2014

The Social Medium: Why the Authenticantion Bar Should Be Raised for Social Media Evidence

Colin Miller
University of South Carolina - Columbia, mille933@law.sc.edu

TEMPLE LAW REVIEW ONLINE

VOL. 87 DECEMBER 2014

THE SOCIAL MEDIUM: WHY THE AUTHENTICATION BAR SHOULD BE RAISED FOR SOCIAL MEDIA EVIDENCE

Colin Miller[*] *& Charles White*[**]

I. INTRODUCTION

Tiffany Parker's trial started and ended with Facebook. On December 2, 2011, Parker fought with Sheniya Brown over Facebook messages regarding a mutual love interest.[1] Later that night, Parker allegedly posted entries on her Facebook page containing content such as "bet tht [sic] bitch didnt [sic] think [I] was going to see her ass . . . bet she wont [sic] inbox me no more, #caughtthatbitch."[2] After the jury rejected Parker's claim of self-defense and convicted her of second-degree assault, the sole basis for her appeal was that the prosecution failed to properly authenticate the Facebook entries as ones she had authored.[3]

In addressing the issue, the Delaware Supreme Court noted that courts have applied two conflicting approaches regarding the authentication of social media evidence. Most courts apply a traditional authentication standard based on the assumption "that the risk of forgery exists with any evidence."[4] Other courts, however, impose a higher authentication bar based on forgery concerns unique to social media evidence.[5] This Essay argues against the majority

* Associate Dean for Faculty Development & Associate Professor, University of South Carolina School of Law; Blog Editor, EvidenceProf Blog: http://lawprofessors.typepad.com/evidenceprof/.

** Student, University of South Carolina School of Law; J.D. expected, 2015.

1. Parker v. State, 85 A.3d 682, 683 (Del. 2014).
2. *Id.* at 684.
3. *Id.*
4. *Id.* at 686.
5. *Id.*

approach and in favor of a more stringent authentication standard for social media evidence.

II. AUTHENTICATION FRAMEWORK

Before a party can introduce evidence, it must first provide some indication that the evidence is what the party claims it to be, i.e., it must authenticate the evidence. For example, a prosecutor seeking to introduce a confession note allegedly written by the defendant must first present evidence that the defendant in fact wrote the letter. According to Federal Rule of Evidence 901(a),

> 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.[6]

This authentication standard is the same as the conditional relevance standard contained in Federal Rule of Evidence 104(b):[7] If a reasonable juror could find the conditional fact—authentication—by a preponderance of the evidence, Rule 901(a) has been satisfied.[8]

Rule 901(b), in turn, provides ten nonexhaustive illustrations of how a party can authenticate evidence. For example, Rule 901(b)(1) allows for authentication through testimony of a witness with knowledge. Under this Rule, any witness who saw the defendant write a confession note could authenticate the note as one written by the defendant. Meanwhile, Rule 901(b)(2) allows for authentication via nonexpert opinion about handwriting, which would allow for the defendant's wife, friend, or co-worker to authenticate a confession note based on familiarity with the way that the defendant "dots his i's and crosses his t's."[9] Furthermore, Rule 901(b)(3) would allow either a handwriting expert (or the trier of fact) to compare the confession note with a handwriting exemplar, or other writing indisputably written by the defendant, to establish that the same person wrote both.[10]

In other cases, the proponent can authenticate an exhibit through an accumulation of circumstantial evidence under Rule 901(b)(4). This Rule permits authentication through "[t]he appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances."[11]

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

7. *See* FED. R. EVID. 104(b) ("When the relevance of evidence depends on whether a fact exists, proof must be introduced sufficient to support a finding that the fact does exist. The court may admit the proposed evidence on the condition that the proof be introduced later.").

8. *See* United States v. Branch, 970 F.2d 1368, 1370 (4th Cir. 1992) (stating that authenticity is a question for the jury, and indicating that admissibility is governed by the procedure set forth in Federal Rule of Evidence 104(b)).

9. *See* FED. R. EVID. 901(b)(2) (providing that a person familiar with the handwriting may testify that it is genuine, provided that the knowledge was not "acquired for the current litigation").

10. *See* FED. R. EVID. 901(b)(3) (providing that "an authenticated specimen" may be used for comparison by an expert witness or the trier of fact).

11. FED. R. EVID. 901(b)(4).

For example, in *Hislop v. State*,[12] the prosecution used the following circumstantial evidence to authenticate a note which allegedly contained the defendant's confession to murdering his mother: (1) an officer found the note in the home shared by the defendant and his mother; (2) the note was underneath a billfold beside the couch on which the defendant was lying; (3) the billfold contained a second note in which the defendant asked his veterinarian to take care of his cat; and (4) the defendant's neighbor and paramedic both testified that the defendant confessed to stabbing his mother.[13] According to the Court of Appeals of Texas, "this combination of factors serve[d] to provide an adequate level of authentication to meet the initial criteria of Rule 901 and provide[d] the necessary condition precedent to admissibility."[14]

III. SOCIAL MEDIA EVIDENCE

According to the Delaware Supreme Court in *Parker v. State*,[15] "[s]ocial media has been defined as 'forms of electronic communications . . . through which users create online communities to share information, ideas, personal messages, and other content.'"[16] On social media sites such as Facebook and Twitter, a user can create a personal profile and post content, including text, pictures, and videos, which are available to Internet users at large and delivered to the author's subscribers.[17]

Attorneys are increasingly introducing social media evidence as exhibits at trial. For example, eighty-one percent of American Academy of Matrimonial Lawyers indicated in response to a survey that "they have seen an increase in the number of cases using social networking evidence during the past five years,"[18] with such evidence being used in an estimated ninety percent of divorce cases.[19] As a result, "[t]he authentication of social media evidence has become a prevalent issue in litigation today, creating much confusion and disarray for attorneys and judges."[20]

12. 64 S.W.3d 544 (Tex. App. 2001).

13. *Hislop*, 64 S.W.3d at 545–46.

14. *Id.* at 546.

15. 85 A.3d 682 (Del. 2014).

16. *Parker*, 85 A.3d at 685 (quoting Honorable Paul W. Grimm et al., *Authentication of Social Media Evidence*, 36 AM. J. TRIAL ADVOC. 433, 434 (2013)) (omission in original).

17. *Id.*

18. Press Release, Am. Acad. Matrimonial Law, Big Surge in Social Networking Evidence Says Survey of Nation's Top Divorce Lawyers (Feb. 10, 2010), http://www.aaml.org/about-the-academy/press/press-releases/e-discovery/big-surge-social-networking-evidence-says-survey-.

19. Janie Porter, *Facebook Used in 90 Percent of Divorce Cases*, WTSP NEWS, http://www.wtsp.com/news/article/189649/8/Facebook-used-in-90-percent-of-divorce-cases (last visited Nov. 11, 2014) (supporting that estimation with anecdotal evidence).

20. Grimm, *supra* note 16, at 433.

IV. THE AUTHENTICATION OF SOCIAL MEDIA EVIDENCE

A. The Business as Usual Approach

Confronted with social media evidence, most courts have applied the traditional approach to authentication, typically relying on Rule 901(b)(4). For instance, in *Tienda v. State*,[21] Ronnie Tienda, Jr. was charged with murdering David Valadez.[22] At trial, the prosecution introduced messages such as "I live to stay fresh!! I kill to stay rich!!" from three MySpace pages allegedly created by Tienda.[23] The trial court found that the prosecution properly authenticated this evidence under Rule 901(b)(4).[24] The Texas Court of Criminal Appeals later agreed, concluding that "the internal content of the MySpace postings—photographs, comments, and music—was sufficient circumstantial evidence to establish a prima facie case such that a reasonable juror could have found that they were created and maintained by the appellant."[25] The court acknowledged that Tienda could have been the victim of "malefactors" who created or hacked the MySpace pages, "somehow stole the appellant's numerous self-portrait photographs, [and] concocted boastful messages about David Valadez's murder and the circumstances of that shooting."[26] But the court concluded that these possibilities merely went to the weight of the evidence and not its admissibility.[27]

Later, in *Parker*, the Delaware Supreme Court relied on *Tienda* and Rule 901(b)(4) to find that the prosecution had properly authenticated Facebook entries in which Tiffany Parker allegedly boasted about attacking Sheniya Brown earlier in the day.[28] According to the court:

> First, the substance of the Facebook post referenced the altercation that occurred between Parker and Brown. Although the post does not mention Brown by name, it was created on the same day after the altercation and referenced a fight with another woman. Second, Brown's testimony provided further authenticating evidence. Brown testified that she viewed Parker's post through a mutual friend. Thereafter, Brown "shared" the post and published it on her own Facebook page. Collectively, this evidence was sufficient for the trial court to find that a reasonable juror could determine that the proffered evidence was authentic.[29]

21. 358 S.W.3d 633, 634 (Tex. Crim. App. 2012).

22. *Tienda*, 358 S.W.3d at 634.

23. *Id.* at 635.

24. *Id.* at 637.

25. *Id.* at 641–42.

26. *Id.* at 645–46.

27. *Id.* at 646; *see also* State v. Assi, No. 1 CA-CR 10-0900, 2012 WL 3580488 (Ariz. App. 2012) (finding that the defendant's arguments about the authenticity of MySpace evidence went to weight and not admissibility).

28. 85 A.3d 682, 686–87 (Del. 2014) (citing FED. R. EVID. 901(b)(4); *Tienda*, 358 S.W.3d at 633).

29. *Id.* at 688.

B. The Stricter Approach

Other courts have raised the authentication bar in cases involving social media evidence. In *Smith v. State*,[30] Scott Smith was convicted of capital murder in connection with the death of his wife's seventeen-month-old daughter, Ally.[31] At trial, the prosecution had admitted Facebook messages allegedly authored by Smith concerning his problems with his wife and her daughter, such as, "[I] feel my temper building and [I] know [I] will hurt someone, they are playing with fire and have no clue."[32] The trial court deemed these messages authenticated under Mississippi Rule of Evidence 901(b)(4), relying on Smith's wife's allegation that the page belonged to him, the fact that the Facebook page was created by "Scott Smith," and the fact that it contained a photograph of Smith.[33]

The Supreme Court of Mississippi later reversed, finding that "[t]he authentication of social media poses unique issues regarding what is required to make a prima facie showing that the matter is what the proponent claims."[34] Specifically, the court observed that "[t]he ease with which defendants and alleged victims alike could fabricate a social media account to corroborate a story necessitates more than a simple name and photograph to sufficiently link the communication to the purported author under Rule 901."[35]

The Court of Appeals of Maryland reached a similar conclusion in *Griffin v. State*.[36] In *Griffin*, Antoine Griffin, also known by the nickname "Boozy," was charged with various crimes in connection with the shooting death of Darvell Guest.[37] At trial, the State sought to prove that the defendant's girlfriend, Jessica Barber, threatened a witness for the prosecution by posting on her MySpace page, "FREE BOOZY!!!! JUST REMEMBER SNITCHES GET STITCHES!! U KNOW WHO YOU ARE!!"[38] The trial court found that the prosecution properly authenticated the MySpace page, and the Court of Special Appeals of Maryland agreed, finding that Barber's "photograph, personal information, and references to freeing 'Boozy'" satisfied Maryland Rule of Evidence 5-901(b)(4).[39]

The Court of Appeals of Maryland reversed, noting that "[t]he potential for fabricating or tampering with electronically stored information on a social networking site . . . poses significant challenges from the standpoint of authentication of printouts of the site."[40] Specifically, the court concluded that

> [t]he potential for abuse and manipulation of a social networking site

30. 136 So.3d 424 (Miss. 2014).
31. *Smith,* 136 So.3d at 426–27.
32. *Id.* at 430 (alterations in original).
33. *Id.* at 433–35.
34. *Id.* at 432, 435.
35. *Id.* at 433–344.
36. 19 A.3d 415 (Md. 2011).
37. *Griffin*, 19 A.3d at 417–18.
38. *Id.* at 418.
39. *Id.* at 423.
40. *Id.* at 422–424.

> by someone other than its purported creator and/or user leads to our conclusion that a printout of an image from such a site requires a greater degree of authentication than merely identifying the date of birth of the creator and her visage in a photograph on the site.[41]

The Court of Appeals of Maryland then suggested three nonexhaustive ways in a which a party could authenticate social media evidence: (1) testimony by the alleged creator of the website that she actually created the page and posted the disputed content, (2) evidence obtained from a search of the Internet history and hard drive of the alleged author's computer, and (3) information directly obtained from the relevant social networking website.[42]

V. RAISING THE BAR

The split of authority acknowledged by the Delaware Supreme Court in *Parker* also suggests the test that should be used for determining whether the authentication bar should be raised for social media evidence: If the risk of forgery with social media evidence is similar to the forgery risk for other evidence, and if the circumstantial evidence typically used to authenticate exhibits under Rule 901(b)(4) is similarly able to quell concerns regarding that risk, the authentication bar should not be raised.[43] But if there is a higher forgery risk with social media evidence, or if the typical circumstantial evidence does not alleviate doubts concerning social media authorship, the authentication bar should be raised.[44]

A. The Higher Forgery Risk Associated With Social Media Evidence

Assume the prosecution claims that the defendant handwrote a confession note, while the defendant claims that the note is a forgery. How easy will it be to determine whether the note was forged? The Advisory Committee Note to Federal Rule of Evidence 901 indicates that "[t]he common law approach to authentication of documents has been criticized . . . as one which . . . present[s] only a slight obstacle to the introduction of forgeries."[45] But the Advisory Committee rejects that concern and notes that "significant inroads upon the traditional insistence on authentication and identification have been made by accepting as at least prima facie genuine items of the kind treated in Rule 902."[46]

Federal Rule of Evidence 902 in turn allows for the self-authentication of twelve types of evidence, meaning that "they require no extrinsic evidence of authenticity in order to be admitted."[47] The Advisory Committee Note accompanying Rule 902 indicates that the Rule is premised on the belief "that

41. *Id.* at 424.

42. *Id.* at 427–28.

43. Parker v. State, 85 A.3d 682, 686–88 (Del. 2014).

44. *See id.* at 688 (noting that the Rule 104 standard is only appropriate if the trial judge determines that the jury has enough facts to evaluate the authenticity of the proposed evidence).

45. FED. R. EVID. 901 advisory committee note.

46. *Id.*

47. FED. R. EVID. 902.

forgery is a crime and detection is fairly easy and certain."[48] In other words, the authentication structure erected by the Federal Rules of Evidence is based upon the foundational belief that the detection of forgeries is not only easy, but certain. This supposition is borne out by the multitude of cases in which handwriting experts testify that "forgeries [a]re easy to detect."[49] These experts frequently use "[c]omputer-based handwriting analysis systems," and "[t]hese systems have shown to be capable of detecting 100% of random and simple forgeries and over 90% of skilled forgeries."[50]

Conversely, it is uniquely easy to create, and difficult to detect, social media forgeries. On most social media websites, a user can create an account by simply providing a "name, home address, e-mail address, age, sex, location, and birth date,"[51] and "[t]he fact that a user profile is entirely self-generated can lead to significant mischief and presents an interesting conundrum for law enforcement."[52] Because "fragments of information, either crafted under our authority or fabricated by others, are available by performing a Google search . . . forever," it does not take much for anyone with Internet access to create a convincing fake Facebook or Twitter profile for someone he barely knows.[53] Moreover, "[b]ecause social media is often stored on remote servers, is assessed through unique interfaces, can be dynamic and collaborative in nature, and is uniquely susceptible to alteration and fabrication, evidentiary standards developed for other types of electronically stored information [ESI] may not be adequate."[54]

In addition, it is exceptionally easy to hack into another person's social media account.[55] Such a feat usually consists of simply coming up with the other person's password, which can be accomplished by something as simple as a guess or more complex methods like a password-guessing tool, social engineering, phishing, and spoofing.[56] In the end, the proof of the ease of social media hacking is largely in the pudding. First, there have been a number of "hacks" of

48. FED. R. EVID. 902 advisory committee note.

49. *E.g.*, Eason Publ'n, Inc. v. Nationsbank of Georgia, 458 S.E.2d 899, 901 (Ga. Ct. App. 1995).

50. Bryan Found., Doug Rogers & Robert Schmittat, '*Matrix Analysis': A Technique to Investigate the Spatial Properties of Handwritten Images*, 11 J. FORENSIC DOCUMENT EXAMINATION 51, 52–53 (1998).

51. Nathan Petrashek, Comment, *The Fourth Amendment and the Brave New World of Online Social Networking*, 93 MARQ. L. REV. 1495, 1499 n.16 (2010).

52. *Id.*

53. David Hector Montes, *Living Our Lives Online: The Privacy Implications of Online Social Networking, Journal of Law and Policy for the Information Society*, J. L. & POL'Y FOR INFO. SOC'Y, Spring 2009, at 508.

54. H. Christopher Boehning & Daniel J. Toal, *Authenticating Social Media Evidence*, N.Y.L.J., Oct. 2, 2012, at para. 4.

55. Kathryn Kinnison Van Namen, Comment, *Facebook Facts and Twitter Tips—Prosecutors and Social Media: An Analysis of the Implications Associated with the Use of Social Media in the Prosecution Function*, 81 MISS. L.J. 549, 565 (2012).

56. *See* Michael Brittain & K. James Sullivan, *5 Principles for Minimizing the Likelihood and Effects of Cyber Attacks*, WESTLAW J. COMPUTER & INTERNET, October 19, 2012, at 2 (2012).

high profile Twitter accounts in recent years.[57] Second, many recent "cases in which romantic partners have accessed social networking accounts illustrate the susceptibility of social media accounts to security breaches."[58]

B. The Impracticality of Standard Rule 901(b)(4)

Such concerns about social media forgery might be acceptable if courts applied an admissibility standard that substantially quelled concerns about authenticity. As noted, courts typically allow for the authentication of social media evidence under Rule 901(b)(4).[59] The problem is that, as currently applied, 901(b)(4) is an analog rule in a digital world.

The Advisory Committee Note to Rule 901(b)(4) proffers three ways in which the characteristics of the offered item itself allow for authentication.

1. Peculiar Knowledge

First, "a document or telephone conversation may be shown to have emanated from a particular person by virtue of its disclosing knowledge of facts known peculiarly to him."[60] As support for this proposition, the Advisory Committee cites *Globe Automatic Sprinkler Co. v. Braniff*.[61]

In *Braniff*, T.E. Braniff brought an action against the Globe Automatic Sprinkler Company, seeking to recover a commission he was owed for securing a contract for the installation of a sprinkler system.[62] The lawsuit hinged on the authenticity of a letter the defendant allegedly wrote, offering to pay Braniff a ten percent commission on the installation of any sprinkler systems installed pursuant to contracts he assisted the defendant in procuring.[63] The Supreme Court of Oklahoma found that the letter was properly authenticated because "[t]he contents of the letter related to facts peculiarly within the knowledge of the defendant's agents and employees, and for the letter to have been written by any person other than the defendant would have been a most unusual and extraordinary thing to have happened."[64]

In the 21st century, however, the extraordinary has become ordinary, and

57. Julianne Pepitone, *AP Hack Proves Twitter Has a Serious Cybersecurity Problem*, CNNMONEY (April 23, 2013, 3:23 PM), http://money.cnn.com/2013/04/23/technology/security/ap-twitter-hacked/index.html.

58. Smith v. State, 136 So.3d 424, 435 (Miss. 2014); *see, e.g.*, Campbell v. State, 382 S.W.3d 545, 552 (Tex. App. 2012) (reviewing evidence relating to Facebook account access for the defendant and his girlfriend, the victim); Simmons v. Commonwealth, No. 2012-SC-000064-MR, 2013 WL 674721, at *1 (Ky. Feb. 21, 2013) (discussing law enforcement obtaining sexually suggestive messages between an adult and a middle-school student, because the adult's girlfriend accessed his Facebook account when he ended their relationship).

59. See *supra* Part IV.A for a discussion of the authentication of social media evidence using FED. R. EVID. 901(b)(4).

60. FED. R. EVID. 901(b)(4) advisory committee note.

61. *Id.* (citing Globe Automatic Sprinkler Co. v. Braniff, 214 P. 127 (Okla. 1923)).

62. *Braniff*, 214 P. at 128.

63. *Id.*

64. *Id.* at 129.

the notion that many facts are peculiarly in the knowledge of a single person or small group of people seems quaint. And yet, many courts deem social media postings authenticated based upon the assumption of such private knowledge.[65] In *State v. Bell*,[66] the Court of Common Pleas of Ohio allowed for the authentication of MySpace messages in part because they allegedly "contain[ed] code words known only to defendant and his [two] alleged victims."[67] Before it was reversed by the Court of Appeals of Maryland, the Court of Special Appeals of Maryland found in *Griffin* that the "SNITCHES GET STITCHES" post was properly authenticated by facts peculiarly in the knowledge of Griffin's girlfriend: her birthdate, the fact that she had two children with Griffin, and the fact that Griffin went by the name "Boozy."[68]

Additionally, as was the case for Tiffany Parker, Travis Campbell's case started and ended with Facebook. On February 26, 2011, Campbell became angry when he saw that his friend had sent a Facebook message to his girlfriend, and Campbell allegedly assaulted his girlfriend the next day.[69] On March 2, Campbell allegedly sent his girlfriend three Facebook messages, including one that stated, "please help me ana i cry every day i am so f—ing stuppid [sic] for hurthig [sic] u i am guilty what was I thinking please message me tell me your mind let me talk please, I am so ashame [sic]."[70] The Court of Appeals of Texas, Austin, found that these messages were properly authenticated in part because "the messages reference the incident and potential charges, which at the time the messages were sent, few people would have known about."[71]

In order for any of these rulings to hold water, it would have to be extraordinary for anyone other than the alleged social media author to have the relevant knowledge. In *Bell*, this was an impossibility because neither of the defendant's two alleged victims could have sent the MySpace messages; alternately, if either the defendant or the victims used the "code words" around other people or anywhere online, the knowledge would no longer have been known peculiarly to them.[72] In *Griffin*, as the Court of Appeals of Maryland acknowledged, any number of people could have known the birth date of Griffin's girlfriend, the fact that Griffin and she had two children together, and the fact that Griffin went by the nickname "Boozy."[73] Moreover, in Campbell,

65. See *supra* Part III for a discussion of cases in which an assumption of private knowledge was a factor in authenticating social media evidence.

66. 882 N.E.2d 502 (Ohio C.P. 2008).

67. *Bell,* 882 N.E.2d at 68.

68. Griffin v. State, 995 A.2d 791, 806–07 (Md. Ct. Spec. App. 2010)*; see also* Michelle Sherman, *The Anatomy of a Trial with Social Media and the Internet*, 14 J. INTERNET L. 1, 13–14 (2011) (discussing the court's reasoning in *Griffin*).

69. Campbell v. State, 382 S.W.3d 545, 547 (Tex. App. 2012).

70. *Id.* at 551.

71. *Id.* at 552.

72. *See* State v. Bell, 882 N.E.2d 502, 512 (Ohio C.P. 2008) (noting electronic communications were authenticated in part because they contained code words known only to the defendant and his alleged victims).

73. Griffin v. State, 19 A.3d 415, 423–24 (Md. 2011).

four days had passed between the assault and the Facebook messages.[74] Four days is more than enough time for a number of people to learn about the attack, especially given that Campbell, his girlfriend, and his friend all had Facebook accounts.

All of these cases reinforce the reality that we live in a brave new digital world in which "almost nothing is private."[75] Moreover, once information is posted online, the word "almost" can be removed from the previous sentence.[76] Thus, it seems appropriate to raise the bar on exactly what type of "peculiar knowledge" that allows for an inference of authentication under Rule 901(b)(4).

For instance, in *State v. Eleck*,[77] Simone Judway testified as a witness for the prosecution that Robert Eleck told her "if anyone messes with me tonight, I am going to stab them" soon before he allegedly stabbed the victim.[78] On cross-examination, Judway claimed that she had not spoken to Eleck in person, by telephone, or by computer since the incident, prompting the defense to seek to impeach her through Facebook messages allegedly exchanged between Eleck and Judway after the incident.[79] One such exchange addressed the prior acrimonious relationship between the two:

> Simone Danielle: Hey I saw you the other day and I just want to say nice bike.
>
> [The Defendant]: why would you wanna talk to me
>
> Simone Danielle: I'm just saying that you have a nice bike that's all. The past is the past.[80]

The "Simone Danielle" Facebook account indisputably belonged to Judway, but Judway claimed that the account was hacked, and the Connecticut Appellate Court found that the messages could not be authenticated, thus indicating that Eleck failed to satisfy the peculiar knowledge standard.[81] Specifically, the court was

> not convinced that the content of this exchange provided distinctive evidence of the interpersonal conflict between the defendant and Judway. To the contrary, this exchange could have been generated by any person using Judway's account as it does not reflect distinct information that only Judway would have possessed regarding the

74. *Campbell*, 382 S.W.3d at 553.

75. Charles E. MacLean, Katz *on a Hot Tin Roof: The Reasonable Expectation of Privacy Doctrine is Rudderless in the Digital Age, Unless Congress Continually Resets the Privacy Bar*, 24 ALB. L.J. SCI. & TECH. 47, 58 (2014).

76. Sarah L. Gottfried, Note, *Virtual Visitation: The New Wave of Communication Between Children and Non-Custodial Parents in Relocation Cases*, 9 CARDOZO WOMEN'S L.J. 567, 592 (2003) ("[N]othing is private over the Internet").

77. 23 A.3d 818 (Conn. App. Ct. 2011).

78. *Eleck,* 23 A.3d at 820.

79. *Id.*

80. *Id.* at 820 n.2.

81. *See id.* at 824 (stating that "this exchange could have been generated by any person using Judway's account as it does not reflect distinct information that only Judway would have possessed regarding the defendant or the character of their relationship").

> defendant or the character of their relationship. In other cases in which a message has been held to be authenticated by its content, the identifying characteristics have been much more distinctive of the purported author and often have been corroborated by other events or with forensic computer evidence.[82]

Eleck reflects the reality of modern communications and the fact that peculiar knowledge is truly peculiar in the social media realm. Accordingly, courts should rely on something more than broad biographical data or the fact that "mere days" have passed since a crime to conclude that such facts are peculiarly within the knowledge of the alleged author of a social media post.

2. "Reply Letter" Doctrine

Second, the Note to Rule 901(b)(4) indicates that "a letter may be authenticated by content and circumstances indicating it was in reply to a duly authenticated one."[83] In order for this "reply letter" doctrine to apply, the proponent must "prove that the first letter was dated, was duly mailed at a given time and place, and was addressed to [the sender of the reply-letter]."[84] Thus, in *National Paralegal Institute Coalition v. Commissioner*,[85] the government was able to authenticate a "reply letter" written by the petitioner by establishing that it was a response to a dated letter sent to the petitioner's address.[86]

In some cases involving the authentication of social media evidence, however, courts have tried to extend this reply letter doctrine to a new medium—the social medium —that is less hospitable to this type of authentication. For instance, in *Parker*, the Delaware Supreme Court primarily found that Tiffany Parker's Facebook posts were authenticated because the victim viewed Parker's post through a mutual friend and shared the post by publishing it on her own Facebook page.[87] Meanwhile, in *Smith*, the Supreme Court of Mississippi found that the prosecution had not properly authenticated Facebook messages only after disagreeing with the Court of Appeals' conclusion that the defendant's messages were replies to his girlfriend's Facebook message.[88]

These cases illustrate at least two problems with applying a liberal version of the "reply letter" doctrine to social media evidence. Under the traditional "reply letter" doctrine, a reply is authenticated in two ways by reference to an original letter: (1) the original letter was sent to the alleged author's house, and (2) the "reply letter" replies to the content of the original letter.[89] In these cases,

82. *Id.*

83. FED. R. EVID. 901(b)(4) advisory committee note.

84. 2 KENNETH S. BROUN ET AL., MCCORMICK ON EVIDENCE § 224 at 95 (7th ed. 2013).

85. 90 T.C.M. (CCH) 623 (T.C. 2005).

86. *Nat'l Paralegal Inst.,* 90 T.C.M. (CCH) at 625.

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

88. Smith v. State, 136 So.3d 424, 435 (Miss. 2014) ("[I]t does not appear that Smith's messages are replying to anything in Waldrop's message.").

89. *See* BROUN ET AL., *supra* note 84, § 224 at 94–95 (discussing the method of authentication under the "reply letter" doctrine).

the fact that the original letter was sent to the alleged author's house can be proven through a deed, mortgage, or rental agreement, and authenticity is established through the unlikelihood that someone else intercepted the original letter and forged a response.[90]

Conversely, because social media websites do not have similar property records, and because such sites are created from user-generated data that can be culled from quick Internet searches, courts in cases like *Parker* and *Smith* are using the content of posts to establish ownership. In *Parker*, there was nothing tying Tiffany Parker to the disputed Facebook page besides her picture and the name "Tiffanni Parker."[91] And in *Smith*, the girlfriend "did not testify as to how she knew that the Facebook account was Smith's, nor did she testify as to how she knew that Smith actually authored the Facebook messages."[92]

Courts such as the *Parker* court also seem to fail to grasp the way that social media websites work in applying the "reply letter" doctrine. For a reply to a snail-mail letter to come from someone other than the addressee, the imposter would have to burglarize the post office or pilfer the letter from the addressee's mailbox. On the other hand, Facebook messages can be copied or re-shared by anyone who can see them, which is usually anyone with a Facebook account, even if the user attempts to keep the information private.[93] Therefore, the fact that the victim in *Parker* saw the Facebook messages on her friend's page and shared them on her own page says nothing more than that the victim thought Parker's Facebook page was authentic.

One of the few courts to recognize the problems with applying a liberal version of the "reply letter" doctrine to social media evidence was the Supreme Judicial Court of Massachusetts in *Commonwealth v. Purdy*.[94] In *Purdy*, the court noted the existence of the "reply letter" doctrine but found that evidence "that the electronic communication originates from . . . a social networking Web site such as Facebook or MySpace that bears the defendant's name is not sufficient alone to authenticate the electronic communication as having been authored or sent by the defendant."[95] That said, the court ultimately found authentication of the messages at issue based upon other evidence such as data recovered from the hard drive of the defendant's computer.[96] In *Eleck*, the Appellate Court of Connecticut applied similar reasoning but found that the reply letter doctrine could not be used to authenticate Facebook messages

90. *See, e.g.*, Commonwealth v. Brooks, 508 A.2d 316, 319–320 (Pa. Super. Ct. 1986) (noting that a writing can be authenticated by circumstantial evidence that may take a number of forms, including evidence of events preceding or following the execution of the delivery of the writing).

91. *Parker*, 85 A.3d at 684.

92. *Smith*, 136 So.3d at 434.

93. Kathryn R. Brown, Note, *The Risks of Taking Facebook at Face Value: Why the Psychology of Social Networking Should Influence the Evidentiary Relevance of Facebook Photographs* 14 VAND. J. ENT. & TECH. L. 357, 363 n.33 (2012) (citing *Data Use Policy*, FACEBOOK, https://www.facebook.com/full_data_use_policy).

94. 945 N.E.2d 372 (Mass. 2011).

95. *Purdy*, 945 N.E.2d at 381 (citing Commonwealth v. Williams, 926 N.E.2d 1162 (2010)).

96. *Id.*

because "there was a lack of circumstantial evidence to verify the identity of the person with whom the defendant was messaging."[97]

Given the difference between a house and a website, courts should apply something approximating the more rigorous analysis utilized by the courts in *Purdy* and *Eleck*. It should not be enough that the alleged author replied to a social media post; instead, courts should require additional evidence that links the alleged author to the message.

3. Language Patterns

Third, the Note to Rule 901(b)(4) states that "[l]anguage patterns may indicate authenticity or its opposite."[98] As support for this proposition, the Committee cites *Magnuson v. State*,[99] a case in which a Swedish native was charged with the bombing death of a victim in Marshfield, Wisconsin.[100] The wrapper on the bomb was preserved, and, on it, "[t]he word 'Marshfield' was misspelled, being written 'Marsfilld,' the 'h' and 'e' being omitted."[101] The Wisconsin Supreme Court observed that at trial the bomb wrapper was authenticated as written by the defendant because (1) a professor "testified that this spelling was characteristic of one familiar with the Swedish language as was also the pronunciation 'Mars' for 'Marsh,'" and (2) the defendant was the only person with known enmity against the victim and "the only person of Swedish nationality in the district."[102] Because the bomb was sent locally in a package in the mail, the court concluded that it was likely the defendant who sent it.[103]

Many courts today use similar analysis to authenticate social media evidence. In *Campbell*, the court found the defendant's Facebook messages were authenticated in large part because "the unique speech pattern presented in the messages [wa]s consistent with the speech pattern that Campbell, a native of Jamaica, used in testifying at trial."[104] Meanwhile, in *Tienda*, the Texas Court of Criminal Appeals used the appellant's alleged three MySpace pages as "ample circumstantial evidence—taken as a whole with all of the individual, particular details considered in combination—to support a finding that the MySpace pages belonged to the appellant and that he created and maintained them."[105]

Again, there are at least a few problems with applying this analysis to social media evidence. First, in *Magnuson*, the defendant could be singled out as the bomb's sender because he was the only person of Swedish nationality in the subject community.[106] Conversely, in a case like *Campbell*, the relevant

97. State v. Eleck, 23 A.3d 818, 825 (Conn. App. Ct. 2011).

98. FED. R. EVID. 901(b)(4) advisory committee note.

99. 203 N.W. 749 (Wis. 1925).

100. *Magnuson*, 203 N.W. at 750.

101. *Id.*

102. *Id.*

103. *See id.* at 750.

104. Campbell v. State, 382 S.W.3d 545, 551–52 (Tex. App. 2012).

105. Tienda v. State, 358 S.W.3d 633, 645 (Tex. Crim. App. 2012).

106. *Magnuson,* 203 N.W. at 750.

community is the online community, where there are millions of people of Jamaican nationality. This issue, of course, could partially be remedied by two of the solutions proposed in *Griffin*: obtaining data from the alleged author's hard drive or the social media website.[107]

Second, anyone with Internet access can view every tweet that a person has tweeted and most content that a Facebook user has posted, making a "pattern" analysis more problematic.[108] Indeed, "social media websites are designed to share information with others," and even information that a user intends to keep private is almost always publicly accessible.[109]

In 1925, the *Magnuson* court could conclude that it was unlikely that somebody else mimicked the way that a person of Swedish decent might communicate; in *Campbell*, anyone with Internet access could have viewed Campbell's Facebook content and created similar-looking content if they had access to his account. Indeed, Campbell's girlfriend admitted at trial that she once had access to Campbell's Facebook account, although she claimed that he changed his password before he assaulted her.[110]

Similarly, the defendant in *Tienda* might in fact have created three separate MySpace pages; alternately, a "malefactor" could have viewed all of the content on the defendant's legitimate MySpace page and created a fake page, or pages, similar to the genuine article in form and substance. Appreciating these concerns, the court in *Eleck* refused to find authentication of a Facebook page where there was evidence of a subsequent hacking of the page because the hacking "highlight[ed] the general lack of security of the medium and raise[d] an issue as to whether a third party may have sent the messages."[111]

Eleck should not be read for the proposition that a pattern analysis can never be used to authenticate particular social media content given the lack of security of the format. But, if a case features evidence of prior or subsequent hacking, multiple accounts on the same platform, or access by an interested third party, the proponent should have to present evidence of something beyond consistency among posts or the ethnic background of the alleged author.

VI. CONCLUSION

Courts are increasingly at a crossroads with regard to the authentication of social media evidence. Most courts cling to the belief that the risk of social media forgery is no different that the forgery risk with other types of evidence and continue to apply an authentication standard put in place when the "written word" was still primarily written. A few courts, however, are beginning to recognize that Rule 901(b)(4) is an analog rule in a digital world that must be

107. Griffin v. State, 19 A.3d 415, 427–28 (Md. 2011).

108. Brian M. Molinari, *When Online Behavior Becomes a Real-World Problem*, 16 N.Y. EMP. L. LETTER, no. 9, 2009, at 1.

109. Agnieszka A. Mcpeak, *The Facebook Digital Footprint: Paving Fair and Consistent Pathways to Civil Discovery of Social Media Data*, 48 WAKE FOREST L. REV. 887, 928–29 (2013).

110. *Campbell*, 382 S.W.3d at 551.

111. State v. Eleck, 23 A.3d 818, 824 (Conn. App. Ct. 2011).

ratcheted up to address an online world where nothing is private and a medium—the social medium—where user profiles are self-generated and highly susceptible to hacking. This essay is a first attempt to address how to raise the bar on the authentication of social media evidence.