id.* at 687–88 ("Although we are mindful of the concern that social media evidence could be falsified, the existing Rules of Evidence provide an appropriate framework for determining admissibility."). The court in *Sublet* relied in part on the *Parker* decision in holding that a reasonable juror standard was the most appropriate means of authenticating social media evidence. *See Sublet*, 113 A.3d at 718. These holdings indicate that courts choose to follow a reasonableness standard in authenticating social media posts rather than

dia post is unique and could involve a potentially infinite number of possible circumstances, an evidentiary rule requiring courts to create a bright line for the particular circumstances relevant to authentication would inevitably lead to arbitrary inclusion or exclusion of evidence.[128] Therefore, using the existing state and federal rules of evidence is an appropriate framework from which to approach these issues.[129]

B. *Too Many Tweets Leads to Courtroom Defeat: Courts Must Determine Level of Circumstantial Evidence Sufficient for Authentication*

The ultimate issue in *Sublet v. State* involved the point at which sufficient circumstantial evidence exists to authenticate the social media evidence.[130] Because incontrovertible proof of authenticity rarely exists for

seeking to develop a new special rule for this evidence. *See* Democko, *supra* note 7, at 400 (emphasizing sufficient flexibility of existing rules of evidence to accommodate changes in technology).

128. *See Vayner*, 769 F.3d at 133 (noting social media authentication must be based on context). The *Vayner* decision emphasizes that a bright-line rule for social media authentication would be unworkable because each item of social media evidence is, by its nature, unique, and therefore, "the 'type and quantum' of evidence necessary to authenticate a web page will always depend on context." *See id.* (quoting United States v. Sliker, 751 F.2d 477, 488 (2d Cir. 1984)). Because of the rapidly developing nature of social media, a bright-line rule would be inappropriate, as social media authentication requires individual analysis based on distinct features and relevant surrounding circumstances. *See Tienda*, 358 S.W.3d at 639 ("[T]he 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."); Democko, *supra* note 7, at 404 (noting authentication rule for social media "would be inadequate to address all forms of electronic evidence offered").

129. *See Sublet*, 113 A.3d at 722 ("[I]n order to authenticate evidence derived from a social networking website, the trial judge must determine that there is proof from which a reasonable juror could find that the evidence is what the proponent claims it to be."). The *Sublet* court's holding is consistent with other jurisdictions that draw from existing rules of evidence to adopt a reasonable juror standard for social media authentication. *See, e.g.*, Campbell v. State, 382 S.W.3d 545, 552 (Tex. Ct. App. 2012) (noting authentication succeeds without definitive proof so long as sufficient evidence is presented to satisfy reasonable juror standard); *see also* State v. Eleck, 23 A.3d 818, 823 (Conn. App. Ct.) (holding that social media evidence should be authenticated using traditional rules of evidence, including circumstantial evidence identifying author of social media content), *cert. granted mem. in part by* 30 A.3d 2 (Conn. 2011), *and aff'd on other grounds by* 100 A.3d 817 (Conn. 2014); *Tienda*, 358 S.W.3d at 638 ("The preliminary question for the trial court to decide is simply whether the proponent of the evidence has supplied facts that are sufficient to support a reasonable jury determination that the evidence he has proffered is authentic.").

130. *See Sublet*, 113 A.3d at 718–22 (affirming trial courts' decisions to admit or deny social media evidence based on level of circumstantial evidence presented by proffering party for authentication). The nature of social media evidence implies that there can be no clear tipping point at which a party has presented enough evidence to authenticate a particular post or message. *See Vayner*, 769 F.3d at 130 (noting authentication of social media evidence depends on context). The highest standard of authentication for social media evidence is testimony by the author confirming that they created the posts in question. *See Griffin*, 19 A.3d at

social media evidence, parties must rely on various types of circumstantial evidence for authentication.[131] One common source of circumstantial evidence parties have utilized in these types of cases is the content of the profile from which the posts or messages at issue originated.[132] Nonetheless, the nature of social media and ease with which a profile can both be created and accessed render this evidence, standing alone, insufficient for authentication.[133]

---

427 ("The first, and perhaps most obvious method [of authentication] would be to ask the purported creator if she indeed created the profile and also if she added the posting in question . . . ."). However, in the majority of cases dealing with authentication objections, the alleged author of a post disputes a claim of authorship. *See, e.g.*, *Vayner*, 769 F.3d at 128 (requiring circumstantial evidence be presented to overcome defendant's claim that he had not created profile at issue). Therefore, parties must rely on circumstantial evidence and distinctive characteristics in order to authenticate social media posts. *See Sublet*, 113 A.3d at 719–22 (relying on testimony, time stamps of messages, and other circumstantial evidence to prove authenticity of social media evidence).

131. *See, e.g.*, Moore v. State, 763 S.E.2d 670, 674 (Ga. 2014) (allowing authentication based on content of profile, structure of posts, defendant's admission of ownership of profile); Burgess v. State, 742 S.E.2d 464, 467 (Ga. 2013) (holding circumstantial evidence based on content of profile and testimony about defendant corresponding to profile information sufficient for authentication); Commonwealth v. Foster F., 20 N.E.3d 967, 971 (Mass. App. Ct. 2014) (finding defendant's actions relating to content of messages, affidavit from Facebook record keeper, and police report regarding messages provided sufficient circumstantial evidence for authentication). For detailed analyses of *Foster F.*, *Burgess*, and *Moore*, see *supra* notes 59 and 60.

132. *See, e.g.*, *Moore*, 763 S.E.2d at 674 (authenticating Facebook profile in part based on private details about defendant posted on page); *Burgess*, 742 S.E.2d at 467 (allowing authentication of MySpace profile based on nickname on profile, photographs, and personal information about defendant on page). *But see* Smith v. State, 136 So. 3d 424, 434–35 (Miss. 2014) (holding name and profile picture alone insufficient to authenticate profile). In both *Moore* and *Burgess*, the Georgia Supreme Court found that the use of circumstantial evidence from the defendant's social media profile met the reasonable juror standard for authentication. *See Moore*, 763 S.E.2d at 674 ("Based on this direct and circumstantial evidence, we find that the Facebook page was properly authenticated."); *Burgess*, 742 S.E.2d at 467 ("In this case, there was sufficient circumstantial evidence to authenticate the printout from the MySpace profile page."). However, in *Smith*, the only evidence offered for authentication was the name on a Facebook profile and an unclear profile picture; the court held that additional circumstantial evidence must be produced to authenticate the Facebook account as belonging to the defendant. *See Smith*, 136 So. 3d at 434 (finding "State failed [to] make a prima facie case that the Facebook profile whence the messages came belonged to Smith . . . . [or] that the messages were actually sent by Smith").

133. *See Campbell*, 382 S.W.3d at 550 (finding evidence of account from which message sent insufficient for authentication). The ease with which any person can create a profile on a social media site renders it impossible to determine, based solely on the information on a page, who actually controls that profile. *See Tienda*, 358 S.W.3d at 641–42 (noting ease at which profiles can be hacked or accessed by parties other than account owner). Similarly, testimony by a party who received messages from an account or who saw posts on a particular page cannot authenticate those messages. *See Eleck*, 23 A.3d at 820–21 (holding testimony by recipient of Facebook messages insufficient standing alone for authentication). Even if the recipient of a message testifies that it came from the alleged party's profile, with-

Testimony by an alleged author that they did not create a disputed post raises significant doubt regarding authenticity.[134] If such testimony is presented, the other party must counter this claim with additional circumstantial evidence.[135] If authorship of a particular post or message is disputed, the trial judge must balance whether the proffering party presented sufficient circumstantial evidence to overcome the alleged author's denial of authorship.[136] The *Sublet* court provided little guidance

out additional evidence, this testimony is insufficient to authenticate the message. *See id.* at 822 ("[P]roving only that a message came from a particular account, without further authenticating evidence, has been held to be inadequate proof of authorship."). The *Sublet* court, in affirming the authentication of the Facebook messages sent in *Monge–Martinez*, relied heavily on testimony by Santa Maria, who claimed that she had received the messages in question and that they were sent by Monge–Martinez. *See Sublet*, 113 A.3d at 721. However, this authentication was based on a compilation of Santa Maria's testimony and other circumstantial evidence, including the style and language of the messages and the reference to events known only by a small number of people. *See id.* at 722 ("[I]n the case *sub judice* there is far more circumstantial evidence of Monge–Martinez's authorship than a bare assertion that he was the author.").

134. *See Sublet*, 113 A.3d at 718–19 (finding Sublet failed to overcome Parker's testimony denying authorship of posts at issue). In *Sublet*, the court gave great weight to Parker's denial of authorship of the disputed Facebook posts. *See id.* (noting denial of authorship "necessarily undercuts the notion of authenticity"). The court, in balancing the circumstantial evidence presented by Sublet against Parker's testimony, determined that Sublet did not present sufficient evidence to overcome Parker's testimony and thus was not properly authenticated. *See id.* at 719 ("No showing was made from which a reasonable juror could have found the pages to be authentic . . . .").

135. *See Campbell*, 382 S.W.3d at 551–52 (finding state presented sufficient evidence overcoming defendant's denial of authorship). In *Campbell*, the court began by noting that the defendant denied having sent the messages at issue, and then examined the additional circumstantial evidence to determine whether sufficient confirming circumstances existed to overcome defendant's claim. *See id.* (finding unique speech pattern and reference to incident and potential charges sufficient to overcome denial of authorship). When a dispute exists regarding authorship, the trial judge's responsibility is not to definitively rule on authorship, but to determine whether sufficient evidence is presented to tip the balance such that "the jury [is] entitled to weigh the credibility of [the] witnesses and decide who was telling the truth." *See id.* at 551; *see also Tienda*, 358 S.W.3d at 645–46 (holding proffered evidence sufficient to go to jury). In *Tienda*, the court recognized that it was "within the realm of possibility that the appellant was the victim of some elaborate and ongoing conspiracy," but noted that this "is an alternate scenario whose likelihood and weight the jury was entitled to assess . . . ." *See id.* at 645–46.

136. *See, e.g.*, Commonwealth v. Williams, 926 N.E.2d 1162, 1172 (Mass. 2010) (finding testimony by recipient, username, and profile picture insufficient to overcome party's denial of authorship; also noting need for more information regarding security of MySpace profile and ease at which third party could access account); *Campbell*, 382 S.W.3d at 551–52 (finding totality of circumstantial evidence sufficient to support rational jury finding that messages were authored by defendant). Additionally, according to one commentator, "[t]he current standard for authentication is low," and therefore the party proffering the contested evidence must only demonstrate sufficient proof such that a reasonable juror could find the evidence to be authentic. *See* Democko, *supra* note 7, at 401 ("A party seeking to admit evidence only needs to make a prima facie showing that it is what the party claims it to be.").

regarding the level of evidence sufficient for authentication in these situations, so courts in the future must seek to develop consistent rules regarding the necessary circumstantial evidence that will help lawyers and judges navigate the currently unsettled field.[137]

VI. *SUBLET* WRITES ON THE WALL FOR FUTURE COURT DECISIONS

Since the Maryland Court of Appeals decided *Sublet*, a number of other courts have decided cases in which a party attempted to introduce social media evidence.[138] Each of these courts explicitly or implicitly utilized a reasonable juror standard, yet varied in the type and amount of circumstantial evidence required for authentication.[139] This indicates a need for greater education and consistency surrounding social media and its use in litigation.[140] In particular, trial judges must have at least a basic understanding of major social media sites, including knowledge of how profiles are created and accessed, as well as how information is shared through the site, so that appropriate circumstantial evidence is admitted to authenticate social media evidence.[141]

137. *See Sublet*, 113 A.3d at 725 (Adkins, J., dissenting in part) ("[T]he Majority set bad precedent in holding that a trial judge can establish such a high bar for authentication as the court did in the *Sublet* case."). The dissent further criticized the majority's finding that the Facebook posts were not authenticated in *Sublet*, claiming "[t]he Majority muddled [the] 'reasonable juror' standard" and created precedent that will not clearly advance the law. *See id.*

138. *See, e.g.*, Wilson v. State, 30 N.E.3d 1264, 1269 (Ind. Ct. App. 2015) (holding username, pictures, content of Twitter profile sufficient to authenticate page); Boyd v. State, 175 So. 3d 1, 5–6 (Miss. 2015) (finding Facebook messages properly authenticated based on cell phone number sent in one message). In each of these cases, it can be inferred that the courts relied on the reasonable juror standard as a basis for authentication. *See Wilson*, 30 N.E.3d at 1268–69 ("[T]aken together, the witness testimony identifying the Twitter account as belonging to Wilson and the content posted on the account, including pictures and gang references, are more than sufficient to authenticate the Twitter posts as being authored by Wilson."); *Boyd*, 175 So. 3d at 6 ("[T]he Facebook messages were properly admitted considering the circumstances laid out here.").

139. *See supra* note 138 for evidence that *Boyd* and *Wilson* courts implicitly used reasonable juror standard.

140. *See* Fred Galves, *Where the Not-So-Wild Things Are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance*, 13 HARV. J.L. & TECH. 161, 275 (2000) (footnote in title omitted) (arguing for "formal and comprehensive educational program" for judges and court officials regarding new technologies). The rapid development of social media suggests that any rule presently developed "may be irrelevant in five years." *See* Democko, *supra* note 7, at 400, 405 (arguing education of judges and attorneys will support courts' efforts to keep up with the rapid development of social media and court participants in a better position to address social media authentication).

141. *See* Democko, *supra* note 7, at 405 ("Therefore, education, rather than a formal amendment, is the appropriate remedy and will ultimately prove more effective [to solve the issues surrounding social media authentication]."). Social media evidence presents unique issues regarding authorship; because anyone can make a profile using another person's information, a viewer can never be sure that a particular profile actually belongs to the purported owner. *See Campbell*, 382 S.W.3d at 550 ("[B]ecause anyone can establish a fictitious profile under any

The role of social media evidence in litigation will only continue to grow and develop, and courts will be faced with an infinite number of unique circumstances by which particular items of evidence may be authenticated.[142] Attorneys and judges must therefore continue to keep up with changes and developments in social media and be aware of the possible authentication issues that may arise.[143] Courts attempting to apply the reasoning of *Sublet* to future cases must recognize that, while the reasonable juror standard provides a proper baseline for social media authentication, the authenticity of each item of evidence must be based on its own unique facts and circumstances.[144]

Just as many courts have used the rules of evidence to determine authenticity of social media accounts, courts should consider applying either the state or federal version of Rule 403 of the Federal Rules of Evidence, which suggest that courts should apply a balancing test to determine whether the probative value of the evidence sufficiently outweighs the concerns regarding authorship.[145] Absent affirmative testimony by a post's

---

name, the person viewing the profile has no way of knowing whether the profile is legitimate."). Further, anyone can access another person's profile by gaining his or her username and password or, in many cases, merely by accessing the profile through the individual's cell phone or personal computer, which already has the password and username cached. *See id.* ("[B]ecause a person may gain access to another person's account by obtaining the user's name and password, the person viewing communications on or from an account profile cannot be certain that the author is in fact the profile owner."); *see also* State v. Eleck, 23 A.3d 818, 822 (Conn. App. Ct.) (noting social media users often store passwords on personal computers and cell phones, and allowing access even without entering password), *cert. granted mem. in part by* 30 A.3d 2 (Conn. 2011), *and aff'd on other grounds by* 100 A.3d 817 (Conn. 2014).

142. *See* Schoen, *supra* note 10 ("With increasing frequency, social media postings, including words, pictures, and other images, are becoming sources of evidence in a variety of cases."). In *Sublet*, the dissent stressed the likely increase of social media use in litigation. *See Sublet*, 113 A.3d at 725 (Adkins, J., dissenting in part) ("Use of social media as evidence in civil and criminal trials is likely to become increasingly important."). With over one billion people using social media worldwide, the potential issues that may arise in litigation are infinite. *See* Delaney & Heitner, *supra* note 2, at 11 (discussing statistics regarding number of Facebook users worldwide).

143. *See* Democko, *supra* note 7, at 405 (emphasizing need for further education in light of increased prevalence of social media in litigation).

144. *See Sublet*, 113 A.3d at 697–98 (applying reasonable juror standard to authentication). Because every case involving social media is unique, analysis of social media evidence must be context-specific and rely on relevant circumstantial evidence supporting authenticity. *See id.* at 715 ("[T]he preliminary determination of authentication must be made by the trial judge and 'depends upon a context-specific determination whether the proof advanced is sufficient to support a finding that the item in question is what its proponent claims it to be' . . . ." (quoting United States v. Vayner, 769 F.3d 125 (2d Cir. 2014))).

145. *See* FED. R. EVID. 403 ("The court may exclude relevant evidence if its probative value is substantially outweighed by a danger of one or more of the following: unfair prejudice, confusing the issues, misleading the jury . . . ."). Absent testimony by the post's creator, courts will have to rely on circumstantial evidence in determining whether a reasonable juror could find the post to be authentic.

creator, courts will always have to rely on some level of circumstantial evidence to determine the authenticity of a particular post.[146] A trial judge, in ruling on whether there is enough evidence for a jury to find that the alleged author actually wrote the post in question, should balance the value of the evidence against the strength of the circumstantial evidence to determine whether a reasonable juror could find the post to be authentic.[147] However courts decide to draw the line for authentication of social media evidence, one thing is obvious: a clearer standard is necessary.[148]

See, e.g., Tienda v. State, 358 S.W.3d 633, 638 (Tex. Crim. App. 2012) ("Evidence may be authenticated in a number of ways, including by . . . circumstantial evidence.").

146. *See* Burgess v. State, 742 S.E.2d 464, 467 (Ga. 2013) (permitting use of circumstantial evidence to authenticate MySpace posts). In *Burgess*, because the authorship of the particular posts was in question, the court relied on witness testimony and other evidence supporting the authentication of the MySpace profile. *See id.*

147. *See* Campbell v. State, 382 S.W.3d 545, 552 (Tex. Ct. App. 2012) ("[J]ury was entitled to weigh the credibility of these witnesses and decide who was telling the truth."). In *Campbell*, the court found that the state presented sufficient circumstantial evidence to surpass the necessary threshold showing to allow for a jury to make an ultimate determination regarding authentication. *See id.* at 553 ("[W]e conclude that there was prima facie evidence such that a reasonable jury could have found that the Facebook messages were created by Campbell."). The court noted that, while more than one scenario existed to explain the authorship of the particular messages, the proffered evidence was "within the zone of reasonable disagreement," such that it could be presented to the jury. *See id.* at 552 (quoting *Tienda*, 358 S.W.3d at 638) (internal quotation marks omitted).

148. *See Sublet*, 113 A.3d at 725 (Adkins, J., dissenting in part) ("The Majority muddled our 'reasonable juror' standard . . . ."); *see also Vayner*, 769 F.3d at 133 (noting social media authentication "will always depend on context"). While technological advances have led to questions of whether the Rules of Evidence should be amended, the existing rules "that have for many years governed the admissibility of evidence are more than adequate to the task." *See* Goode, *supra* note 10, at 63 (recognizing concerns regarding manipulation of electronic evidence and noting existing rules adequately address concerns). Indeed, because social media evidence is particularly susceptible to manipulation, courts must be especially aware of these susceptibilities and better articulate procedures for the amount and type of circumstantial evidence needed for authentication. *See, e.g.*, Parker v. State, 85 A.3d 682, 688 (Del. 2014) (finding circumstantial evidence adequate for authentication); *Tienda*, 358 S.W.3d at 647 (comparing circumstantial evidence to that presented in *Griffin v. State*, 19 A.3d 415 (Md. 2011) and finding greater "circumstantial indicia of authenticity" supporting prima facie authentication). In *Tienda*, the court compared the available evidence to that presented in *Griffin* and attempted to develop some consistency in the type and amount of circumstantial evidence needed for authentication. *See id.*