Catholic University Law Review

Volume 62
Issue 1 *Fall 2012*

Article 6

2012

The Return of "Voodoo Information": A Call to Resist a Heightened Authentication Standard for Evidence Derived from Social Networking Websites

Richard Fox

The Return of "Voodoo Information": A Call to Resist a Heightened Authentication Standard for Evidence Derived from Social Networking Websites

Cover Page Footnote

J.D. Candidate, May 2013, The Catholic University of America, Columbus School of Law; B.A., 2006, Boston University. The author wishes to thank Hans Moore for his perspective from the trenches, as well as the staff and editors of the Catholic University Law Review, whose comments and edits were indispensable. The author also wishes to thank his family, particularly his mother, Carol, whose love and support made him the man he is. Finally, thank you, Sarah, for making me a better man every day.

THE RETURN OF "VOODOO INFORMATION": A CALL TO RESIST A HEIGHTENED AUTHENTICATION STANDARD FOR EVIDENCE DERIVED FROM SOCIAL NETWORKING WEBSITES

Richard W. Fox[+]

> Plaintiff's electronic 'evidence' is totally insufficient. . . . [T]he Court continues to warily and wearily view [the Internet] largely as one large catalyst for rumor, innuendo, and misinformation. . . . [A]ny evidence procured off the Internet is adequate for almost nothing. . . . Instead of relying on the voodoo information taken from the Internet, Plaintiff must hunt for hard copy back-up documentation in admissible form. . . .[1]

This quote, from Federal District Court Judge Samuel Kent in 1999, roughly coincides with the dawn of the Internet era.[2] Eight years later, this same judge presided over a case in which he used a "quick search on the [I]nternet" to hold that it would not be prohibitively expensive for plaintiffs to fly from Ecuador to San Diego to attend court.[3] Is this judge being hypocritical, or does he simply no longer believe that the Internet is "voodoo information" that is "adequate for almost nothing"?[4]

Judge Kent's attitude is not unique among American jurists who are skeptical of evidence derived from new forms of technology.[5] Judges have expressed this attitude in opinions concerning the admissibility of audio

---

[+]J.D. Candidate, May 2013, The Catholic University of America, Columbus School of Law; B.A., 2006, Boston University. The author wishes to thank Hans Moore for his perspective from the trenches, as well as the staff and editors of the *Catholic University Law Review*, whose comments and edits were indispensable. The author also wishes to thank his family, particularly his mother, Carol, whose love and support made him the man he is. Finally, thank you, Sarah, for making me a better man every day.

1. St. Clair v. Johnny's Oyster & Shrimp, Inc., 76 F. Supp. 2d 773, 774–75 (S.D. Tex. 1999).

2. *See* Andrew C. Payne, Note, *Twitigation: Old Rules in A New World*, 49 WASHBURN L.J. 841, 844 (2010) ("In the late 1990s and early 2000s, companies jumped on the Internet bandwagon and put their full faith in e-commerce.").

3. Tobar v. United States, No. G-07-003, 2007 WL 1296717, at *1 n.1, 2 (S.D. Tex. Apr. 30, 2007).

4. *St. Clair*, 76 F. Supp. 2d at 775; *see also* Steven Goode, *The Admissibility of Electronic Evidence*, 29 REV. LITIG. 1, 66 n.14 (2009) (noting the inconsistency in Judge Kent's opinions on the evidentiary value of the information procured from the Internet).

5. Goode, *supra* note 4, at 4 ("Our jurisprudence is littered with examples of courts confronting the admissibility of evidence based on new technologies, and courts have reacted in a predictable pattern. At first, new technologies meet with judicial resistance.").

recordings,[6] photographs,[7] motion pictures,[8] and computer generated business records.[9] As the prevalence and judicial acceptance of these technologies have grown, courts have lowered the barriers to admissibility.[10]

As exemplified by Judge Kent, judicial treatment of electronic evidence[11] appears to mirror the same pattern as other forms of new technological evidence: initial recalcitrance followed by begrudging acceptance.[12] However, what has not yet become apparent is whether evidence derived from social networking websites[13] will also follow this trend.[14] The manner in which courts will handle this issue is significant for a number of reasons. First, society's practice of posting personal information on social networking sites[15] has led a growing number of litigators to search these sites for evidence.[16] However, the time and effort spent searching these sites is useless if uncovered

---

6. *See* Goode, *supra* note 4, at 4 (quoting State v. Simon, 174 A. 867, 872 (N.J. Sup. Ct. 1934), *aff'd*, 178 A. 728 (N.J. 1935)) ("We know of no case, and counsel cite none, in which a phonograph record of an alleged conversation was admitted in a court of law as evidence thereof.")).

7. *See id.* (quoting Cunningham v. Fair Haven & W. R. Co., 43 A. 1047, 1049 (Conn. 1899)) (excluding photographic evidence and noting that "either through want of skill on the part of the artist, or inadequate instruments or materials, or through intentional and skillful manipulation, a photograph may be not only inaccurate, but dangerously misleading").

8. *See id.* at 4 n.8 (quoting JORDAN S. GRUBER, ELECTRONIC EVIDENCE § 8:1 (1995)) (explaining that "[m]otion pictures were at first often objected to, and sometimes excluded, because they were said to provide ample opportunity for fabrication, falsification, or distortion.").

9. United States v. Scholle, 553 F.2d 1109, 1125 (8th Cir. 1977) (upholding the trial court's admission of computer generated business records, but noting that "the complex nature of computer storage" requires controls that assure accuracy and reliability).

10. *See* Goode, *supra* note 4, at 4.

11. For the purposes of this Comment, "electronic evidence" is defined as "information stored or transmitted in digital form that a party to a legal action may use to further his or her case." John S. Wilson, *MySpace, Your Space, or Our Space? New Frontiers in Electronic Evidence*, 86 OR. L. REV. 1201, 1204 (2007).

12. Goode, *supra* note 4, at 4–6.

13. The phrase "evidence derived from social networking websites," will hereinafter be referred to as "social networking evidence."

14. *See* Katherine Minotti, *The Advent of Digital Diaries: Implications of Social Networking Web Sites for the Legal Profession*, 60 S.C. L. REV. 1057, 1070 (2009) (observing that there is no consensus on whether information from social networking websites should be admitted as evidence).

15. For example, as of June 2012, Facebook had 955 million active users and 522 million daily active users. *Key Facts*, FACEBOOK NEWSROOM, http://newsroom.fb.com/content/default.aspx?NewsAreaId=22 (last visited Sept. 27, 2012).

16. *See* Minotti, *supra* note 14, at 1059 (citing Vesna Jaksic, *Litigation Clues Are Found on Facebook: Lawyers Use Social Networks as a Tool*, 30 NAT'L L.J. 1, 1 (2007)) (noting that prosecutors have used social networking sites to "prove a defendant's subsequent questionable conduct or lack of remorse").

information is inadmissible at trial.[17] Second, the admissibility of such information will have significant bearing on how fact finders will determine the outcomes of future cases.[18] Despite the importance of these issues, legal practitioners continue to neglect a critical step[19] when seeking to admit electronically generated documents into evidence: the authentication requirement.[20]

The starting point for any discussion involving authentication of evidence is Rule 901 of the Federal Rules of Evidence.[21] Courts have applied Rule 901[22] to cases involving the authentication of e-mails,[23] instant messages,[24] and website postings.[25] One notable exception to this development is the lack of consensus that has emerged regarding the rule's applicability to social networking evidence.[26] This uncertainty, in part, is due to the scarcity of cases that discuss social networking evidence.[27] Ambiguity in this area also stems from

17. *See* Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 538 (D. Md. 2007) (noting that it "makes little sense" to spend the time and money to procure electronic evidence that may ultimately be deemed inadmissible).

18. *See* Minotti, *supra* note 14, at 1066–68.

19. This "step" has been referred to as "a series of hurdles to be cleared by the proponent of the evidence." *Lorraine*, 241 F.R.D. at 538. One legal commentator has gone so far as to note that in certain circumstances, litigators must "jump through . . . hoops" to have evidence admitted. Goode, *supra* note 4, at 7–8.

20. Hon. Paul Grimm et. al., *Back to the Future:* Lorraine v. Markel American Insurance Co. *and New Findings on the Admissibility of Electronically Stored Information*, 42 AKRON L. REV. 357, 366 (2009) (noting that courts struggle with basic authentication principles for electronic data). This phenomenon may be attributable to the fact that "the most challenging aspect of admitting digital evidence is to establish its authenticity." *Id.* at 365. However, as this Comment explains, an even more troubling scenario arises when a litigant properly authenticates electronic evidence, and the *court* misconstrues the authentication standard. *See infra* Part II.A.

21. *See infra* Part I.A. Although none of the ten illustrations contained in Rule 901(b) specifically mention electronic evidence, the advisory committee's note indicates that the drafters intended for Rule 901 to apply to electronic evidence. FED. R. EVID. 901 advisory committee's note.

22. Although Rule 901 is a federal rule, most states have adopted similar provisions. *See* 3 BARBARA E. BERGMAN & NANCY HOLLANDER, WHARTON'S CRIMINAL EVIDENCE § 14:2 (15th ed. Supp. 2011) ("Most of the states have adopted evidentiary provisions essentially identical to Fed. R. Evid. 901(b)(1)."). Unless specifically addressing a unique provision of a state rule, discussion of the Federal Rules of Evidence in this Comment applies to state rules as well.

23. *See* United States v. Siddiqui, 235 F.3d 1318, 1322 (11th Cir. 2000); *see also infra* Part I.B.1.

24. *See* United States v. Gagliardi, 506 F.3d 140, 151 (2d Cir. 2007); *see also infra* Part I.B.2.

25. *See* Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1154 (C.D. Cal. 2002); *see also infra* Part I.B.3.

26. *See supra* note 14 and accompanying text.

27. Minotti, *supra* note 14, at 1070 ("Like federal case law, there is limited state case law on social networking web sites . . . .").

conflicting opinions[28] and factual differences[29] in the few cases that have addressed the issue.[30]

Of the relatively few court decisions discussing social networking evidence, the opinion of the Maryland Court of Appeals in *Griffin v. State* deserves a more thorough examination.[31] The *Griffin* court addressed whether the government properly authenticated a MySpace profile page of the defendant's girlfriend.[32] Over the defense counsel's objection that the State failed to authenticate the MySpace page, the trial judge admitted a redacted version of the profile into evidence.[33] After the jury convicted the defendant on all counts, the defendant appealed on the grounds that the trial court erred in admitting the MySpace page.[34] The case eventually reached the highest court in Maryland, the Maryland Court of Appeals, which reversed the lower court decision based on a finding that the trial judge committed reversible error by admitting the MySpace page into evidence.[35]

This Comment will explore the question of how courts should confront the issue of authenticating social networking evidence. Part I begins with a comprehensive overview of how courts have addressed authenticating other forms of electronic evidence, including e-mail, instant messages, and website content. Part I continues by examining the court decisions that have addressed the issue of authenticating social networking evidence, particularly the majority and dissenting opinions of *Griffin*. Next, in Part II, this Comment analyzes how most case law, with the exception of *Griffin*, has correctly applied the existing legal framework for authentication to address the issues raised by electronic evidence. Part II also discusses the troubling nature of *Griffin*'s overly burdensome authentication standard for social networking evidence.[36] In Part III, this Comment concludes by arguing that *Griffin*'s

---

28. *Compare* State v. Bell, No. CA2008-05-044, 2009 WL 1395857, at *5 (Ohio Ct. App. May 18, 2009) (finding no error in the trial court's ruling that MySpace printouts were properly authenticated), *with* Griffin v. State, 19 A.3d 415, 423–24 (Md. 2011) (finding that the trial court erred by admitting MySpace pages as properly authenticated). *See also* Minotti, *supra* note 14, at 1061 (noting that there is no consensus among courts on the admissibility of websites).

29. *See* Minotti, *supra* note 14, at 1061 (noting that cases discussing the application of the authentication rule to social networking websites are often decided through fact-specific analysis).

30. Minotti, *supra* note 14, at 1063 (observing that "case law discussing the applicability of the Federal Rules to social networking web sites specifically is scarce").

31. *Griffin*, 19 A.3d at 415.

32. *Id.* at 417.

33. Griffin v. State, 995 A.2d 791, 796–97 (Md. Ct. Spec. App. 2010), *rev'd*, 19 A.3d 415. Defense counsel objected on the grounds that the prosecutor did not establish a sufficient connection between the profile page and Barber, and that Barber was not questioned about the page. *Id.* at 796.

34. *Id.* at 794.

35. *Id.* at 418.

36. *See id.* at 427–48 (listing ways in which authentication can be obtained).

heightened standard should be abandoned and replaced with the "reasonable juror" standard advocated by the *Griffin* dissent.[37]

I. APPLICABILITY OF RULE 901 TO ELECTRONIC EVIDENCE

A. The "Reasonable Juror" Standard

A litigant seeking to introduce an item into evidence must first authenticate it.[38] Rule 901 sets the basic standard for authentication: "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."[39] Courts have often observed that the authentication requirement imposes "a relatively low bar."[40] In fact, counsel does not necessarily have to convince *the court* that the evidence is what it is purported to be.[41] Rather, the test for authentication is whether a *reasonable juror* would find in favor of authenticity.[42] All forms of evidence that a proponent seeks to admit into evidence must be authenticated.[43] Consequently, the reasonable juror standard has been applied to resolve authentication issues involving different types of evidence,[44] including physical evidence,[45] audio recordings,[46]

37. *See id.* at 428 (Harrell, J., dissenting) (arguing that the standard should be to require "evidence sufficient to support a finding that the matter in question is what its proponent claims").

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

39. *Id.* In other words, "is the evidence what it purports to be?" Hon. Randy Wilson, *Admissibility of Web Based Data*, 52 THE ADVOC. (TEXAS) 31, 31 (2010).

40. Grimm, *supra* note 20, at 367; *accord* United States v. Gagliardi, 506 F.3d 140, 151 (2d Cir. 2007) (stating the authentication standard is "minimal"); United States v. Safavian, 435 F. Supp. 2d 36, 38 (D.D.C. 2006) ("The threshold for the Court's determination of authenticity is not high.").

41. *See Safavian*, 435 F. Supp. 2d at 38.

42. Ricketts v. City of Hartford, 74 F.3d 1397, 1411 (2d Cir. 1996) (quoting United States v. Ruggiero, 928 F.2d 1280, 1303 (2d Cir. 1991)); Blake Tartt & Jeffrey S. Wolff, *Article IX: Authentication and Identification*, 30 HOUS. L. REV. 1029, 1035 (1993) ("The proponent, therefore, need not convince the court that the matter is genuine; he must only produce sufficient evidence so that a reasonable jury could properly find that it is.").

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

44. 7 BARBARA E. BERGMAN & NANCY HOLLANDER, WHARTON'S CRIMINAL EVIDENCE § 101:8, n.2 (15th ed. 2002).

45. *See, e.g.*, Coleman v. State, 833 S.W.2d 286, 289 (Tex. App. 1992) (finding that a vial of blood was properly authenticated because a reasonable jury could find that the evidence had been properly authenticated or identified).

46. *See, e.g.*, State v. Williams, 150 P.3d 111, 118 (Wash. Ct. App. 2007) (finding that a 911 recording was properly authenticated when the proponent "introduce[d] sufficient proof to permit a reasonable juror to find in favor of authenticity or identification").

surveillance video,[47] and photographs.[48]

The underlying legal justification for the reasonable juror standard is illustrated in *Lorraine v. Markel American Insurance Co.*, where the court describes the relationship between Rule 104(b) and Rule 901.[49] Rule 104(b), which governs "matters of conditional relevance generally," provides that the relevancy of evidence depends on whether the proponent has introduced facts "sufficient to support a finding" that a factual condition has been fulfilled.[50] The *Lorraine* court observed that, according to Rule 901's advisory committee's note, Rule 104(b) governs Rule 901's application because authentication is a type of relevancy that depends on the proponent fulfilling a condition of fact.[51] Therefore, because authentication is a "subset" of conditional relevance, authentication depends on whether the proponent introduces facts that a jury will determine are "sufficient to support a finding" that the evidence is authentic.[52]

Although Rule 901 lays out the general standard for authenticating evidence, "the rule is silent as to how, exactly, courts and lawyers should demonstrate that evidence is what its proponent claims."[53] Rule 901(b) provides a non-exhaustive list of ten examples that demonstrate how to authenticate evidence.[54] Judges and attorneys have most often turned to Rules 901(b)(1) (testimony of a knowledgeable witness) and 901(b)(4) (distinctive

---

47. *See, e.g.*, Sanford v. State, No. 12-08-00012-CR, 2009 WL 3161505, at *2 (Tex. App. Sept. 30, 2009) (holding that a surveillance video was properly authenticated and observing that "the ultimate test for authentication is always whether the proponent of the evidence has made a showing sufficient to permit a reasonable juror to find that the evidence is what its proponent claims").

48. Christine A. Guilshan, *A Picture Is Worth a Thousand Lies: Electronic Imaging and the Future of the Admissibility of Photographs into Evidence*, 18 RUTGERS COMPUTER & TECH. L.J. 365, 368 (1992) (observing that "[a]uthenticating photographs and thereby satisfying the second prong of the admissibility test is also not difficult").

49. 241 F.R.D. 534, 539 (D. Md. 2007). The author of the *Lorraine* opinion, Chief Magistrate Judge Paul William Grimm, is "a recognized authority on evidentiary issues concerning electronic evidence." Griffin v. State, 19 A.3d 415, 422 (Md. 2011). Judge Grimm also authored a law review article on the *Lorraine* opinion, which explains that *Lorraine* was intended to be "a 'how to' for the authentication of electronic evidence." Grimm, *supra* note 20, at 366.

50. FED. R. EVID. 104(b).

51. *Lorraine*, 241 F.R.D. at 539–40 (citing United States v. Branch, 970 F.2d 1368 (4th Cir. 1992)) (classifying authentication as a type of relevance by noting that it would be impossible for an item of evidence to have any bearing on a consequential fact in a case if the evidence is not what its proponent claims); *see also* FED. R. EVID. 901 advisory committee's note.

52. *Lorraine*, 241 F.R.D. at 539–40 ("[B]ecause authentication is essentially a question of conditional relevancy, the jury ultimately resolves whether the evidence admitted for its consideration is that which the proponent claims." (internal quotation marks omitted)).

53. Grimm, *supra* note 20, at 367.

54. *See* FED. R. EVID. 901(b)(1)–(10).

characteristics) to authenticate electronic evidence,[55] while authentication through Rule 901(b)(3) (comparison by trier or expert witness) has occurred less frequently.[56] The discussion that follows examines how courts have applied these 901(b) illustrations[57] to authenticate e-mail, instant messages, and website content.[58]

B. Application of Rule 901 to Electronic Evidence

1. E-Mail

To authenticate e-mail evidence, courts have applied the Rule 901(b) illustrations, as well as the reasonable juror standard.[59] In order to understand how and why courts have done this, one must comprehend the legally relevant aspects of e-mail communication itself.[60] As opposed to traditional mail, e-mail provides individuals the ability to transmit information instantly to an intended recipient's electronic mailbox.[61] This capability allows for people to transmit or reveal, often impulsively, information about themselves or others that may later become crucial evidence in court.[62] In fact, the court in *Lorraine* opined that e-mail is unquestionably the most prevalent form of

---

55. Goode, *supra* note 4, at 9.

56. United States v. Safavian, 435 F. Supp. 2d 36, 40 (D.D.C. 2006).

57. Rule 901 sets a low standard for proof that permeates each of these illustrations. *See* FED. R. EVID. 901 advisory committee's note ("The characteristics of the item itself, considered in the light of circumstances, afford authentication techniques in great variety."); *Lorraine*, 241 F.R.D. at 546 ("Although the common law origin of Rule 901(b)(3) involved its use for authenticating handwriting or signatures, it is now commonly used to authenticate documents. . . ."); 5 JACK B. WEINSTEIN & MARGARET A. BERGER, WEINSTEIN'S FEDERAL EVIDENCE § 901.03[2] (2d ed. 2012). ("[I]n recognition of the proponent's light burden of proof in [authenticating an exhibit] . . . the 'knowledge' requirement of Rule 901(b)(1) is liberally construed.").

58. Courts have applied other authentication measures in addition to 901(b)(1) and (4) to authenticate electronic evidence, such as online government publications. *See* Hon. Randy Wilson, *Admissibility of Web-Based Data*, 52 ADVOC. 31, 31–32 (2010), *available at* http://www.litigationsection.com/downloads/Advocate_V52_Fall2010Web.pdf. A discussion of these authentication measures is beyond the scope of this Comment.

59. United States v. Tank, 200 F.3d 627, 630 (9th Cir. 2000).

60. United States v. Safavian, 435 F. Supp. 2d 36, 40 (D.D.C. 2006) (discussing "distinctive characteristics" of e-mail as part of its Rule 901 analysis).

61. *Compare Mail Definition*, OXFORD ENGLISH DICTIONARY ONLINE, http://www.oed.com/view/Entry/112481?rskey=1PMBjw&result=2&isAdvanced=false#eid (last visited Oct. 17, 2012) (defining mail as "the letters, packages, etc. delivered to or intended for one address or individual"), *with E-mail Definition*, OXFORD ENGLISH DICTIONARY ONLINE, http://www.oed.com/view/Entry/60701?rskey=JDbs3W&result=2&isAdvanced=false#eid (last visited Oct. 17, 2012) (defining electronic mail as "[a] system for sending textual messages . . . to one or more recipients via a computer network").

62. *Lorraine*, 241 F.R.D. at 554 ("Perhaps because of the spontaneity and informality of e-mail, . . . e-mail evidence often figures prominently in cases where state of mind, motive, and intent must be proved.").

electronic evidence,[63] noting that "it is not unusual to see a case consisting entirely of e-mail evidence."[64]

As previously noted, a proponent seeking to admit e-mail into evidence must first authenticate it.[65] The largest obstacle to authentication is confirming that a particular individual authored a specific e-mail.[66] Litigants have overcome this challenge by creatively employing the 901(b) illustrations to introduce evidence sufficient to satisfy a reasonable juror that an e-mail is what the proponent claims.[67]

Shea v. State, a criminal case from Texas, provides a straightforward illustration of how a litigant can use Rule 901(b)(1) and Rule 901(b)(4) to authenticate an e-mail.[68] In this case, a jury convicted Kevin Shea of indecency with a child.[69] Shea appealed his conviction on the grounds that the State had not authenticated a series of e-mails Shea had sent to his underage victim,[70] and therefore, the trial court erred in admitting them into evidence.[71] Citing Rule 901(b)(1) of the Texas Rules of Evidence, the appellate court held that the trial court did not err in admitting the e-mails because "[t]he

---

63. *Id.*

64. *Id.*

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

66. WEINSTEIN & BERGER, supra note 57, at § 900.07[3][c] (stating that reliance on the sending address is misplaced because "e-mail messages can be sent by persons other than the sender"); Goode, *supra* note 4, at 10 (arguing that the biggest challenge to authenticating e-mails is determining the e-mail's author).

67. *See, e.g.*, Shea v. State, 167 S.W.3d 98 (Tex. Ct. App. 2005) (employing 901(b)(1) and 901(b)(4) to authenticate an e-mail). There is a subtle distinction between evidence that proves a computer printout is an accurate representation of the electronic data, and evidence that establishes a connection between the electronic evidence and a particular person. *See* United States v. Tank, 200 F.3d 627, 630 (2d. Cir 2000) (distinguishing between evidence showing that printouts were "an accurate representation of the chat room conversations" and evidence that "established a connection between [the defendant] and the chat room log printouts"). Unlike establishing a connection between the person and the chat room log, the accuracy of a printout only affects "the weight of the printouts, not their admissibility." *Id.* (quoting United States v. Catabran, 836 F.2d 453, 458 (9th Cir. 1988)).

68. *Shea*, 167 S.W.3d at 104–05.

69. *Id.* at 100.

70. *Id.* at 104. Electronic communications, like all communications, challenge the proponent to establish that a particular person was the communication's author. *See* Andrew M. Grossman, *No, Don't IM Me—Instant Messaging, Authentication, and the Best Evidence Rule*, 13 GEO. MASON L. REV. 1309, 1310 (2006) (observing that "connecting the identity of an online friend to that of a prosecutable human being can be difficult"); *see also* Griffin v. State, 19 A.3d 415, 419–20 (Md. 2011) (noting that the authorship of the MySpce account was at issue); *In re* F.P., 878 A.2d 91, 95–96 (Pa. Super. Ct. 2005) ("A signature can be forged; a letter can be typed on another's typewriter; distinct letterhead stationary [sic] can be copied or stolen" (citation omitted)); *Shea*, 167 S.W.3d at 104 ("[T]he issue of authentication arises whenever the relevancy of any evidence depends upon its identity, source, or *connection with a particular person*, place, thing or event." (quoting Kephart v. State, 875 S.W. 2d 319, 321 (Tex. Crim. App. 1994)) (emphasis added)).

71. *Shea*, 167 S.W.3d at 104.

complainant testified that she was familiar with Shea's e-mail address and that she had received the six e-mails in question from Shea."[72] Accordingly, the court held that the victim's testimony sufficiently authenticated the e-mails.[73]

The court also addressed how the "distinctive characteristics" of e-mail can be used for authentication purposes under Rule 901(b)(4), and found that several distinctive characteristics of the e-mails in question supported their authenticity.[74] Specifically, the victim testified that Shea had called her to confirm that she had received his e-mails, and that two of the e-mails referenced Shea's employment as a furniture maker.[75] Thus, the court in this case held that the evidence was properly admitted under both Rule 901(b)(1) and Rule 901(b)(4).[76]

2. Instant Messages[77]

Although e-mail messages are delivered to users' electronic inboxes,[78] instant messages are sent and received between users in real-time, on-line conversations.[79] For example, user A will send a message under her online pseudonym[80] to user B, which user B instantly receives. Using her own online

---

72. *Id.* at 105.

73. *Id.*

74. *Id.* Under the Federal Rules of Evidence as well as the Texas Rules of Evidence, Rule 901(b)(4) provides that authentication can be shown by "distinctive characteristics and the like." FED. R. EVID. 901(b)(4); TEX. R. EVID. 901(b)(4). This means, "[a]ppearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances." TEX. R. EVID. 901(b)(4).

75. *Shea*, 167 S.W.3d at 105. Other distinctive characteristics in a particular email included a statement that Shea liked the victim's locker number (22) because it was the number of years in age difference that separated Shea and the victim. *Id.* The victim also testified that her telephone conversations with Shea were similar to the content of the e-mail. *Id.* Finally, the court observed that four of the e-mails were signed "Kev." *Id.*

76. *Id.*

77. Instant messages are "generally the class of services that allows users of computers, data-enabled cellular phones, and other electronic devices to send one another text messages (and sometimes audio and video messages) instantaneously." Grossman, *supra* note 70, at 1311 (noting that instant messaging, initially popular among teens, is used now by adults, large business, and government agencies, indicating that "adeptness at instant messaging is now the new threshold for computer literacy").

78. *Inbox Definition*, OXFORD ENGLISH DICTIONARY ONLINE, http://www.oed.com/view/Entry/248369?redirectedFrom=inbox#eid (last visited Oct. 17, 2012) (defining "inbox" as "the (notional) part of an electronic mailbox in which incoming messages are stored").

79. *In re* F.P., 878 A.2d 91, 96 (Pa. Super. Ct. 2005) ("Instant messaging differs from e-mail in that conversations happen in realtime. . . . Generally, both parties in the conversation see each line of text right after it is typed (line-by-line), thus making it more like a telephone conversation than exchanging letters.").

80. Various courts and commentators have used different synonyms to describe an instant messenger's online pseudonym. *See In re F.P.*, 878 A.2d at 94 (referring to the online pseudonyms used in instant message conversations as "screen names"); Grossman, *supra* note 70, at 1314 (referring to these pseudonyms as "handles"). Grossman also notes that two people

pseudonym, user B responds to user A's message, creating a dialogue. As with e-mail, these digital conversations may later turn into critical evidence that determines the outcome of a case.[81] Additionally, like e-mail, the major authentication hurdle is establishing the requisite connection between a message and the alleged user.[82] *In re F.P.*, a Pennsylvania court decision, demonstrates how courts have overcome Rule 901's traditionally minimal authentication standard and have, in the process, eschewed a heightened authentication standard.[83]

In *In re F.P.*, a trial court found a defendant minor, F.P., delinquent on a single count of aggravated assault.[84] The assault resulted from F.P.'s belief that the victim had stolen a DVD from him.[85] The trial judge admitted into evidence printouts of two separate instant message conversations between F.P. and the victim that occurred before the assault.[86] These conversations revealed that F.P. threatened the victim with violence for stealing the DVD.[87] F.P. appealed his delinquency adjudication on the grounds that the trial judge erred in admitting the printouts into evidence.[88] Specifically, F.P. argued that the government had not properly authenticated the pages because it failed to establish that F.P. authored the messages.[89]

On appeal, the Pennsylvania Superior Court upheld the trial court's decision, using Pennsylvania Rule of Evidence 901 as the basis for its holding.[90] The

---

cannot have the same handle at once. *Id.* This observation is particularly relevant for establishing authorship of an instant message because it limits the number of people who may author instant messages under a given name. *Id.* Although a person other than the handle's creator may still access the account by stealing the account owner's password, it is impossible to create a separate account using the same handle. *Id.*

81. *See* Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 554 (2007) (discussing how an e-mail's spontaneous and informal qualities make it valuable in cases "where state of mind, motive and intent must be proved").

82. *See supra* notes 66–67 and accompanying text.

83. *In re F.P.*, 878 A.2d at 93 (using circumstantial evidence to authenticate the instant message printouts and disagreeing with the defendant's contention that instant message printouts could only be authenticated by producing the source's background information from the Internet service provider or by having a computer forensics expert testify); Grossman, *supra* note 70, at 1309.

84. *In re F.P.*, 878 A.2d at 92–93. F.P. approached the victim, Z.G., from behind and struck him in the head and face numerous times, causing the victim to be hospitalized for his injuries. *Id.* at 93.

85. *Id.*

86. *Id.* at 93–94.

87. *Id.* at 93.

88. *Id.*

89. *Id.* (arguing that the source needed to be identified or that a computer forensics expert should have testified).

90. *In re F.P.*, 878 A.2d at 93–96. The provisions of Pennsylvania Rule of Evidence 901 are substantively similar to Rule 901 of the Federal Rules of Evidence. Commonwealth v. Brooks, 508 A.2d 316, 319 (1986) (finding it "noteworthy" that Pennsylvania's approach to

court began its analysis by noting that Rule 901(a) establishes "'[t]he requirement of authentication or identification as a condition precedent to admissibility.'"[91] With regard to how a proponent may authenticate evidence, the court noted that Rule 901(b)(1),[92] as well as "direct and/or circumstantial evidence,"[93] were appropriate authentication measures.[94] It is notable that the court in *In re F.P.* methodically established Rule 901 as the appropriate analytical framework before discussing the law's application to the facts.[95]

The court noted that the victim testified that he used the screen name "WHITEBOY Z" and F.P. used the screen name "Icp4Life30" in the contested instant message conversation.[96] The victim also testified that F.P. sent him text messages that expressed F.P.'s desire to fight the victim because of the stolen DVD.[97] Comparing these text messages to the instant message conversation, the court observed that the conversation in question took place between individuals using those screen names, and that F.P. (Icp4Life30) repeatedly threatened the victim (WHITEBOY Z) with physical violence because of a stolen DVD.[98] The court also based its conclusion on evidence that F.P. referred to himself by his first name during the instant message conversation.[99]

---

authentication mirrors the circumstantial evidence analysis in the Federal Rules of Evidence); *see also infra* notes 91–93 and accompanying text.

91. *In re F.P.*, 878 A.2d at 93–96 (quoting PA. R. EVID. 901(a)). *Compare* PA. R. EVID. 901(a) (establishing "the requirement of authentication or identification as a condition precedent to authenticity"), *with* FED. R. EVID. 901(a) (establishing "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").

92. *Compare* PA. R. EVID. 901(b)(1) ("Testimony of witness with knowledge . . . that a matter is what it is claimed to be."), *with* FED. R. EVID. 901(b)(1) ("Testimony of a Witness with Knowledge . . . that an item is what it is claimed to be.").

93. Somewhat curiously, the court does not cite Pennsylvania Rule of Evidence 901(b)(4) to support its use of circumstantial evidence, even though the language mirrors Fed. R. Evid. 901(b)(4). *Compare* PA. R. EVID. 901(b)(4) ("Distinctive characteristics and the like [include] [a]ppearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with the circumstances."), *with* FED. R. EVID. 901(b)(4) ("Distinctive Characteristics and the Like [include] [a]ppearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken in conjunction with the circumstances."). Rather, the *In re F.P.* court supports its proposition that "[a] document may be authenticated by direct proof and/or by circumstantial evidence" by citing case law. *In re F.P.*, 878 A.2d at 94 (citing Commonwealth v. Brooks, 508 A.2d 316, 318 (Pa. Super. Ct. 1986)). Despite this, the language and context of the *In re F.P.* decision support the conclusion that the court regards Rule 901(b)(4) as a proper authentication method. *Id.*

94. *In re F.P.*, 878 A.2d at 93–94.

95. *Id.* at 93–95.

96. *Id.* at 94.

97. *Id.*

98. *Id.* (noting that the conversations occurred over a period of at least two days).

99. *Id.* The victim also testified that he notified school officials of F.P.'s threats after the first instant message conversation. *Id.* at 95. During the school's attempt to mediate the matter, the second threatening instant message conversation took place, in which F.P chastised the victim for bringing the matter to the attention of school officials. *Id.*

In applying the Rule 901 illustrations to the case facts, the court did not specifically categorize certain facts as authenticating the transcripts through Rule 901(b)(1), and other facts as authenticating the transcripts through direct or circumstantial evidence.[100] Rather, the court discussed its Rule 901(b)(1) analysis concurrently with its "circumstantial evidence" analysis to demonstrate how the victim's testimony reinforced the conclusion that F.P. authored the threatening messages.[101] Although the court viewed the victim's testimony as circumstantial evidence that supported the authenticity of the instant message printouts,[102] the court also explicitly referenced Rule 901(b)(1).[103]

3. Website Content[104]

As opposed to the two-way communication of e-mail and instant messaging, website content "flow[s] from the website owner to the viewer—a one-way street."[105] Despite these technological differences, the authentication issues that arise with e-mail and instant messaging also appear in cases involving the authentication of website content.[106] Specifically, authentication issues center around whether the website is automatically "attributable to the owner of the

100. *Id.* at 95. The *Shea* court employed a similar approach. *See supra* Part I.B.1.

101. *In re F.P.*, 878 A.2d at 93–95.

102. *Id.* at 95–96 ("[T]he foundation may consist of circumstantial evidence and may include factors relating to the contents of the writing and the events before and after the execution of the writing." (quoting Commonwealth v. Brooks, 508 A.2d 316, 321 (Pa. Super. Ct. 1986))). *But see* People v. Von Gunten, No. C035261, 2002 WL 501612, at *6 (Cal. Ct. App. Apr. 2, 2002) (holding that, despite the existence of circumstantial evidence supporting authenticity, a proponent had not adequately authenticated a transcript of an instant message conversation because "[t]here is no direct proof connecting [the person] with the screen name of BukaRoo20 in this case"). Requiring direct proof appears to conflict with Rule 901(b)(4) and its low standard. *See supra* Part I.A.

103. *In re F.P.*, 878 A.2d at 93–94 (citing PA. R. EVID. 901(b)(1)).

104. Website content refers to what Internet experts have defined as "Web 1.0." Web 1.0 is a term describing the first iteration of the web where users were predominantly fed content but had few ways to interact with other users. Brian Getting, *Basic Definitions: Web 1.0, Web 2.0, Web 3.0*, PRACTICAL ECOMMERCE (Apr. 18, 2007), http://www.practicalecommerce.com/articles/464-Basic-Definitions-Web-1-0-Web-2-0-Web-3-0 (describing Web 1.0 as "read only" web); Tim O'Reilly, *What is Web 2.0: Designed Patterns and Business Models for the Next Generation of Software*, O'REILLY (Sept. 30, 2005), http://oreilly.com/web2/archive/what-is-web-20.html (coining the terms Web 1.0 and Web 2.0 to describe the changes made to the web in the early part of this decade).

105. Payne, *supra* note 2, at 843. Payne notes that Web 1.0 has evolved from this basic form into Web 2.0, which is more interactive and embodies "dynamic information sharing." *Id.*; *see infra* Part I.C.1.

106. *See* Jarritos, Inc. v. Los Jarritos, No. C 05-02380 JSW, 2007 WL 1302506, at *10 (N.D. Cal. May 2, 2007), *rev'd and remanded sub. nom. on other grounds* Jarritos, Inc. v. Reyes, 345 F. App'x. 215 (9th Cir. 2009) (addressing the authentication of a picture printed from a website).

site."[107] This is a fair question given the possibility that a hacker might access a website and post unauthorized information.[108] A similar concern implicates whether the proffered content ever actually existed on the alleged website.[109] As the following case illustrates, courts have addressed these issues by applying Rule 901.[110]

Although the most common method of authenticating website content is Rule 901(b)(1) (testimony of a knowledgeable witness),[111] one important question arises: "what kind of personal knowledge is required?"[112] Must the website owner testify as to the exhibit's authenticity, or will the testimony of a person other than the website owner suffice to authenticate?[113] The court in *Jarritos, Inc. v. Los Jarritos* held that the latter was sufficient.[114]

In *Jarritos*, the plaintiff sought to authenticate a picture of the defendant's restaurant sign that the plaintiff's attorney had printed from the defendant's website, www.losjarritos.com.[115] Plaintiff's counsel explained that he personally typed the web address into his Internet browser, accessed the defendant's website, and printed the picture.[116] According to the court, counsel's explanation of these steps demonstrated his "*personal knowledge* of the exhibit," and thus sufficiently authenticated the evidence.[117] In *Jarritos*, the "one-way" nature of the defendant's restaurant website[118] contributed to

---

107. Goode, *supra* note 4, at 11 (citing Gregory P. Joseph, *Internet and Email Evidence*, PRAC. LITIGATOR, Mar. 2002, at 45, 46, *reprinted in* 5 STEPHEN A. SALTZBURG ET AL., FEDERAL RULES OF EVIDENCE MANUAL 4–21 (9th ed. 2006)). This is essentially a variation of the authentication issues that arise from instant messages or e-mail. *See supra* Part I.B.1–2.

108. St. Clair v. Johnny's Oyster & Shrimp, Inc., 76 F. Supp. 2d 773, 775 (S.D. Tex. 1999) ("[T]he Court holds no illusions that hackers can adulterate the content on *any* web-site from *any* location at *any* time."); *see also* Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 555 (D. Md. 2007) ("The issues that have concerned courts include the possibility that third persons other than the sponsor of the website were responsible for the content of the posting . . . .").

109. Goode, *supra* note 4, at 11 ("What was actually on the website?").

110. *See Jarritos, Inc.*, 2007 WL 1302506, at *10–11 (using the "sufficient to support a finding" standard to overrule defense counsel's objection that information on a one-way website was properly authenticated).

111. FED. R. EVID. 901(b)(1).

112. Goode, *supra* note 4, at 13 (comparing courts that require the website's owner to authenticate with courts allowing third-party authentication).

113. *Id.* at 13–14.

114. 2007 WL 1302506, at *10 (finding third-party knowledge of the website's contents as adequate to authenticate the picture).

115. *Id.*

116. *Id.*

117. *Id.* (emphasis added).

118. Many websites are interactive, allowing, for example, customers to make reservations online. *See e.g.* RISTORANTE PICCOLO, http://www.piccolodc.com/about.php (scroll to bottom of page; then enter data in fields labeled "Party Size", "Date", and "Time"; then follow "Find A Table" hyperlink). Some restaurants, including the former Los Jarritos restaurant (currently operating as "San Jalisco"), allow customers to place orders through the website. *See* SAN JALISCO, www.losjarritos.com (follow "www.sanjalisco.com" hyperlink). However, this type of

this relatively simplistic authentication method.[119]

C. A New Frontier for the Authentication of Electronic Evidence: Social Networking Websites

1. Technological and Functional Similarities Between Social Networking Websites and Other Forms of Electronic Evidence

The term "social networking website" is difficult to define because of the complexity and variety of these types of websites.[120] Nevertheless, one article provides a comprehensive and useful definition of social networking sites and defines them as "web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system; (2) articulate a list of other users with whom they share a connection; and (3) view and traverse their list of connections and those made by others within the system."[121] Both MySpace and Facebook[122] contain technical capabilities that are identical or nearly identical in functionality to e-mail, instant messages, and one-way websites.[123] Like e-mail, Facebook allows its users to send messages to

---

interaction differs significantly from the interactive capabilities available through social networking websites. *See infra* Part I.C.1.

119. *See supra* note 118. The fact that the website printout of the defendant's restaurant sign was evidence of the plaintiff's trademark infringement claim also contributed to this straightforward authentication procedure. *See Jarritos, Inc.*, 2007 WL 1302506, at *10. It is unclear whether the court's holding would have been different if the plaintiff would have attempted to prove that a specific individual posted the photograph on the website. *See supra* notes 66–67.

120. Payne, *supra* note 2, at 846 ("A completed profile contains approximately forty different ways to express information."); Mary White, *What Types of Social Networks Exist*, LOVETOKNOW SOCIAL NETWORKING, http://socialnetworking.lovetoknow.com/What_Types_of_Social_Networks_Exist (last visited Sept. 28, 2012) ("Given the constant evolution of the online world, it would be difficult to place a limit on how many types of social networks exist.").

121. Danah M. Boyd & Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship*, 13 J. COMPUTER-MEDIATED COMM. (2007), *available at* http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html. Another author has defined social networking sites as "interactive web sites that connect users based on common interests and that allow subscribers to personalize individual web sites." Wilson, *supra* note 11, at 1204.

122. This Comment focuses on the two popular social networking websites, Facebook and MySpace, for the sake of simplicity and legal relevance. *See* White, *supra* note 120 (explaining that the leading websites do not represent the full scope of existing social networking websites); *see also* Minotti, *supra* note 14, at 1059 (citations omitted) ("MySpace and Facebook have proven especially useful to attorneys who seek incriminating evidence in family law matters, personal injury claims, and criminal law cases.").

123. Minotti, *supra* note 14, at 1063–64 (comparing the messaging features of social networking websites with e-mails and noting the similarities between their inboxes and third-party facilitation of the communication despite both being password protected).

another user's Facebook inbox.[124] Facebook also has a chat function, which enables users to have instant message conversations with other users.[125] Finally, Facebook enables users to post information that is available either to the general public or to a selected group of other Facebook users.[126] This function makes posted information available to a large audience, similar to a "one-way street" website.[127] However, unlike one-way websites, Facebook allows individuals other than the user to post information on the user's Facebook webpage.[128] Although the user retains control over his Facebook webpage's operation, other users have an abundance of options in terms of the type, form, and amount of information they can post on the webpage.[129] Like Facebook, MySpace also allows users to send e-mail-like messages through "MySpace Mail," have instant message conversations through "MySpace IM," and upload unrestricted amounts of profile information for consumption by the general public or a restricted group.[130]

2. Social Networking Evidence in Case Law

Despite the growing importance of Facebook and MySpace to the legal community, few courts have discussed authentication of social networking evidence.[131] With the exception of *Griffin v. State*, courts discussing this issue

---

124. *See generally Sending a Message*, FACEBOOK, http://www.facebook.com/help?page=938 (last visited Sept. 29, 2012) ("When you send someone a message, it gets delivered to the person's Facebook Messages.").

125. *See generally Basics: How to Chat*, FACEBOOK, http://www.facebook.com/help?page=824 (last visited Sept. 29, 2012) (explaining how a user can use Facebook chat).

126. *When I Share Something, How Do I Choose Who Can See It?*, FACEBOOK, http://www.facebook.com/help/?faq=120939471321735 (last visited Sept. 29, 2012) (noting that users have the option of sharing information with the pubic, friends, friends of anyone in the "tagged" picture, or only with themselves).

127. *Id.*

128. *See* Payne, *supra* note 2, at 845 ("[I]nformation flows not only from website owner to website viewer, but also from viewer to owner and viewer to viewer.").

129. *Id.* at 845. Payne observes:

> Facebook members can share text with multiple people through a "status update" or through information placed on the user's profile. A completed profile contains approximately forty different ways to express information. Users can also share text with another user individually through a direct message to the user or a wall post to the user's profile, or users can have a direct conversation with another user through Facebook's chat feature . . . A user's "news feed" displays all the information that his or her friends create, change, or share.

Id. (citations omitted). The ability to share pictures and videos can have particularly far reaching legal consequences. *See* Minotti, *supra* note 14, at 1059 (highlighting a case where a defendant was sentenced to two years' imprisonment for lack of remorse based on the defendant's Facebook page that showed him wearing a shirt displaying the words "Jail Bird" on Halloween).

130. *See generally* MYSPACE, http://www.myspace.com (last visited Sept. 29, 2012).

131. Minotti, *supra* note 14, at 1070 (noting that there is very little state or federal case law on using social networking websites as evidence).

provide minimal practical guidance or legal rationale for their holdings.[132] For example, in *In re T.T.*, a Texas court held that there was sufficient evidence to support a trial court's ruling that termination of parental rights was in the best interests of the children.[133] The court based its ruling, in part, on incriminating content on the father, Johnny's, MySpace page, which indicated that he was single and did not want children.[134] Although Johnny took ownership of the MySpace page, he argued that he had no knowledge of the incriminating statements, claiming that a third party created the MySpace page for him.[135] When called to testify, the third party testified that he had not set up the MySpace page for Johnny.[136] Further, Johnny's wife testified that Johnny had been unfaithful to her.[137] The court held that the testimony of these witnesses was "sufficient evidence for the jury reasonably to conclude" that Johnny had set up the page and authored the damaging statements.[138] Despite using language parallel to Rule 901, the court did not explicitly address Rule 901, presumably because Johnny had not raised the issue of the authenticity of his MySpace page.[139] Thus, although the court in *In re T.T.* "allow[ed] information from a MySpace page"[140] as evidence, it is hardly illustrative.

State v. Bell, an Ohio court decision, provides more guidance on authenticating social networking evidence.[141] Similar to *Shea*, the defendant in *Bell* was charged with a number of sex crimes involving children.[142] In support of its case, the State sought to introduce evidence of MySpace instant message conversations between the defendant and his victims.[143] These conversations contained code phrases, such as "The Donkey Game," which referred to sexual acts known only to the defendant and his victims.[144] The defendant argued that the transcripts should not be admitted into evidence for lack of authenticity because (1) the transcripts could have been edited after

---

132. *See* Griffin v. State, 995 A.2d 791, 804 (Md. Ct. Spec. App. 2010), *rev'd*, 19 A.3d 415 (Md. 2011) (noting that the court's research revealed "only a handful of reported cases involving evidence specifically pertaining to social networking Web sites").

133. 228 S.W.3d 312, 322 (Tex. App. 2007).

134. *Id.*

135. *Id.* at 322 (citing the defendant's claim that he e-mailed a photograph of himself to a friend who subsequently created a page for him).

136. *Id.*

137. *Id.*

138. *Id.* at 322–33.

139. *Id.* at 322.

140. Minotti, *supra* note 14, at 1054 n.10.

141. No. CA2008-05-044, 2009 WL 1395857, at *5 (Ohio Ct. App. May 18, 2009) (concluding that the MySpace page could be authenticated under Rule 901(b) by testimony from a witness with knowledge of ownership).

142. *Id.*

143. State v. Bell, 882 N.E.2d 502, 511 (Ct. Com. Pl. Ohio 2008), *aff'd*, 2009 WL 1395857, at *1.

144. *Id.* at 511–12.

they were taken from his computer; and (2) someone else could have used his MySpace account.[145] Citing to the "low standard" of Rule 901, the court held that the victim could authenticate the MySpace printouts through testimony regarding his knowledge of the defendant's MySpace screen name and the sexual code phrases.[146] In the court's view, "this would permit a reasonable juror to conclude that the offered printouts [were] . . . authentic."[147]

The *Bell* court has been described as "especially progressive" in its treatment of social networking evidence.[148] A New York appellate court in *People v. Clevenstine* did not take such a "progressive" approach in its application of Rule 901.[149] In this case, the government charged the defendant with criminal sexual acts with underage persons.[150] Similar to *Bell*, the prosecution's evidence consisted mainly of sexually explicit MySpace conversations between the victims and the defendant.[151] In this case, instead of printouts, the conversations were recorded on a computer disk, which the defendant argued were not properly authenticated.[152] The court rejected this argument, holding that the evidence was authenticated through the victims' testimony that they had participated in the MySpace chats with the defendant.[153] In addition to the victims, the government called a State Police computer expert and a MySpace legal compliance officer as witnesses to authenticate the evidence.[154] Both witnesses confirmed that the conversations in question had been recovered from the victims' hard drives and had taken place between the MySpace accounts created by the defendant and the victims.[155] Although the court did not explicitly address Rule 901, it observed that the defendant's argument "presented a factual issue for the jury."[156]

---

145. *Id.* at 512.

146. *Id.*

147. *Id.*

148. Minotti, *supra* note 14, at 1071–72 (noting the decision in *Bell* to allow authentication of the MySpace chat was in accordance with the progressive approach that Ohio courts had generally taken).

149. 891 N.Y.S.2d 511, 514 (N.Y. App. Div. 2009) (finding that MySpace instant messages were authenticated properly).

150. *Clevenstine*, 891 N.Y.S.2d at 513.

151. *Id.* at 514.

152. *Id.* at 513–14.

153. *Id.* at 514. In support of its decision, the court also referenced the testimony of the defendant's wife, who stated that she discovered the sexually explicit conversations between her husband and the victims on the couple's home computer. *Id.*

154. *Id.*

155. *Id.*

156. *Id.*

D. Into the Abyss: Griffin v. State *Confronts MySpace Profile Evidence*

1. Scarcity of Social Networking Case Law Creates an Issue of First Impression for the Griffin *Court*

Given the small number of cases discussing the authentication of social networking evidence, *Griffin v. State* presented the Maryland Court of Appeals with an issue of first-impression:[157] whether the government properly authenticated printed pages from a MySpace profile under Maryland Rule 5-901?[158] In *Griffin*, the State of Maryland charged the defendant, Antoine Griffin, with murder.[159] A key eyewitness for the State, Dennis Gibbs, provided inconsistent testimony about what he witnessed on the night of the murder.[160] Gibbs attributed his conflicting testimony to being threatened by the defendant's girlfriend, Jessica Barber, before the first trial.[161] To corroborate Gibbs's testimony about being threatened, the government sought to introduce a printout of a MySpace profile page, allegedly owned and authored by Barber, that contained the following statement: "FREE BOOZY!!!! JUST REMEMBER SNITCHES GET STITCHES!! U KNOW WHO YOU ARE!!"[162] The profile indicated that the owner and creator of the page was a female from Port Deposit, Maryland, born on October 2, 1983.[163] The trial court admitted the evidence over defense counsel's objection, and

---

157. 995 A.2d 791, 804 (Md. Ct. Spec. App. 2010), *rev'd*, 19 A.3d 415 (Md. 2011) (noting that the court's research revealed "only a handful of reported cases involving evidence specifically pertaining to social networking Web sites"). The few cases that have addressed authentication of social networking evidence have focused on instant messages and e-mail conversation conducted through MySpace. *See* State v. Bell, No. CA2008-05-044, 2009 WL 1395857 at *5 (Ohio Ct. App. May 18, 2009); *Clevenstine*, 891 N.Y.S.2d at 514. These cases were little help to the *Griffin* court because the government sought to introduce evidence from a MySpace profile page. Griffin v. State, 19 A.3d 415, 417 (Md. 2011). As the Court of Special Appeals observed, "profile information posted on social networking Web pages differs from chat logs of instant message correspondence conducted through such sites." *Griffin*, 995 A.2d at 805.

158. *Griffin*, 19 A.3d at 416–17 (citation omitted) (presenting the issue as "determining the appropriate way to authenticate, for evidential purposes, electronically stored information printed from a social networking website, in particular, MySpace"). The court later narrowed the inquiry: "Did the trial court err in admitting a page printed from a MySpace profile alleged to be that of Petitioner's girlfriend?" *Id.* at 417.

159. *See Griffin*, 995 A.2d at 794.

160. *Id.* at 794–95. The inconsistent testimony pertained to whether Gibbs saw Griffin follow the victim into the bathroom with a gun. *Id.* At the first trial, Gibbs stated that he had not witnessed this. *Id.* at 794. During the second trial, which resulted because of a mistrial, Gibbs testified that he had seen Griffin and the victim enter the bathroom just before he heard the sound of gunfire. *Id.* at 794–95.

161. *Id.* at 795 (stating that he was told that he "might catch a bullet" if he appeared in court).

162. *Id.* at 796.

163. *Id.* The printout of the MySpace profile also had a photograph of an embracing couple that looked like Griffin and Barber. *Id.* The government supported the printout's authenticity by introducing the testimony of the Maryland State Police investigator who originally printed the MySpace page from the internet. *Id.* at 796–97.

Griffin was ultimately convicted on all counts.[164] Griffin appealed to the Maryland Court of Special Appeals, which affirmed the judgment of the trial court.[165] Griffin appealed again to the Maryland Court of Appeals.[166]

2. The Griffin *Majority: Concerns About the Potential for Technological Manipulation and Impersonation*

The Maryland Court of Appeals reversed the decision and held that the government did not meet the authenticity threshold to admit the MySpace page.[167] In reaching its conclusion, the court described its concern with information taken from MySpace: "[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."[168] After providing several examples of these "fictitious account[s]," the court addressed the general authentication provision of Maryland Rule 5-901(a), as well as the illustrations relevant to the facts of this case, Rule 5-901(b)(1), and Rule 5-901(b)(4).[169]

However, the court quickly returned to the "fictitious account" theme, and ultimately held that the lower court "failed to acknowledge the possibility or likelihood that another user could have created the profile in issue or authored the 'snitches get stitches' posting."[170] The court found that Barber's picture, date of birth, location, and reference to the defendant's nickname on the MySpace page were insufficient to alleviate the court's concerns.[171] The court narrowed its decision by noting that its holding did not altogether preclude admission of evidence from social networking sites and that authentication methods for such evidence would gradually evolve over time.[172]

---

164. *Id.*

165. *Id.*

166. Griffin v. State, 19 A.3d 415 (Md. 2011).

167. *Id.* at 418.

168. *Id.*

169. *Id.* at 422 (citing the knowledgeable witness and circumstantial evidence illustrations).

170. *Id.* The court presumes that this type of evidence was authored by a third-party. As such, the *Griffin* court transforms the burden of establishing authenticity into a rebuttable presumption that someone other than the purported owner of an online profile page created the page or authored its content. *Id.* Other courts have rejected this approach. *See In re* F.P., 878 A.2d 91, 95 (Pa. Super. Ct. 2005) (finding that the rules of authentication for electronic communication should not differ from their application to written documents).

Moreover, the majority's contention that the lower court did not address the possibility that someone other than Barber created the MySpace post is misplaced. *Griffin*, 995 A.2d at 805 (noting that "[a] proponent should anticipate the concern that someone other than the alleged author may have accessed the account and posted the message in question."), *rev'd*, 19 A.3d 415.

171. *Griffin*, 19 A.3d at 424.

172. *Id.* at 427. The court lists three rigid ways to authenticate social networking evidence: (1) ask the purported creator if she created the cite or the content; (2) "examine the computer's internet history and hard drive to determine whether that computer was used to originate the

3. The Griffin *Dissent: The Majority's "Technological Heebie Jeebie's"*[173] *and the "Reasonable Juror" Standard*

In contrast with the majority opinion, the dissent began its analysis with a discussion of Maryland Rule 5-901.[174] Noting the overwhelming similarities between Maryland Rule 901 and Federal Rule 901, the dissent observed that every federal circuit court has adopted the standard "that a document is properly authenticated if a *reasonable juror could find in favor of authenticity*."[175] Addressing the majority's concern that an imposter could have created an account in Barber's name or posted the "snitches get stitches" threat, the dissent opined that these concerns go to the weight of the evidence with the trier of fact, not to its admissibility.[176]

II. THE *GRIFFIN* MAJORITY ADOPTS AN UNNECESSARILY STRINGENT AUTHENTICATION STANDARD FOR SOCIAL NETWORKING EVIDENCE

A. The Rehabilitation of "Voodoo Information": The Griffin *Majority's Flawed Rationale*

The *Griffin* majority's uneasiness with the MySpace page is problematic[177] because the three alternative authentication measures the majority proposes do not adequately address its concerns of fraud.[178] The first suggested method, asking Barber whether she created the page or posted the threat, ignores the fact that Barber has a motive to lie.[179] The second suggested method,

---

social networking profile and posting in question"; and (3) obtain information from the social networking site. *Id.*

173. *Id.* at 430 (Harrell, J., dissenting) (suggesting that the majority's approach underscores their "technological heebie jeebies").

174. *Id.* at 428.

175. *Id.* at 429 (noting that federal and Maryland's rules of evidence are in accordance with the reasonable juror standard).

176. *Id.* at 430.

177. *See In re* F.P., 878 A.2d 91, 95–96 (Pa. Super. Ct. 2005) (rejecting the argument that because an imposter could send an electronic communication in someone else's name, the court should construct new authentication rules). *But see* Rebecca Greenfield, *Facebook Has A New Feature That Can Help Liars*, THE ATLANTIC WIRE (Nov. 15, 2011), http://www.theatlanticwire.com/technology/2011/11/facebook-has-new-feature-can-help-liars/45011/ ("A new 'edit date' icon has appeared [on Facebook], hidden behind a pencil icon link at the top corner of timeline wall postings, allowing users to change someone's wall post from the date it was actually posted to a previous moment in history."). Although this function does not pertain to the majority's concern that an imposter could have posted the threat, it does relate to the broader fraudulence concerns of social networking evidence in general. *See Griffin*, 19 A.3d at 428 (noting that the majority's concern centered on the ability of an imposter to send an electronic communication in someone else's name).

178. *See infra* notes 179–80 and accompanying text.

179. Although Barber's admission that she created the MySpace page and authored the "snitches get stitches" comment would have provided *direct* evidence of authenticity, Rule 901 and cases interpreting Rule 901 have held that *circumstantial* evidence is sufficient to

searching Barber's computer, fails to account for the possibility that a third party could have used Barber's computer.[180] The third suggested approach, obtaining information from the social networking site that links the profile with its owner, overlooks the relative ease with which fraudulent accounts can be created.[181] Because anyone can create an e-mail account to fabricate a MySpace account, it is not clear why a MySpace legal compliance officer's testimony that a particular account was created with a particular e-mail establishes authenticity.[182] To be fair, each of these suggested methods does address, albeit narrowly, the specific fraudulence concerns raised by the majority by making it somewhat less likely that a third party posted the material in question. However, as illustrated, these methods raise an entirely separate set of impersonation issues.[183] The slight increase–if any–in reliability resulting from the utilization of the majority's proposal would also be grossly outweighed by the high costs and undue burden imposed through implementation.[184]

B. Off the Mark: The Griffin *Majority's Disconnect with Prior Case Law*

1. Cherry-picking Lorraine*:* Griffin*'s Selective Use of a Seminal Case*

Admittedly, the *Lorraine* opinion, which is often cited for its legal justification for the reasonable juror standard, does appear in the majority's

---

authenticate. *See* FED. R. EVID. 901(b)(4); *In Re F.P.*, 878 A.2d at 94 ("A document may be authenticated by direct proof and/or by circumstantial evidence."). Case law supports the conclusion that the *Griffin* trial court adopted the correct approach by admitting the evidence, thus affording the defense the opportunity to call its reliability into question in front of the jury. *Griffin*, 19 A.3d at 430 (Harrell, J., dissenting) (citing Hays v. State, 40 Md. 633, 648 (1874) (noting that the majority's concern about whether Barber actually authored the statement goes to its weight, not its admissibility)).

180. *See Griffin*, 19 A.3d. at 423 (majority opinion) (arguing that the court of appeals gave too little concern to the notion that a third party may have pretended to be Barber and posted on the social networking website).

181. *Id.* at 420. Ironically, the majority seems expressly aware of this fact. *Id.* (noting that anyone fourteen or older who has an e-mail address can create a MySpace profile at no cost).

182. Courts have also expressly rejected the court's third suggestion. *See In re F.P.*, 878 A.2d at 93 (disagreeing with the defendant's contention that instant message printouts could only be authenticated "by introducing evidence of their source from the Internet service provider or presenting the testimony of a computer forensics expert").

183. *See supra* notes 179–81 and accompanying text.

184. *See* Goode, *supra* note 4, at 7–8 (rejecting a heightened authentication standard as "counterproductive" and noting that "[a]part from the difficulty of defining what types of evidence the new rules would apply to, the costs of imposing a new rule would greatly outweigh its benefits"). Goode also argues that "[r]equiring lawyers to adduce additional proof before introducing any piece of electronic evidence, even in the absence of concerns about tampering or manipulation, will result in additional litigation costs and, where lawyers fail to jump through all the new hoops, the loss of reliable evidence." *Id.*

opinion.[185] For example, the *Griffin* majority correctly cites the *Lorraine* court's observation that judges are increasingly requiring litigators to increase focus on the "foundational requirements" when authenticating electronic evidence.[186] However, the *Lorraine* court also noted that Rule 901 imposes only a *prima facie* showing, which is "not a particularly high barrier to overcome."[187] Nowhere in its opinion does the *Griffin* majority address or distinguish itself from *Lorraine's* low barrier interpretation of Rule 901.[188]

Further, the *Griffin* majority misconstrues the *Lorraine* opinion as supporting its position, noting that *Lorraine* "recognized that authenticating electronically stored information presents a myriad of concerns because 'technology changes so rapidly' and is 'often new to many judges.'"[189] Although *Lorraine* mentions that "technology changes so rapidly" and is

---

185. *Griffin*, 19 A.3d. at 423 (citing Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 543–44 (D. Md. 2007)).

186. *Id.* (citing *Lorraine*, 241 F.R.D. at 543–44).

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

188. *Griffin*, 19 A.3d at 416–28. Moreover, the majority casually dismisses the reasonable juror standard in a footnote when it states, "the 'reasonable juror' standard to which the dissent refers is apparently derived from the federal analogue to Maryland Rule 5–104(b), concerning 'relevance conditioned on fact,' a protocol not addressed in this case." *Id.* at 424 n.12. By noting the distinction between Maryland Rule 5-104(b) and its "federal analogue," the majority suggests that the reasonable juror standard derives only from the latter, and not the former. *Id.* This approach is odd in light of the similarity between the two. *Compare* MD. R. EVID. 5-104(b) ("RELEVANCE CONDITIONED ON FACT. When the relevance of evidence depends upon the fulfillment of a condition of fact, the court shall admit it upon, or subject to, the introduction of evidence sufficient to support a finding by the trier of fact that the condition has been fulfilled."), *with* FED. R. EVID. 104(b) ("RELEVANCE THAT DEPENDS ON A FACT. When the relevance of evidence depends on whether a fact exists, proof must be introduced sufficient to support a finding that the fact does exist. The court may admit the proposed evidence on the condition that the proof be introduced later."). This language severely undercuts the majority's contention that the reasonable juror standard "is apparently derived from the federal analogue to Maryland Rule 5-104." *Griffin*, 19 A.3d at 424 n.12. To the contrary, the reasonable juror standard is "apparently" (if not explicitly) derived from the phrase "by the trier of fact," which is contained in the Maryland Rule. MD. R. EVID. 5-104(b). Additionally, the majority's attempt to distinguish between Maryland Rule 5-104 and its "federal analogue" makes no sense in light of the advisory committee's note to Maryland Rule 5-104 that states, "[t]his Rule is derived from F.R.E. 104." MD. R. EVID. 5-104 advisory committee's note. Maryland case law also undermines the majority's refusal to interpret Maryland Rule 5-104 in accordance with its federal equivalent. *Griffin*, 19 A.3d at 429 (Harrell, J., dissenting) ("Maryland courts have traditionally relied on the federal courts' interpretations of analogous rules as persuasive authority. . . ." (quoting Higgins v. Barnes, 530 A.2d 724, 729 (1987))).

The majority's assertion that the court had "not been asked in this case to address the efficacy of the Rule 5-104(b) protocol" is similarly misplaced. *Id.* at 428 n.15 (majority opinion). The majority correctly recognizes that the central issue in the case is authentication. *Id.* at 422. As Judge Grimm observes, "authentication is essentially a question of conditional relevancy. . . ." *Lorraine*, 241 F.R.D. at 539 (quoting United States v. Branch, 970 F.2d 1368, 1370 (4th Cir. 1992)). It is therefore not clear how the *Griffin* court thought it could properly resolve the authentication issue without "address[ing] the efficacy of the 5-104(b) protocol."

189. *Griffin*, 19 A.3d at 423 (quoting *Lorraine*, 241 F.R.D. at 544).

"often new to many judges," the court does not state that these observations should give rise to a "myriad of concerns."[190] The "myriad of concerns" language is purely a creation of the *Griffin* court.[191] Thus, the majority's approach conflates the *Lorraine* opinion it purports to apply, and instead invokes a questionable analysis akin to Judge Kent's "voodoo information."[192]

2. Missing the Obvious: Rule 901 is Appropriate

A majority of courts and commentators agree that the current authentication standard under Rule 901 is adequate for authenticating electronic evidence.[193] In particular, appellate courts consistently recognize that Rule 901's standard is appropriate for addressing the issue of electronic evidence authentication.[194] These appellate court opinions usually reference either the 901(b) illustrations, the minimal requirements of the reasonable juror standard, or both.[195] The *Griffin* majority's analysis is inconsistent with these appellate decisions that

---

190. *Lorraine*, 241 F.R.D. at 544. Rather, the *Lorraine* court does not support a "one size fits all" approach for authenticating electronic evidence. *Id.*

191. *See Griffin*, 19 A.3d. at 430 (Harrell, J., dissenting) (characterizing this attitude as the "technological heebie jeebies"); *supra* note 173.

192. *See supra* notes 1–4 and accompanying text; *Lorraine*, 241 F.R.D. at 584 (describing *St. Clair* as treating online evidence with a "extreme" skepticism); *see also* Wilson, *supra* note 39, at 31 (describing the *St. Clair* opinion as "infamous."). The *Griffin* majority's rationale for its reluctance to accept a MySpace profile as evidence has undertones of late 19th and early 20th century cases that rejected evidence in the form of photographs, motion pictures, and computerized records. *Compare Griffin*, 19 A.3d at 421 (discussing its concerns with authenticating social networking website evidence), *with* State v. Simon, 174 A. 867, 872 (N.J. Sup. Ct. 1934) (indicating the court's lack of knowledge of any cases in which a a phonograph record of an alleged conversation was authenticated), *aff'd*, 178 A. 728 (N.J. 1935), *and* Cunningham v. Fair Haven & W. R. Co., 43 A. 1047, 1049 (Conn. 1899) (excluding photographic evidence, the court noted that "either through want of skill on the part of the artist, or inadequate instruments or materials, or through intentional and skillful manipulation, a photograph may be not only inaccurate, but dangerously misleading."), *and* United States v. Scholle, 553 F.2d 1109, 1125 (8th Cir. 1977) (reluctantly upholding the trial court's admission of computer generated business records but arguing for a more comprehensive review of their authenticity).

193. Grimm, *supra* note 20, at 362. (arguing that the existing evidence rules apply to electronic evidence authentication); *see also In re* F.P., 878 A.2d 91, 95 (Pa. Super. Ct. 2005) (holding that "electronic [evidence] can be properly authenticated within the existing framework of [the rules of evidence]"); MANUAL FOR COMPLEX LITIGATION § 11.446 (4th ed. 2007) (observing that "the Federal Rules of Evidence apply to computerized data as they do to other types of evidence"). Even courts that have expressed these concerns concede that the traditional standards of authentication should apply to electronic evidence. *See In re* Vee Vinhnee, 336 B.R. 437, 445 (B.A.P. 9th Cir. 2005) (noting that although "[t]he paperless electronic record . . . presents more complicated variations on the authentication problem, . . . [u]ltimately, . . . it all boils down to the *same question* of assurance that the record is what it purports to be") (emphasis added).

194. *See supra* Parts I.B.1–3 (discussing how different forms of electronic evidence have been authenticated through Rule 901).

195. *See supra* Parts I.B.1–3 (discussing ubiquitous use of the reasonable juror standard).

consistently reference the "slight,"[196] "minimal,"[197] and "relatively low"[198] Rule 901 standard.[199]

For example, in *Shea v. State*, the court devoted a significant portion of its discussion to an analysis of the facts of the case under the 901(b)(1) and 901(b)(4) illustrations.[200] Although the importance of the court's 901(b)(4) discussion should not be understated, it is significant that the court authenticated the e-mails *before* it analyzed the 901(b)(4) evidence.[201] This suggests that the court would have authenticated the e-mails based only on the victim's testimony pursuant to Rule 901(b)(1).[202] In other words, the 901(b)(4) "distinctive characteristics" identifying Shea as the author of the e-mails were helpful for authentication, but not required.[203] That the court likely would have authenticated the e-mails based only on the Rule 901(b)(1) testimony reinforces the argument that Rule 901 imposes only a minimal burden of proof for authentication.[204]

Additionally, the *Shea* court's employment of both Rule 901(b)(1) and 901(b)(4)[205] demonstrates the adaptability of the Rule 901(b) illustrations.[206] The court discussed the victim's testimony, that Shea called her to confirm that she had received his e-mails, under the 901(b)(4) analysis.[207] However, this testimony was also clearly relevant to the victim's knowledge under Rule 901(b)(1);[208] the victim knew that Shea sent the e-mails because she spoke to him about them.[209] Because this testimony could have served to authenticate the e-mails under either Rule 901(b)(1) *or* Rule 901(b)(4), *Shea* demonstrates that the Rule 901 standard is not only minimal, but also flexible in its

196. Dickens v. State, 927 A.2d 32, 37 (Md. Ct. Spec. App. 2007).

197. United States v. Gagliardi, 506 F.3d 140, 151 (2d Cir. 2007) (quoting United States v. Tin Yat Chin, 371 F.3d 31, 38 (2d Cir. 2004)).

198. Grimm, *supra* note 20, at 367.

199. Griffin v. State, 19 A.3d 415, 416–28 (Md. 2011).

200. 167 S.W.3d 98, 104–05 (Tex. Ct. App. 2005) (regarding the facts in light of a knowledgeable witness and in conjunction with the circumstances).

201. *Id.* at 105.

202. *Id.* (discussing the victim's familiarity "with Shea's e-mail address and that she had received the six e-mails in question from Shea").

203. *Id.*

204. *See supra* Part I.A (outlining Rule 901's low standard).

205. *Shea*, 167 S.W.3d at 105.

206. *See* Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 553–54 (D. Md. 2007) (arguing for creativity from counsel in authenticating evidence "regardless of whether there is a particular example in Rule[] 901 . . . that neatly fits").

207. *Shea*, 167 S.W.3d at 105.

208. WEINSTEIN & BERGER, *supra* note 57, § 901.03[2] ("[T]he 'knowledge' requirement of Rule 901(b)(1) is liberally construed.").

209. *Shea*, 167 S.W.3d at 105.

application.[210] The *Griffin* majority's rigid authentication analysis conflicts with this reality.

III. THE *GRIFFIN* DISSENT ARTICULATES THE APPROPRIATE AUTHENTICATION STANDARD FOR SOCIAL NETWORKING EVIDENCE

The *Griffin* dissent's approach represents a continuous and logical progression of evidence law because it recognizes that the current legal framework for authenticating social networking evidence is adequate.[211] Rule 901 provides the language of this framework—authenticity depends on whether a proponent has introduced evidence that is sufficient to support a finding that the evidence to be authenticated is genuine.[212] Courts have overwhelmingly interpreted this language to mean that evidence can be authenticated if "a reasonable juror could find in favor of authenticity."[213]

Historically, courts have applied the reasonable juror standard to different forms of evidence.[214] Because of the tremendous growth of electronic communication and information storage, courts quickly adapted by applying this standard to electronic evidence.[215] From there, the question of whether "the existing rules of evidence adequately deal with the admissibility of electronic evidence" arose.[216] Although some commentators answer this question in the negative, the overwhelming consensus is that courts should continue to apply the reasonable juror standard when authenticating electronic evidence.[217]

In re F.P., in which the court upheld Rule 901's traditionally low standard, best articulates the rationale behind this consensus.[218] There the court deliberately eschewed the notion that it should apply a heightened authentication standard when dealing with electronic evidence:

> Essentially, appellant would have us create a whole new body of law just to deal with e-mails or instant messages. The argument is that

---

210. *See supra* notes 100–03 and accompanying text (discussing an analysis in which circumstantial evidence can supplement an analysis under Rule 901(b)(1)); *see also* WEINSTEIN & BERGER, *supra* note 57, § 901.03[1] ("Parties may use any of the methods listed in Rule 901(b), any combination of them, or any other proof that may be available to carry their burden of showing that the proffered item of evidence is what they claim it to be.").

211. Griffin v. State, 19 A.3d 415, 429 (Md. 2011) (Harrell, J., dissenting) (arguing that a reasonable juror standard under Rule 901 could be applied to the authentication of information taken from a social networking website).

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

213. *Griffin*, 19 A.3d at 429 (Harrell, J., dissenting) (citations omitted).

214. *See supra* notes 44–48 and accompanying text.

215. *See supra* Parts I.B.1–3.

216. Grimm, *supra* note 20, at 361–62 (finding that admitting and authenticating electronic evidence is an inevitable outcome).

217. *See supra* note 211.

218. 878 A.2d 91, 95–96 (Pa. Super. Ct. 2005) (noting that electronic evidence does not require unique rules).

> e-mails or text messages are inherently unreliable because of their relative anonymity and the fact that while an electronic message can be traced to a particular computer, it can rarely be connected to a specific author with any certainty. Unless the purported author is actually witnessed sending the e-mail, there is always the possibility it is not from whom it claims.[219]

The court also observed that the danger arising from this uncertainty of authorship is not a novel issue; written documents have always posed the same problem.[220] Therefore, the court saw no reason to craft an entirely new set of rules to govern the admissibility of evidence that was presented in a unique form but created no unique issues.[221]

This same rationale should apply to the authentication of social networking websites. Comparable to other advances in electronic media, social networking websites provide users with a new means through which they can communicate and share information.[222] As a result, social networking websites also create new opportunities for people to masquerade online as someone else.[223] However, does this mean that courts should "create a whole new body of law"[224] for social networking sites? If so, what will happen when courts are again confronted with the next inevitable evolution in communication technology? The implementation of new authentication standards for every advancement in telecommunications will create tremendous burdens on courts and practitioners while providing only marginal benefits.[225] Although social networking websites present evidence in a unique form, they do not present unique authentication issues that require a heightened authentication

---

219. *Id.*

220. *Id.* at 95 (observing that "[a] signature can be forged; a letter can be typed on another's typewriter; distinct letterhead stationary can be copied or stolen").

221. *Id.* at 95–96.

222. *See supra* Part I.C.1.

223. *See supra* note 168 and accompanying text; *see also* John Robinson Thomas, *Legal Responses to Commercial Transactions Employing Novel Communications Media*, 90 MICH. L. REV. 1145, 1158 (1992) ("Although the propensity of telefacsimiles toward darkening, skipped lines or pages, and undetected alteration is worrisome, these characteristics should not . . . increase the required standard of authentication beyond that of ordinary writings.").

224. *In re F.P.*, 878 A.2d at 95–96.

225. *See supra* note 184 and accompanying text.

standard.[226] The existing authentication framework will suffice, just as it did when other forms of electronic evidence emerged.[227]

One could easily imagine a *Griffin*-like scenario arising in the future. For example, Party A posts on her Facebook profile page, and Party B seeks to use the post in court. Under the *Griffin* standard, Party B would need to: (a) get A to admit that A owns the profile and authored the incriminating post; (b) obtain A's computer; or (c) bring a Facebook legal compliance officer into court to testify.[228] These options leave B in a position of either "jump[ing] through [burdensome] hoops"[229] to authenticate the page or foregoing the opportunity to present potentially valuable evidence.

Alternatively, under the reasonable juror standard, B would likely be able to authenticate the post based on the information contained in the profile page. Most profile pages contain information similar to Barber's profile: a picture of the profile owner and personally identifying information.[230] Admittedly, this information, by itself, does not guarantee that Party A owns the page and created the incriminating post. There is a small possibility that an imposter

---

226. Warren Moïse, *BTW, R U Ready 4 Electronic Communications?*, 19 S.C. LAW. 11, 11 (2008) ("Law journal articles abound about 'e-mails,' 'e-discovery,' e-this and e-that, as if authentication of electronic communications were something new. However, we've been doing this for a century with telegraphs, telephone calls and even radio communications. Under the common law, a telegraph, telephone call, radio transmission or old-fashioned letter may be authenticated by circumstantial evidence though the recipient of the message never saw the sender of the message. (Not much different from an e-mail, huh?).").

227. Sheldon M. Finkelstein & Evelyn R. Storch, *Admissibility of Electronically Stored Information: It's Still the Same Old Story*, 23 J. AM. ACAD. MATRIM. LAW. 45, 68 (2010) ("Admissibility of ESI underscores the adage that everything old is new again. We must apply the familiar rules to types of evidence not even contemplated when the rules were written. Yet, those rules are sufficiently adaptable to those who are prepared."); Jonathan D. Frieden & Leigh M. Murray, *The Admissibility of Electronic Evidence Under the Federal Rules of Evidence*, 17 RICH. J.L. & TECH. 1, 2 (2011) ("It is important to remember that there is nothing 'magical' about the admission of electronic evidence. The prevalence of electronic evidence has required no substantial changes to the Federal Rules of Evidence. In analyzing the admissibility of such evidence, it is often best to treat it as originating from the most similar, non-electronic source as thoughtful application of traditional evidentiary principles will nearly always lead to the correct result. Thus, while electronic evidence may present some unique challenges to admissibility and complicate matters of establishing authenticity and foundation, it does not require the proponent to discard his knowledge of traditional evidentiary principles or learn anything truly new."); Keiko L. Sugisaka & David F. Herr, *Admissibility of E-Evidence in Minnesota: New Problems or Evidence As Usual?*, 35 WM. MITCHELL L. REV. 1453, 1456 (2009) (concluding that the Minnesota evidence law had successfully dealt with authentication of electronic evidence for years); *see also supra* Parts I.B.1–3.

228. Griffin v. State, 19 A.3d 415, 418 (Md. 2011).

229. Goode, *supra* note 4, at 7–8 (stating that requiring additional proof for electronic evidence makes lawyers jump through hoops or risk losing reliable evidence).

230. *Help Center*, FACEBOOK http://www.facebook.com/help/?page=216501321702579 (last visited Oct. 3, 2012); *see also Griffin*, 19 A.3d at 418 (illustrating that the MySpace profile in question had the characteristics of a typical profile page because it contained the alleged owner's age, gender, hometown, birth date, and photographs).

could have obtained A's picture and personal identification information, created a fake Facebook account in A's name, posted A's stolen picture and identification information on the fake account, and authored the incriminating post on the fake account in A's name. However, litigants should not be required to go through an extraordinary and burdensome process simply to assuage a concern that fraud might exist. A court faced with this scenario is confronting the same issue that exists with a handwritten letter, an instant message as in *In re F.P.*, an e-mail as in *Shea*, or a one-way website as in *Jarritos*. As the court in *In re F.P.* discussed, "[u]nless the purported author is actually witnessed sending the e-mail, there is *always* the possibility it is not from whom it claims."[231] Although social networking evidence presents a new form of evidence, it does not present a new problem. Therefore, a new authentication standard is unnecessary.

IV. CONCLUSION

Computer technology's exponential rate of change[232] will continue to present challenges to lawyers and judges alike.[233] Thus far, the flexibility of the Federal Rules of Evidence and the analogous state rules has enabled their successful application to evidence in the form of e-mail, instant messages, and websites. The legal community now faces a new, yet deceptively familiar, type of technology in social networking websites. The meteoric rise and well-documented popularity of these websites leaves no doubt that computer users will continue to make massive quantities of information available on these sites. Litigators will inevitably seek to use this information against their opponents, and opponents will inevitably seek to minimize their damaging effects, with the finder of fact ultimately deciding which side is more convincing. Imposing a heightened authentication standard for fear of the unknown needlessly disrupts this process. Opinions, such as *Griffin*, that have imposed such a standard should be relegated to the dusty bin with landlines, tv anenna, and those marginalized cases in which courts have taken an overly cautious approach toward technological progression and the rules of evidence.[234]

---

231. *In re* F.P., 878 A.2d 91, 95 (Pa. Super. Ct. 2005) (emphasis added).

232. *See supra* note 105 (discussing the evolution of the Internet from "web 1.0" to "web 2.0"). Not only has the technology evolved, but also the number of people using the technology—and the amount that they use it—has dramatically increased. *See supra* note 15. The legal relevance of the number of people using these websites cannot be understated. *See* Minotti, *supra* note 14, at 1059–68 (discussing cases where evidence derived from social networking websites has profoundly affected the outcome of a case).

233. *See supra* Part I.D.1 (discussing the challenges faced by the Maryland Court of Special Appeals and the Maryland Court of Appeals in deciding *Griffin*).

234. Finkelstein & Storch, *supra* note 227, at 46 ("After a time, when more judges will have been raised on computers, the suspicion in several judicial quarters surrounding the creation and potential alteration of ESI may diminish, and the requirements for admissibility may be less

demanding. But, for now, there remain substantial pockets of judicial skepticism which result, in some courts, in exacting foundational requirements you must be prepared to satisfy.").