Endnotes

2012

Griffin v. State: Setting the Bar Too High for Authenticating Social Media Evidence

Brendan W. Hogan

Note

GRIFFIN v. STATE: SETTING THE BAR TOO HIGH FOR AUTHENTICATING SOCIAL MEDIA EVIDENCE

BRENDAN W. HOGAN*

In *Griffin v. State*,[1] the Court of Appeals of Maryland found that a printout from a MySpace page, offered to demonstrate that a witness had been threatened into providing inaccurate testimony at an earlier trial, was not properly authenticated at trial because, despite the fact that the printout contained identifying characteristics the lower courts found sufficient for authentication,[2] the risk of "manipulation . . . by someone other than [the] purported creator and/or user" was too great to allow the printout into evidence.[3] This holding improperly distinguished social media evidence from other forms of electronic evidence and suggested an artificially high authentication threshold for social media evidence presented at trial.[4] The court further erred in creating a higher standard for authentication of social media evidence by stating a non-exclusive list of three means for authentication, because neither the plain text of the Maryland Rules of Evidence nor traditional authentication procedures support such a system.[5] The court should have affirmed the lower court ruling that the evidence was admissible because the prosecution met its burden of proof and showed that the evidence was what it was purported to

* Brendan Hogan is a second-year student at the University of Maryland Francis King Carey School of Law, where he is a staff member of the *Maryland Law Review*. He wishes to thank his wife, Nora-Anne Hogan, son, Declan Michael Hogan, family, and friends for their continued love and support. He also wishes to thank Chief Magistrate Judge Paul W. Grimm for his invaluable insight and suggestions in writing this Note, and his editors Lindsey N. Lanzendorfer, Kristina V. Foehrkolb, D. Jack Blum, Molly K. Madden, Esther R. Houseman, and Stephen Kiehl.

1. 419 Md. 343, 19 A.3d 415 (2011).

2. Griffin v. State, 192 Md. App. 518, 544, 995 A.2d 791, 807 (2010), *rev'd*, 419 Md. 343, 19 A.3d 415 (2011).

3. *Griffin*, 419 Md. at 348, 357–58, 19 A.3d at 418, 424.

4. *See infra* Part IV.A.

5. *See infra* Part IV.B.

be; the defense offered no evidence to rebut this presumption.[6]

I. THE CASE

Early in the morning of April 24, 2005, Darvell Guest was shot seven times in the women's bathroom of Ferrari's Bar in Perryville, Maryland.[7] Antoine Levar Griffin was charged with the murder and subsequently tried for the first time in August 2006.[8] At the first trial, Griffin's cousin, and an eyewitness to the murder, Dennis Gibbs, "testified that [he] did not see [Griffin] pursue the victim into the bathroom with a gun."[9] The first trial ended in a mistrial and Griffin was retried in January 2008.[10]

At the second trial, Gibbs testified again.[11] This time, however, other witnesses stated that Griffin *did* pursue Guest into the bathroom and Gibbs testified that Griffin and Guest were the only other individuals in the bathroom at the time the shots were fired.[12] Gibbs stated that he lied in the first trial because he had been threatened by Griffin's girlfriend, Jessica Barber, before the start of the first trial.[13]

To prove that Barber had threatened Gibbs before the first trial, the prosecution offered a printout from a MySpace profile page allegedly belonging to Barber.[14] The page contained the statement: "JUST REMEMBER, SNITCHES GET STITCHES!! U KNOW WHO YOU ARE!!"[15] The State introduced this evidence to corroborate Gibbs's contention that he had been threatened.[16] The MySpace profile was in the name of "SISTASOULJAH," but the State contended that it belonged to Ms. Barber.[17] The printout contained biographical data indicating that the author was a 23-year-old female from Port Deposit, Maryland, and listing the individual's birthday as "10-2-83."[18]

6. *See infra* Part IV.B.1.
7. *Griffin*, 192 Md. App. at 523, 995 A.2d at 794.
8. *Id.*
9. *Id.*
10. *Id.*
11. *Id.*
12. *Id.* at 523–24, 995 A.2d at 794–95.
13. *Id.* at 524, 995 A.2d at 795.
14. *Id.*
15. *Id.*
16. *Id.*
17. *Id.* at 526–27, 995 A.2d at 796.
18. *Id.* at 526, 995 A.2d at 796. While the Court of Special Appeals' opinion states the printout identified the author as from "Fort Deposit," Maryland, there is no Fort Deposit in Maryland. The town is *Port* Deposit. The Court of Appeals, in its opinion, correctly identified the town.

The profile also contained a photo of an embracing couple, which all parties agreed appeared to be Griffin and Barber.[19]

The defense counsel objected to the printout, arguing that the State had failed to sufficiently establish a "connection" to Barber, and that it had failed to question her about the profile when she was on the stand.[20] The prosecution asserted that the profile could be authenticated by Sgt. John Cook, whom the defense was permitted to question through a *voir dire* exam outside the presence of the jury.[21] Sgt. Cook testified that he knew the profile page belonged to Barber because of the picture of her and Griffin on the page, the reference to their children, and the listed birth date.[22] The State also called Barber to testify, during which time Barber said that she was dating Griffin, who sometimes went by the nickname "Boozy," and that Barber and Griffin lived together with their two children.[23] Barber, who was called to testify by only the prosecution, was not asked about the MySpace profile by either party.[24]

The trial court admitted a redacted portion of one page of the profile including the photo, "a description of the page creator as a 23 year-old female from Fort Deposit, and a portion of the" statement, finding that the evidence was admissible for the limited purpose of corroborating the threat Barber allegedly made to Gibbs.[25] The trial court did not comment on the authenticity of the printout.[26] Without waiving Griffin's objection, defense counsel stipulated to a statement about the authenticity of the printout in lieu of testimony from Sgt. Cook.[27] The court reviewed the stipulation during jury instruction, stating that "Sergeant Cook went online to the Web site My Space and downloaded an entry there, the redacted version of which is in evidence, and that he would have testified that there was a photo there of Miss Barber."[28]

The jury convicted Griffin of second degree murder, first degree assault, and use of a handgun in the commission of a felony or crime of violence in the fatal shooting of Darvell Guest on April 24, 2005.[29]

19. *Id.* at 526–27, 995 A.2d at 796.
20. *Id.* at 527, 995 A.2d at 796.
21. *Id.*, 995 A.2d at 796–97.
22. *Id.*, 995 A.2d at 797.
23. *Id.* at 526, 995 A.2d at 796.
24. *Id.* at 526–27, 529, 995 A.2d at 796, 798.
25. *Id.* at 527–29, 995 A.2d at 797–98.
26. *Id.*
27. *Id.* at 528, 995 A.2d at 797.
28. *Id.* at 529, 995 A.2d at 798.
29. *Id.* at 523, 995 A.2d at 794.

Griffin appealed to the Maryland Court of Special Appeals on the grounds that the trial court erred in admitting the MySpace printout.[30] The Court of Special Appeals affirmed the conviction, ruling that the evidence was properly admitted because the prosecution, through the stipulated testimony provided by the police officer, had provided sufficient evidence to authenticate the printout.[31] Griffin petitioned for a writ of certiorari, and the state filed a conditional cross appeal.[32]

The Court of Appeals granted certiorari to consider whether the trial court erred in admitting the MySpace printout and, if so, whether the error was reversible.[33]

II. LEGAL BACKGROUND

The rapid growth and spread of new types of communication technology in the past twenty years—cell phones, text messaging, online instant messaging programs, and social media—have prompted a reevaluation of an often overlooked area of evidentiary law: authentication.[34] Maryland courts have had few opportunities to address the authentication of electronic sources of evidence and have never before addressed the issue of social media evidence in the authentication context.[35] Authentication standards, however, have not changed from their early common law origins—requiring only that the party seeking to introduce the evidence establish by a preponderance of the

30. *Id.* The petitioner also argued that the trial court erred in permitting the prosecution to incorrectly describe "reasonable doubt" in his rebuttal and that the trial court erred in denying appellant's request for a mistrial following an outburst by the mother of a witness. *Id.* These arguments were not ultimately relevant to the final disposition of the appeal as the court ruled against Griffin on his additional grounds for appeal. *Id.* at 548, 552, 995 A.2d at 809, 811.

31. *Id.* at 523, 543–44, 995 A.2d at 794, 806–07.

32. Griffin v. State, 419 Md. 343, 346–47, 19 A.3d 415, 417 (2011).

33. *Id.*

34. *See generally* Hon. Paul W. Grimm, *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, 370–71 (2009) (noting that "[c]hat room and text or instant messaging 'dialogues' . . . pose unique challenges to authentication . . . .").

35. *See* State v. Bryant 361 Md. 420, 422, 761 A.2d 925, 926 (2000) (determining the authenticity of toxicology report under MD. R. 5-902); Clark v. State, 188 Md. App. 110, 118–19, 981 A.2d 666, 670–71 (2009) (determining the authenticity of a 911 emergency call); Dickens v. State, 175 Md. App. 231, 237–38, 927 A.2d 32, 36 (2007) (discussing the authenticity of text messages sent to the victim prior to her murder). *See also Griffin*, 192 Md. App. at 538, 995 A.2d at 803 ("Despite the pervasive popularity of social networking sites and their potential as treasure troves of valuable evidence, Maryland appellate courts have not yet addressed the issue of authenticating anonymous or pseudonymous documents printed from social media Web sites.").

evidence that the information is what its proponent claims it to be.[36] The same authentication standards that originated in the common law and were codified by the Federal Rules of Evidence and, later, by the Maryland Rules of Evidence have been applied to electronic sources of evidence without modification.[37]

A. Authentication Generally

The existence of specifically and individually codified authentication standards is a relatively new development in the history of Maryland law.[38] The basic purpose of authentication, however, has not changed for centuries: the proponent of the evidence must, as a condition precedent to the evidence's admission, demonstrate that the evidence is what the proponent purports it to be.[39]

Prior to the adoption of the Maryland Rules of Evidence in 1993, the Maryland standard for authentication was based on common law, state statutes, and court rules,[40] but following a trend which began in the federal courts in the 1970s, the Maryland Court of Appeals opted for a rules-based approach modeled on the success of the Federal Rules of Evidence.[41] The rules-based approach laid out in the Maryland Rules of Evidence has reduced the number of authentication disputes warranting a written decision in Maryland.[42] Indeed, since

36. *See infra* Part II.A–B.

37. *See infra* Part II.B.

38. *See* Alan D. Hornstein, *The New Maryland Rules of Evidence: Survey, Analysis and Critique*, 54 MD. L. REV. 1032, 1032 (1995) (discussing the adoption of the Maryland Rules of Evidence).

39. *Id.* at 1078.

40. *Id.* at 1032.

41. *See* Adoption of New Title 5, Rules of Evidence, 333 Md. XXXV, XXXIX (1993) (Chasanow, J., dissenting in part) (noting that the new rules of evidence adopted by the court, despite changes to "over 80%" of the rules, were "patterned after the Federal Rules of Evidence"). The similarity between the state and federal rules is obvious when compared side-by-side. In fact, the wording of the rules is almost identical in many places. *Compare, e.g.*, FED. R. EVID. 901(a) ("To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce *evidence sufficient to support a finding that the item is what the proponent claims it is.*") (emphasis added), *with* MD. R. 5-901(a) ("The requirement of authentication or identification as a condition precedent to admissibility is satisfied by *evidence sufficient to support a finding that the matter in question is what its proponent claims.*") (emphasis added).

42. Only thirteen cases involving authentication have been decided by Maryland appellate courts since 1993. Miller v. State, 421 Md. 609, 28 A.3d 675 (2011); Washington v. State, 406 Md. 642, 961 A.2d 1110 (2008); State v. Bryant, 361 Md. 420, 761 A.2d 925 (2000); Dep't of Pub. Safety and Corr. Serv. v. Cole, 342 Md. 12, 672 A.2d 1115 (1996); Carpenter v. State, 196 Md. App. 212, 9 A.3d 99 (2010); Clark v. State, 188 Md. App. 110, 981 A.2d 666 (2009); Dickens v. State, 175 Md. App. 231, 927 A.2d 32 (2007); Wagner v. State, 160 Md. App. 531, 864 A.2d 1037 (2005); Odum v. State, 156 Md. App. 184, 846

the adoption of the new rules in 1993, Maryland's appellate decisions on authentication have dealt almost solely with applying the authentication rules to new types of technology, each of which applied authentication standards in the Maryland Rules of Evidence without modification.[43]

1. Development of Authentication Standards in Maryland Prior to the Adoption of the Federal Model

Prior to the adoption of the Rules of Evidence, Maryland used statutory provisions, rules of practice, and common law precedent to determine what evidence was admissible at trial.[44] Authentication standards were not considered a separate area of law, but rather, the authenticity of a piece of evidence, as well as its relevancy to the charges or claims in the case, was considered as part of the foundation of the evidence.[45]

Early authentication standards were relatively lax, only requiring a prima facie showing that the evidence was what its proponent claimed it to be.[46] Authenticity, similar to relevance, was therefore treated as a threshold issue with the ultimate decision as to the believability and value of the evidence left to the jury.[47] Common law methods of authentication were generally divided into two groups: authentication by direct proof and authentication by circumstantial

A.2d 445 (2004), *aff'd*, 412 Md. 593, 989 A.2d 232 (2010); Bradshaw v. State, 139 Md. App. 54, 773 A.2d 1087 (2001); Gerald v. State, 137 Md. App. 295, 768 A.2d 140 (2001); State v. Brown, 129 Md. App. 517, 743 A.2d 262 (1999); Champion Billiards Cafe, Inc. v. Hall, 112 Md. App. 560, 685 A.2d 901 (1996).

43. *See, e.g.*, *Dickens*, 175 Md. App. 231, 238–39, 927 A.2d 32, 36–37 (analyzing authenticity of several text messages and applying MD. R. 5-901). *But see* Clark v. State, 188 Md. App. 110, 118–19 981 A.2d 666, 670 (2009) (applying MD. R. 5-901 and discussing the admissibility of a 911 emergency call, which was not a new technology in 2009).

44. Hornstein, *supra* note 38, at 1032.

45. *See e.g.*, Camphor v. State, 233 Md. 203, 204–05, 196 A.2d 75, 75–76 (1963) (holding that evidence was admissible at trial without separately considering its authentication, but discussing testimony which tended to show that the evidence was authentic).

46. *See, e.g.*, Lauder v. State, 233 Md. 142, 144, 195 A.2d 610, 611 (1963) (admitting a store price tag as evidence of the price of the stolen object during a larceny trial after testimony from the store clerk stating that the tag would have been on the stolen item and a finding that the tag was not inadmissible hearsay).

47. *See Lauder*, 233 Md. at 144, 195 A.2d at 611 (assuming a document to be authentic when applying potential hearsay exceptions as a condition precedent to admissibility). *See also* CHARLES T. MCCORMICK, HANDBOOK ON THE LAWS OF EVIDENCE 395 (1954) (noting the connection between authenticity and relevance); 7 JOHN HENRY WIGMORE, EVIDENCE IN TRIALS AT COMMON LAW §§ 2128–29 (J.H. Chadbourn ed., Little, Brown & Co. rev. ed. 1978) (1901) [hereinafter WIGMORE, EVIDENCE]; Edmund M. Morgan, *The Law of Evidence, 1941–1945*, 59 HARV. L. REV. 481, 490 (1946) (opining that disputes over authenticity should be submitted to the jury).

evidence.[48] Authentication by direct proof required either (1) testimony by a witness with personal knowledge of the creation of the document (or knowledge of the "books of concern" for custodians of business records) or (2) testimony by an individual familiar with the handwriting of the purported author to confirm that the handwriting on the document is the same as the handwriting of the purported author.[49] In contrast, authentication by circumstantial evidence could be proven by a showing that (1) "a generation had passed since a document was written" and the document is "unsuspicious in appearance;"[50] (2) the document was obtained from the custody of a public official who would have such documents in the course of his regular duties;[51] (3) the document in question was obtained from the custody of a private person who is purported to be the author, if the court determined this was appropriate;[52] or (4) the letter or telephone message was a reply to an earlier conversation.[53]

Maryland courts have generally addressed authentication issues indirectly, treating the issue of authentication as a part of the broader question of admissibility. For example, in *Lauder v. State*[54] the Court of Appeals held that the price tag on a stolen tape recorder was admissible as evidence showing the recorder's value because the tag was identified by a witness and was a business record rather than hearsay.[55] In some instances, the "trustworthiness"—a term used interchangeably with authentication—of a document was considered along with possible hearsay exceptions as part of the same question of admissibility.[56] The development of authentication law in this manner left no clear standards for courts to determine whether a piece of evi-

48. MCCORMICK, *supra* note 47, at 398–406.

49. *Id.* at 398–401.

50. *Id.* at 401.

51. *Id.* at 403.

52. Propst v. State, 5 Md. App. 36, 43, 245 A.2d 88, 92 (1968) ("We hold, however, that the evidence was admissible as to Ruth Virginia May under the principle that writings taken from an accused pursuant to a lawful search are admissible without further proof of the genuineness.").

53. McCormick, *supra* note 47, at 404–05.

54. 233 Md. 142, 195 A.2d 610 (1963).

55. *Id.* at 144, 195 A.2d at 611.

56. *See, e.g.*, Morrow v. State, 190 Md. 559, 562–63, 59 A.2d 325, 326 (1948) (holding a receipt admissible where there was a statutory hearsay exception and it "would seem to meet the tests of 'necessity and circumstantial guaranty of trustworthiness'"(quoting Backun v. United States, 112 F.2d 635, 639 (4th Cir. 1940)). *See also* Jennifer L. Mnookin, *The Image of Truth: Photographic Evidence and the Power of Analogy*, 10 YALE J.L. & HUMAN. 1, 52 n.187 (1998) (noting that over time, in the context of photographic evidence, judges substituted tests looking to the trustworthiness of sources for strict authentication requirements).

dence was "trustworthy" or "authentic," leading to relatively lax standards for authentication.[57] Such lax standards were demonstrated in *Morrow v. State*,[58] in which the Court of Appeals ruled that a receipt was sufficiently trustworthy to be admitted into trial where it was generated in the normal course of business and there was no evidence that the receipt was not "trustworthy."[59] These lax standards of authentication remain evident in the modern application of authentication rules.[60]

2. The Process of Authentication at Trial

As a condition precedent to admissibility, the party seeking to admit a document or other information into evidence must show, by a preponderance of the evidence, that the document or information is authentic, and that information "is what its proponent claims."[61] Some sources of evidence—such as government publications or newspapers—are considered to be inherently trustworthy and therefore are self-authenticating.[62] These self-authenticating sources do not need additional evidence to be admitted, provided they are relevant.[63] All evidence that does not fall into one of the eleven exceptions of self-authenticating sources described in Md. Rule 5-902(a) requires that the party introducing the evidence make a prima facie

57. *Cf.* Propst v. State, 5 Md. App. 36, 43, 245 A.2d 88, 92 (1968) (holding that a document was properly authenticated because the writings were taken from an accused pursuant to a lawful search, and stating that such a finding "seems inherent in the holding of the Court of Appeals of Maryland in *Lauder v. State*, 233 Md. 142, 195 A.2d 610 [(1963)], and more particularly in *Camphor v. State*, 233 Md. 203, 196 A.2d 75 [(1963)]"). This statement reveals a lack of clear standards regarding authentication of evidence. The logic of the holding indicates exactly how lax the standards were because the *Propst* court held that simply because a piece of paper was taken from the defendant, he was assumed to have written it. *Id.*

58. 190 Md. 559, 59 A.2d 325 (1948).

59. *Id.* at 562–63, 59 A.2d 326.

60. *See* MD. R. 5-901, which only requires that a party show that the evidence is "sufficient to support a finding that the matter in question is what its proponent claims" and provides a non-exhaustive list of illustrations demonstrating authenticity.

61. MD. R. 5-901. Additionally, the process of authentication in Maryland courts is identical in almost all respects to the federal method—the only exception being the "comparison with authenticated specimens" method of authentication. In federal courts, both the jury and the judge (if it is a bench trial) can compare the specimens. *See* FED. R. EVID. 901(b)(3) (allowing "[a] comparison with an authenticated specimen by an expert witness *or the trier of* fact) (emphasis added). In Maryland, however, only an expert witness or the judge in a bench trial may compare an authenticated specimen with an unauthenticated one to determine if they are the same. MD. R. 5-901(b)(3).

62. MD. R. 5-902(a)(1)–(6).

63. MD. R. 5-902(a).

showing that the evidence is authentic.[64] This showing can be made in one of nine suggested ways: testimony of a witness with knowledge; non-expert opinion on handwriting; comparison with an authenticated specimen by the court or an expert; circumstantial evidence; voice identification; a telephone conversation where the circumstances show that the call was authentic; public records; evidence that the document is more than twenty years old and not suspicious; or a showing that the document is the result of a process or system that produces accurate results,[65] such as a breathalyzer test. If the court determines that the party seeking to introduce the evidence meets its burden of proving authenticity, then the document is admitted into evidence.[66] In some cases, however, authenticity can be demonstrated only if a condition of fact were found to be true; in these cases the court must "admit [the evidence] upon, or subject to, the introduction of evidence sufficient to support a finding by the trier of fact that the condition has been fulfilled."[67]

3. Authentication in the Maryland Rules of Evidence

The Maryland Rules of Evidence require "authentication or identification as a condition precedent to admissibility" which "is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims."[68] The Maryland Rules were adopted on December 15, 1993, by the Maryland Court of Appeals and made effective on July 1, 1994.[69] The rules were derived from the Federal Rules of Evidence, which were adopted on January 2, 1975, as an attempt to organize and update the common law rules of evidence.[70] Despite a change in the language of the Federal Rules of Evidence with the adoption of the Maryland Rules of Evidence, the methods and standards of authentication have remained consistent with common law principles.[71]

64. Gerald v. State, 137 Md. App. 295, 304–05, 768 A.2d 140, 145 (2001).

65. MD. R. 5-901(b).

66. MD. R. 5-901; MD. R. 5-104(a).

67. MD. R. 5-104(b).

68. MD. R. 5-901(a).

69. Adoption of Maryland Rules of Evidence, 333 Md. XXXV, XXXV (1993).

70. Pub L. No. 93-595, § 1, 88 Stat. 1943 (1975); *see* Adoption of Maryland Rules of Evidence, 333 Md. XXXV, XXXVI (1993) (Eldridge, J., dissenting) ("There has long been a movement in this country towards codifying all areas of the law and away from the common law approach.").

71. *Compare* MD. R. 5-901(a) (requiring evidence sufficient to support a finding of authenticity as a "condition precedent" to admissibility), *with* WIGMORE, EVIDENCE, *supra*

Maryland courts generally have applied two principles in interpreting the authentication rules since their adoption: first, the interpretation of the Federal Rules of Evidence is instructive in the application of the Maryland rules; and second, the burden of proof for auauthentication is "slight," requiring only "sufficient evidence that the jury ultimately might [find that the evidence is what its proponent claimed]."[72] Indeed, several authentication cases decided in Maryland since the adoption of the rules initially address the question of authentication by considering the application of Federal Rule of Evidence 901,[73] which Maryland Rule of Evidence 5-901 greatly resembles.[74] Each of these cases also sets low authentication standards and places a high level of trust in the jury's ability to judge the trustworthiness of evidence presented.[75] The broad scope of possible authentication methods is emphasized in the rules themselves, which in addition to providing eleven possible types of self-authenticating sources of evidence,[76] also explicitly state that the ten authentication methods outlined in Maryland Rule 5-901 are included "[b]y way of illustration only, and not by way of limitation."[77]

Maryland courts have broadly construed specific rules to apply across a number of diverse factual situations.[78] For example, in *Clark*

note 47, at 694 (noting that authentication rules ensure that evidence is "sufficient to go to the jury").

72. Dickens v. State, 175 Md. App. 231, 239, 927 A.2d 32, 37 (2007).

73. *See, e.g.*, Miller v. State, 421 Md. 609, 620–21, 28 A.3d 675, 681–82 (2011) (discussing the application of MD. R. 5-901(b)(3) and authentication by comparison with authenticated specimens in light of FED. R. EVID. 901(b)(3)); *Dickens*, 175 Md. App. at 239, 927 A.2d at 37 ("Under Federal Rule 901, from which Maryland Rule 5-901 is derived, the burden of proof for authentication is slight, and the court 'need not find that the evidence is necessarily what the proponent claims, but only that there is sufficient evidence that the jury ultimately might do so.'" (quoting United States v. Safavian, 435 F. Supp. 2d 36, 38 (D.D.C. 2006))).

74. *Compare* MD. R. 5-901 *with* FED. R. EVID. 901.

75. *Miller*, 421 Md. at 621, 28 A.3d at 682; *Dickens*, 175 Md. App. at 239, 927 A.2d at 37 (quoting *Safavian*, 435 F. Supp. 2d at 38).

76. MD. R. 5-902(a).

77. MD. R. 5-901(b).

78. *See, e.g.*, Bradshaw v. State, 139 Md. App. 54, 65–66, 773 A.2d 1087, 1094 (2001) (authenticating a violent "written poem or rap song" allegedly written by the defendant near the time of the murder after considering circumstantial evidence); Gerald v. State, 137 Md. App. 295, 304–05, 768 A.2d 140, 145–46 (2001) (holding that a letter was properly authenticated using circumstantial evidence under Md. R. 5-901(b)(4)). In both of these cases the court applied a single method of authentication, circumstantial evidence under Md. R. 5-901(b)(4), to evaluate the evidence presented to the court, despite differing contexts, sources of circumstantial evidence, and possible other methods of authentication. *Bradshaw*, 139 Md. App. at 65–66, 773 A.2d at 1094; *Gerald*, 137 Md. App. at 304–05, 768 A.2d at 145–46.

v. State,[79] the Maryland Court of Special Appeals broadly applied authentication rules in a 2007 domestic battery case involving the authentication of 911 recordings from the victim that described the assailant and the nature of the assault.[80] The 911 call was authenticated under Rule 5-901(b)(4), which permits "appearance, contents, substance, internal patterns, location, or other distinctive characteristics" to substitute for direct testimony or evidence as to the authentication.[81] The woman on the 911 call identified herself as "Marsha Thomas," stated that her assailant had abused her and told the operator that she would be waiting for the police near the front desk of the hotel in which she was staying.[82] Additionally, when police officers arrived at the hotel, they found a woman suffering from multiple injuries who had a driver's license with the name "Marsha Thomas."[83] The court found that this information provided sufficient "distinctive characteristics" under 5-901(b)(4).[84]

Even though Maryland has adopted formal rules of evidence, many of the cases that consider authentication issues look to cases handed down before the passage of the rules of evidence to determine whether or not the evidence presented is what its proponent purports it to be.[85] While the courts have not looked to the common law in every circumstance,[86] the influence of the early common law

79. 188 Md. App. 110, 981 A.2d 666 (2009).

80. *Id.* at 118–19, 981 A.2d at 670–71.

81. MD. R. 5-904(b); *Clark*, 188 Md. App. at 118–19, 981 A.2d at 670–71.

82. *Id.* at 119, 981 A.2d at 671.

83. *Id.*

84. *Id.*; MD. R. 5-901(b)(4). This rule is the descendent of the common law rule that "sundry circumstances (including other admissions and the like) may suffice" to authenticate evidence where no direct testimony is possible. *See also* Knoedler v. State, 69 Md. App. 764, 772–74, 519 A.2d 811, 815 (1987) (holding that circumstantial evidence was sufficient to authenticate phone calls and records, and mitigate the possibility of fraud or imposition). The implication of this holding is that sufficient circumstantial evidence is enough to overcome the minimal threshold for authentication and protect against the fear of fraud or imposition, while still allowing the jury to determine the proper weight for the evidence presented to it in the case.

85. *See Clark*, 188 Md. App. at 118–19, 981 A.2d at 671 (citing and quoting *Knoedler*, 69 Md. App. at 772–74, 519 A.2d at 815); Bradshaw v. State, 139 Md. App. 54, 66, 773 A.2d 1087, 1094 (2001) (citing Gray v. State, 53 Md. App. 699, 456 A.2d 1290 (1983)). *See also* Gerald v. State, 137 Md. App. 295, 305, 768 A.2d 140, 145–46 (2001) (suggesting a "totality of the circumstances" method of authentication not explicitly listed in the rules of evidence).

86. *See, e.g.*, Carpenter v. State, 196 Md. App. 212, 225–28, 9 A.3d 99, 106–08 (2010) (discussing the authentication of text messages without referencing the common law rules for the authentication of evidence in Maryland).

standards has played a significant role in how the Maryland courts have interpreted authentication standards in the rules of evidence.[87]

B. Authentication of Electronic Evidence

While the Maryland Court of Appeals has not adopted a formal standard for authenticating electronic evidence, the Court of Special Appeals has evaluated electronic evidence authentication issues in much the same way it has considered non-electronic evidence cases.[88] The federal courts and other jurisdictions that have adopted similar rules of evidence have considered electronic evidence in the authentication context and have established a relatively clear baseline for the analysis of similar types of evidence under the existing rules of evidence.[89] Some courts in other states have explicitly stated that the rules of evidence do not need to be supplemented to handle authentication of text messages, emails, social media, and the like.[90]

1. Application of Authentication Standards to Electronic Evidence in Maryland

The Court of Appeals has never addressed the authentication of electronic evidence and the lower Maryland courts have had only limited opportunities to consider how evidence from text messages, recovered cell phones, computers, websites, and other electronic sources can be authenticated.[91] In 2007, in *Dickens v. State*,[92] the Court of Special Appeals addressed the admissibility of a text message that a defendant purportedly sent to the victim in a domestic murder case.[93] The court found the text message was properly admitted because the defendant possessed the cell phone connected to the text message at the time of his arrest, and the defendant had made verbal

87. For example, in *Bradshaw*, 139 Md. App. at 65–66, 773 A.2d, 1094, the Maryland Court of Special Appeals cited the common law precedent of *Gray*, 53 Md. App. 699, 426 A.2d. 1290, to analyze an authentication issue under the Maryland Rules.

88. *See infra* Part II.B.1.

89. *See infra* Part II.B.2.

90. *See infra* Part II.B.3.

91. Other than *Griffin v. State*, there have only been three published Maryland cases dealing with authentication of "electronic communications," none of which have dealt with social media. *Carpenter*, 196 Md. App. at 225, 9 A.3d at 106 (addressing the authentication of information taken from a recovered cellular telephone); Dickens v. State, 175 Md. App. 231, 239, 927 A.2d 32, 37 (2007) (considering the authentication of text messages); Chaney v. Family Dollar Store of Md., No. 24-C-06-11462, 2007 WL 5997994, at *2 (Md. Cir. Ct. Dec. 26, 2007) (dealing with the authentication of a printout from a website).

92. 175 Md. App. 231, 927 A.2d 32 (2007).

93. *Id.* at 239, 927 A.2d at 37.

statements contemporaneous with and similar to the text message in question.[94] The court held that the evidence presented was sufficient to meet the "slight" burden on the proponent of the evidence.[95]

In *Carpenter v. State*,[96] the Court of Special Appeals found that caller ID information, including the name of the caller and the time of the phone call, recovered from a cell phone was properly authenticated where, along with additional circumstantial evidence, it was proven that "when [the victim], after answering a call to the cell phone, agreed to meet the caller at a gas station, the person who met [the victim] at the gas station was [the defendant]."[97] In *Carpenter*, the court adopted the *Dickens* standard for the authentication of evidence at trial, stating that because "the jury 'could infer, legitimately,' that [the defendant] made the calls missed and received by the cell phone" the information was properly authenticated by the party seeking its introduction.[98]

In *Chaney v. Family Dollar Store of Maryland*,[99] Circuit Court Judge W. Michel Pierson refused to admit a printout from the website "wunderground.com" in the absence of additional authenticating information.[100] The website printout contained weather reports stating that there was no precipitation in the location of the defendant's parking lots on the date of the plaintiff's slip and fall.[101] The court rejected the website's admission because the printout was unaccompanied by any other identifying evidence and lacked further information about the source.[102]

2. Federal Case Law on the Authentication of Electronic Evidence

Federal courts have had numerous opportunities to address the authentication of electronic evidence in recent years and have opted to apply existing evidentiary standards in these cases.[103] The devel-

94. *Id.* at 239–40, 927 A.2d at 37.

95. *Id.* at 239, 927 A.2d at 37 (discussing FED. R. EVID. 901) (quoting United States v. Safavian, 435 F. Supp. 2d. 36, 38 (D.D.C. 2006)).

96. 196 Md. App. 212, 9 A.3d 99 (2010).

97. *Id.* at 219–20, 228, 9 A.3d at 103, 108.

98. *Id.* at 228, 9 A.3d at 108 (quoting *Dickens*, 175 Md. App. at 239, 927 A.2d at 37).

99. No. 24-C-06-11462, 2007 WL 5997994 (Md. Cir. Ct. Dec. 26, 2007).

100. *Id.* at *1.

101. *Id.*

102. *Id.*

103. *See, e.g.*, Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 543 (D. Md. 2007) (noting that federal courts have been "quick to reject calls to abandon the existing rules of evidence" for electronic information, but stating that "courts increasingly are demanding that proponents of evidence obtained from electronically stored information pay more atten-

opment of electronic authentication standards in the federal system tracks closely to the historical origins of authentication standards with an emphasis on a prima facie showing of authenticity and a focus on the role of the jury in determining the relative weight to apply to evidence introduced by the parties and admitted by the court.[104] The consideration of electronic evidence has generally followed the same standards of authentication used for traditional forms of evidence.[105] In *Lorraine v. Markel American Insurance Co.*,[106] Chief Magistrate Judge Paul W. Grimm described the authentication of electronic evidence as "not a particularly high barrier to overcome" and noted that where electronic evidence is not admitted, the "failure to authenticate . . . almost always is a self-inflicted injury which can be avoided by thoughtful advance preparation."[107] The party seeking to introduce the exhibit must make a prima facie showing that the evidence is what he says it is.[108] The court does not need to find that the evidence is what its proponent claims it is, only that a reasonable jury might ultimately do so.[109]

Despite the similarities with the general approach to authentication of evidence, federal courts have noted that there is a duty to properly scrutinize electronic evidence and that such evidence may require higher levels of examination than traditional forms of evi-

tion to the foundational requirements than has been customary for introducing evidence not produced from electronic sources"). In some ways, the consideration of "electronic evidence" predates the modern concept of electronic communication, see, for example, *United States v. Reilly*, 33 F.3d 1396, 1404 (3d Cir. 1994), discussing the admissibility of radio telegrams.

104. *See Lorraine*, 241 F.R.D. at 541–42 (discussing the prima facie threshold for authentication of evidence regardless of the origin or type of evidence). *See also* United States v. Safavian, 435 F. Supp. 2d 36, 38 (D.D.C. 2006) (stating that the burden for authentication is met by a prima facie showing that the evidence is what its proponent claims it to be).

105. *Compare Lorraine*, 241 F.R.D. at 542 (stating that electronic evidence only requires a prima facie showing of authenticity to be admitted), *with* First State Bank of Denton v. Md. Cas. Co., 918 F.2d 38, 41 (5th Cir. 1990) (holding that to authenticate a phone call for evidentiary purposes, the proponent need only "offer 'sufficient authentication to make a prima facie case that would allow the issue of identity to be decided by the jury" (quoting United States v. Register, 496 F.2d 1072, 1077 (5th Cir. 1974))).

106. 241 F.R.D. 534 (2007). In *Lorraine*, the Court dismissed the parties' cross-claims for summary judgment in a civil action to enforce an arbitration award because neither party supported its affidavit with admissible relevant evidence. *Id.* at 534–35, 585. In writing the *Lorraine* opinion, Judge Grimm provided a comprehensive overview of the process required to thoroughly vet electronic evidence prior to admitting it in a court proceeding. *Id.* at 537–85.

107. *Id.* at 542.

108. *Id.*

109. *See* United States v. Safavian, 435 F. Supp. 2d. 36, 38 (2006) *(*explaining that authentication requires only "that there is sufficient evidence that the jury might find that the evidence is what it purports to be").

dence in some cases.[110] The analysis used by the courts, however, fits within the existing rules of evidence, rather than limiting the consideration to certain types of methods to show authentication.[111]

While a large number of cases in the federal system deal with electronic evidence,[112] there are no federal cases that have addressed the admissibility of evidence in the social media context.[113] The federal courts have, however, had the opportunity to consider social media in other contexts and have generally treated social media communication no differently than other forms of electronic evidence when considering such evidence in a non-authentication context.[114] Courts have had the opportunity to consider several types of similar factual circumstances: authentication of chat logs,[115] authentication of postings to a public Internet forum,[116] and authentication of informa-

110. *In re* Vee Vinhee, 336 B.R. 437, 444–45 (9th Cir. B.A.P. 2005) (recognizing that while the only difference between electronic and paper records is the format, the unique nature of the electronic format "presents more complicated variations on the authentication problem than for paper records").

111. For examples of federal courts applying traditional authentication methods while considering whether a proper foundation had been laid for the admission of electronic evidence, see United States v. Tank, 200 F.3d 627, 630–31 (9th Cir. 2000) (analyzing admissibility of exhibits reflecting chat room conversations); United States v. Simpson, 152 F.3d 1241, 1249–50 (10th Cir. 1998) (analyzing authentication of chat room printouts in a child pornography case); Telewizja Polska USA, Inc. v. Echostar Satellite Corp., No. 02 C 3293, 2004 WL 2367740, at *6 (N.D. Ill. Oct. 15, 2004) (analyzing admissibility of the content of a website).

112. *See supra* note 111 for a list of several cases discussing electronic evidence in a non-social media context. *See also Lorraine*, 241 F.R.D. 534 (discussing the applications of the Federal Rules of Evidence to electronic evidence in general).

113. There are many cases where social media is considered in other contexts, most often commercial law, civil procedure, or free speech contexts. The facts of those cases, however, very rarely turn on whether or not a specific piece of social media evidence is authentic and the issue of authenticity is rarely, if ever, addressed in those contexts. *See, e.g.*, Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 969 (C.D. Cal. 2010) (discussing the effect of the Stored Communications Act on subpoenas duces tecum served on Facebook, MySpace, and other social networking sites); Indep. Newspapers, Inc. v. Brodie, 407 Md. 415, 419, 966 A.2d 432, 435 (2009) (finding that a circuit court judge abused his discretion when ordering that five anonymous Internet forum posters' identities be revealed in a defamation case, without discussing the authentication of electronic evidence).

114. *See, e.g.*, United States v. Ragland, 434 F. App'x 863, 871 (11th Cir. 2011) (analyzing under Fed. R. Evid. 403 and 400, and admitting into evidence the partial music video taken from the defendant's MySpace page in a Hobbs Act case with ten armed convenience store robberies).

115. *Tank*, 200 F.3d at 630–31 (applying traditional rules of evidence and finding that chat records were admissible in a child molestation case).

116. Univ. of Kansas v. Sinks, 565 F. Supp. 2d 1216, 1231 (D. Kan. 2008) (holding that postings to a message board at the website KUsports.com were admissible only to show the declarants' mental state but not for the truth of the matter asserted).

tion posted directly to a website.[117] Despite these opportunities, courts have not found it necessary to augment or change the existing rules of evidence to deal with those very similar circumstances.[118]

3. Authentication of Electronic Evidence in Other States

While Maryland and federal courts have not had the opportunity to consider the authentication of evidence from a social media website, courts in several other jurisdictions have done so. A New York court held, in *People v. Clevenstine*,[119] that chat logs from MySpace were properly authenticated in a child molestation case where there was testimony from both victims stating that they had spoken to the defendant online, the defendant's wife testified that she had seen sexually explicit conversations on her husband's MySpace account, the messages were recovered from the victims' computer, and a MySpace employee testified that the message logs were created by a MySpace chat.[120] The defendant's claim that his account had been hacked was found to present a factual issue for the jury and was not proper grounds for appeal because it had not been asserted at trial.[121]

In *State v. Eleck*,[122] the Connecticut Appellate Court held that the defendant, who was convicted of assault, had failed to authenticate the authorship of messages sent via Facebook that were introduced at trial to impeach the victim witness for the State, who claimed she had not spoken to the defendant.[123] The only authentication of the message printouts was the testimony of the defendant, who stated that he had printed the messages from his computer and knew that the account which had sent the messages to him belonged to the victim.[124] Additionally, the victim denied sending the messages, claiming that

117. Williams v. Long, 585 F. Supp. 2d 679, 689 (D. Md. 2008) (finding that a printed webpage from the Maryland Judiciary Case Search website is self-authenticating under Rule 902(5)).

118. Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 543 (D. Md. 2007) (noting that courts have been "quick to reject calls to abandon the existing rules of evidence" when dealing with electronic information); *See also In re* F.P., 878 A.2d 91, 95 (Pa. Super. Ct. 2005) (applying existing authentication standards to Internet chat records and explicitly declining to change the authentication rules for electronic evidence).

119. 891 N.Y.S.2d. 511, 511 (N.Y. App. Div. 2009).

120. *Id.* at 514.

121. *Id.*

122. It is important to note that this case was decided after *Griffin v. State* and cites to the Court of Appeals decision as persuasive authority. *Id.* at 823–24 (citing Griffin v. State, 419 Md. 343, 363–64, 19 A.3d 415 (2011)).

123. *Id.* at 819–20, 824.

124. *Id.* at 821.

her account had been hacked.[125] The court, citing the Connecticut Code of Evidence,[126] found that the information provided by the defendant was insufficient to authenticate the messages as having been authored by the victim, especially in light of the fact that the victim claimed her account had been "hacked."[127]

Similarly, the Supreme Judicial Court of Massachusetts, in *Commonwealth v. Williams*,[128] held that chat records from MySpace were not properly authenticated in a murder trial where the only evidence of authenticity was the testimony of a single witness who claimed to have received the messages from the defendant's brother's account.[129] Unlike in *Eleck*, however, there was no testimony that the account was hacked, rather the court found that because there was "no testimony . . . regarding how secure such a Web page is, who can access a MySpace Web page, [or] whether codes are needed for access" the messages were not properly authenticated.[130]

III. THE COURT'S REASONING

In *Griffin v. State*, the Maryland Court of Appeals held that the pages allegedly printed from Barber's MySpace profile were not properly authenticated as per the Maryland Rules of Evidence, reversing the judgment of the Court of Special Appeals.[131] Judge Battaglia, writing for the majority, reasoned that "[t]he potential for abuse and manipulation of a social networking site by someone other than its purported creator and/or user" required a higher level of authentication than the prosecution had provided.[132] The court held that the information on the MySpace printout—a picture of Barber, along with her birth date and location—"were not sufficient 'distinctive characteristics' to authenticate" the redacted printout.[133] The court fur-

125. *Id.* at 824.

126. CONN. CODE OF EVID. § 9-1(a) (which states, in relevant part, "the requirement of authentication as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the offered evidence is what its proponent claims it to be").

127. *Eleck*, 23 A.3d at 824. It is interesting to note that the court did not address this issue as a matter of conditional relevance. There is conflicting evidence that the messages were authentic—the court accepts that the messages came from the victim's account, but the consideration as to whether or not the account had, in fact, been "hacked" would seem to be a matter for the jury to consider, and therefore, the messages should have been conditionally admitted under Conn. Code Evid. § 1-3(b).

128. 926 N.E.2d 1162 (Mass. 2010).

129. *Id.* at 1172.

130. *Id.*

131. 419 Md. 343, 347–48, 19 A.3d 415, 418 (2011).

132. *Id.* at 357–58, 19 A.3d at 424.

133. *Id.* at 357, 19 A.3d at 424.

ther suggested three means by which social media evidence could be authenticated, all of which impose a higher standard on social media evidence than other types of evidence.[134]

The court began its examination by restating a definition of social networking websites from an earlier case, in which such sites were defined as "'sophisticated tools of communication where the user voluntarily provides information that the user wants to share with others.'"[135] The primary focus of the court's analysis was the ease with which an individual could establish a social network account under a fictitious name or even assume the identity of another person by fraudulently creating an account in another person's name.[136] The court reasoned that the "potential for fabricating or tampering with electronically stored information on a social networking site . . . poses significant challenges from the standpoint of authentication of printouts of the site."[137]

The court then discussed the Maryland rules governing authentication of evidence, noting that two possible rules could apply: Md. Rule 5-901(b)(1), testimony of a witness with knowledge, and Md. Rule 5-901(b)(4), circumstantial evidence.[138] The court noted that this issue had not been considered previously in Maryland courts.[139]

The court continued its analysis of related opinions from other jurisdictions by noting that several courts have "suggested greater scrutiny" for authentication of electronic evidence due to "the heightened possibility for manipulation by other than the true user or post-

134. *Id.* at 363–65, 19 A.3d at 427–28. The three suggested means of authentication are: (1) asking the purported creator if he created the posting in question; (2) using computer forensics to examine a computer's Internet history and hard drive to determine whether a specific computer created the content in question; and (3) obtaining information directly from the social networking site in question. *Id.* These suggestions impose a higher standard than is articulated in the Maryland Rules of Evidence, which allow authentication of all types of evidence by circumstantial evidence alone, or by testimony of any witness with knowledge. MD. R. 5-901(b)(1), (4).

135. *Id.* at 351, 19 A.3d at 420 (quoting Indep. Newspapers, Inc. v. Brodie, 407 Md. 415, 424 n.3, 966 A.2d 432, 438 n.3 (2009)). The court also noted that MySpace, like other social networking sites, allows members to share photos, videos, and other information on personal web pages. *Id.* (quoting Doe v. MySpace, Inc., 474 F. Supp.2d 843, 845 (W.D. Tex. 2007), *aff'd*, 528 F.3d 413 (5th Cir. 2008)).

136. *Griffin*, 419 Md. at 352, 19 A.3d at 421. The court noted that one Boston-based Internet company had succeeded in obtaining nearly 200 Facebook "friends" for an account created in the name of a toy frog called "Freddi Staur." *Id.* at 353–54, 19 A.3d at 421 (citing Samantha L. Miller, Note, *The Facebook Frontier: Responding to the Changing Face of Privacy on the Internet*, 97 KY. L.J. 541, 542 (2009)).

137. *Griffin*, 419 Md. at 354, 19 A.3d at 422.

138. *Id.* at 354–55, 19 A.3d at 422.

139. *Id.* at 355, 19 A.3d at 422.

er."[140] The court, however, did draw a distinction between emails, instant messages, and text messages, on the one hand, and information posted on social networking or other websites, on the other, noting that the dangers of emails and similar communications are markedly reduced because they are intended for a limited number of recipients rather than the public at large.[141] In the end, the court suggested three possible ways to authenticate printouts from social networking sites.[142]

After reciting the facts of the case, the court determined that, because the prosecution had only offered limited evidence pertaining to the origin of the profile (the photo on the profile page of Barber and the purported location and birth date of the owner of the page), the prosecution failed to provide sufficient "distinctive characteristics" to properly authenticate the MySpace printouts.[143]

The court explicitly stated that, despite the prosecution's failure to authenticate the posting in this case, printouts from social media sites were not de facto inadmissible.[144] Rather, the court suggested a non-exhaustive list of three potential methods for authenticating social networking printouts: (1) testimony from the purported creator affirming that he had created the content; (2) forensic evidence from the computer of the purported creator; and (3) information about the creation of the content from the social networking site itself.[145] None of these methods were used to authenticate the MySpace printout in this case.[146]

The court found that, because the prosecution had described Gibbs as its "most important witness" and highlighted the importance of the "snitches get stitches" posting in its closing argument, the trial

140. *Id.* at 358–61, 19 A.3d at 424–26. Specifically, the court discussed the decisions of *Commonwealth v. Williams*, 926 N.E.2d 1162 (Mass. 2010), *People v. Lenihan*, 911 N.Y.S.2d. 588 (N.Y. Sup. Ct. 2010), and *United States v. Jackson*, 208 F.3d 633 (7th Cir. 2000), in noting the higher level of scrutiny that other courts had placed on electronic evidence from social networking sites. In all those cases, the courts found that the electronic evidence that was presented for admission was not properly authenticated due to a fear of fabrication or falsification. The court distinguished In Re *F.P.*, 878 A.2d 91 (Pa. Super. Ct. 2005), a case involving authentication of instant message chat, on the grounds that it was "unpersuasive in the context of a social networking site, because the . . . recipient [identified] his own distinctive characteristics," which was not the case in *Griffin*. *Griffin*, 419 Md. at 361, 19 A.3d at 426.

141. *Griffin*, 419 Md. at 361 n.13, 19 A.3d at 426 n.13.

142. *Id.* at 363–65, 19 A.3d at 427–28.

143. *Id.* at 357–58, 19 A.3d at 423–24.

144. *Id.* at 363, 19 A.3d at 427.

145. *Id.* at 363–64, 19 A.3d at 427–28.

146. *See id.* at 348–50, 19 A.3d at 418–19.

court's admission into evidence of the improperly authenticated MySpace printouts was reversible error.[147]

Judge Harrell, joined by Judge Murphy, dissented, arguing that the information presented by the prosecution—the photo of Ms. Barber and the defendant, Ms. Barber's birth date on the printout, a description of the purported creator of the website as a 23-year-old woman from Port Deposit, and references to freeing "Boozy"—were sufficient to authenticate the printout.[148] The dissent further argued that the Court of Appeals should have adopted the "reasonable juror" standard articulated by the Maryland Court of Special Appeals in *Dickens v. State*,[149] which states evidence should be admitted where there is enough information such that a reasonable juror could find the evidence presented to be authentic.[150] Judge Harrell argued that the "technological heebie jeebies" discussed in the majority opinion—the possibility of manipulation or abuse—should go to the weight of the evidence rather than its admissibility.[151]

IV. ANALYSIS

In *Griffin v. State*, the Court of Appeals attempted to reconcile the existing rules of evidence—authentication, specifically—with the rapid development of electronic communication, suggesting that separate rules of authentication should be applied to social media evidence used at trial.[152] The court's suggestion that social media evidence should be subject to a separate, higher level of authentication does not comport with the existing rules of evidence or the common-law origins of authentication standards.[153] Furthermore, under the existing rules of authentication, the prosecution provided sufficient circumstantial evidence for the trial court to admit the MySpace printout.[154]

147. *Id.* at 362–63, 19 A.3d at 427.

148. *Griffin*, 419 Md. at 365, 367, 19 A.3d at 428–29 (Harrell, J., dissenting).

149. 175 Md. App. 231, 239, 927 A.2d 32, 37 (2007) (quoting United States v. Safavian, 435 F. Supp. 2d 36, 38 (D.D.C. 2006)) (stating that "the burden of proof for authentication is slight").

150. *Griffin*, 419 Md. at 366–67, 19 A.3d at 429 (Harrell, J., dissenting) (citing *Dickens*, 175 Md. App. at 239, 927 A,2d at 37).

151. *Id.* at 367, 927 A.2d at 430.

152. *See supra* Part III.

153. *See infra* Part IV.A.

154. *See infra* Part IV.B.

A. Social Media Evidence Does Not Require Separate Authentication Standards

The court incorrectly concluded that social media evidence requires separate authentication standards. This conclusion was incorrect because, while social media evidence does pose a risk of possible manipulation or fraud, this risk is not more present in social media evidence than it is in other forms of evidence, electronic or otherwise.[155] Furthermore, the authentication methods suggested by the court for social media evidence fit within the existing authentication framework, thus there is no need to create a separate process of authentication specifically for this type of evidence.[156] Finally, the rules of evidence and the common-law precedent for authentication do not support the court's decision to establish a more stringent set of authentication standards solely for social media evidence.[157]

1. Social Media Is Not Distinguishable from Other Forms of Electronic Communication

The court's primary grounds for distinguishing social media from other forms of electronic evidence was that social media is an inherently insecure method of communication that can be easily fabricated.[158] While social media significantly changed the landscape of online communication, these changes are superficial from an authentication standpoint.[159] The court's distinction fails to consider that the two methods of fabrication or tampering mentioned by the court—"hacking" into a social media account or creating a false account on behalf of someone else—are at least as easy to accomplish with email and chat communication as they are with social media ac-

155. *See infra* Part IV.A.1.

156. *See infra* Part IV.A.2.

157. *See infra* Part IV.A.3.

158. Griffin v. State, 419 Md. 343, 361 n.13, 19 A.3d 415, 426 n.13 (2011).

159. The major contribution of sites like Facebook, MySpace, Friendster, Google+, LinkedIn, and Twitter has been a new ability to "friend," "follow," or "link" with other users to share personal, social, and professional information, or pass along an interesting bit of news. While this development has certainly changed with whom and how people communicate and the topics they communicate about, these social media developments have not changed much that would affect the central inquiry of an authentication issue: Is this evidence actually from the person its proponent claims it is? The question of authorship is central to determining the authenticity of any written statement, and as far as authorship is concerned the possibility of "fraud or imposition" is not very different in the social media context than it is in context of email or any other method of online communication. This is especially true where the security measures to protect email and social media accounts are often very similar, if not exactly the same (as is the case with Google's email and social media services).

counts because the security of these applications are largely similar.[160] The court found that online chat communication differed from the postings on a social networking site because the victim identified the distinctive characteristics in the chat records in *In re F.P.* (references in the chat record to the first name of the defendant, personal threats made by the defendant, and reference to the high school where the children attended) as the reason why he knew with whom he was communicating.[161] In *Griffin*, however, the police sergeant who printed the MySpace page listed the distinctive characteristics of the profile that led him to believe that it belonged to Barber, and these characteristics were stipulated to by both parties, though the parties disagreed with how these facts affected authenticity.[162]

The similarities drawn between the nonbinding case law cited by the court and the facts of *Griffin* do not support the court's finding in this case. While *Commonwealth v. Williams* and *Griffin v. State* bear some superficial similarities, as both are murder cases with evidence from MySpace, the "distinctive characteristics" identified in *Griffin*—a photo of Barber and Griffin, references to the defendant and their child, as well as Barber's birth date, city of residence, and a direct reference to the case[163]—are far more significant than the testimony of the one witness in *Williams*, who claimed that the messages she received were from the defendant's brother.[164] The facts of *People v. Lenihan*,[165] a New York murder case in which the defendant appealed because the trial judge refused to allow cross examination based on photos from MySpace, are similarly unpersuasive. *Lenihan* dealt with photographs that, while printed from MySpace, could have been doctored or altered regardless of their source in the manner suggested by

160. For example, compare the account creation procedures at Gmail (mail.google.com/mail/signup), Yahoo (new.mail.yahoo.com/addresses), Facebook (http://www.facebook.com), and MySpace (https://www.myspace.com/signup), all of which require a user name and password to be created and have similar protocols for determining password security. For a discussion of relative password security, see Dennis Guster et al., *Weak Password Security: An Empirical Study*, 17 INFO. SEC. J.: A GLOBAL PERSPECTIVE 45, 45–46 (2008). The conventional wisdom that average password security is weak has been proven to be accurate, regardless of the type of website for which the password is used. *See* Dinei Florêncio & Cormac Herley, A Large-Scale Study of Web Password Habits (2007), http://research.microsoft.com/pubs/74164/www2007.pdf (noting that users "frequently re-use passwords across multiple sites").

161. *Griffin*, 419 Md. at 361, 19 A.3d at 426 (discussing In re *F.P.*, 878 A.2d 91, 94 (Pa. Super. Ct. 2005)).

162. *Griffin*, 419 Md. at 350–51, 19 A.3d at 419.

163. *Id.* at 349, 357, 19 A.3d at 418–19, 424.

164. Commonwealth v. Williams, 926 N.E.2d. 1162, 1171–72 (Mass. 2010).

165. 911 N.Y.S.2d 588 (N.Y. Sup. Ct. 2010).

the judge in that case.[166] *United States v. Jackson*,[167] a wire fraud and obstruction of justice case where the defendant was alleged to have defrauded the United Parcel Service and racially harassed numerous prominent African-Americans, is also not an appropriate or persuasive authority in this case because the court discussed the authentication issue in dicta as the evidence was not admissible on other grounds.[168]

Furthermore, in all three cases, the court assumed facts that were not presented into evidence in *Griffin*—the possibility of a user other than the owner of the account in *Commonwealth v. Williams*,[169] the threat of photo-doctoring in *Lenihan*,[170] and the fraudulent creation of web postings in *Jackson*[171]—as its basis for finding that the information was not authentic. Even if these facts had been part of the record, however, the proper resolution of the discrepancy would have been to conditionally admit the evidence and allow the jury to determine which arguments were more credible.[172] In this case, there was no information in the record that supported the court's suggestion that the account was fabricated or falsified in some manner.[173]

Finally, the court ignored several appropriate comparisons when it sought to distinguish social media evidence from other forms of electronic evidence. For example, the majority addressed the authentication of emails only in a footnote, stating that "authentication concerns attendant to e-mails, instant messaging correspondence, and text messages differ significantly from those involving a MySpace profile and posting printout, because such correspondence is sent directly from one party to an intended recipient or recipients, rather than published for all to see."[174] The suggestion that the intended recipient has a bearing on the authenticity of the communication is not supported by the structure of the rules of evidence, which do not limit possible methods of authentication based on the origin of the evidence.[175] The court failed to consider the fact that the pri-

166. *Id.* at 592.

167. 208 F.3d 633 (7th Cir. 2000).

168. *Id.* at 635, 637–38.

169. 926 N.E.2d at 1172.

170. 911 N.Y.S.2d at 592.

171. 208 F.3d at 638.

172. FED. R. EVID. 104(b); Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 539–40 (D. Md. 2007).

173. Griffin v. State, 419 Md. 343, 357–58, 19 A.3d 415, 423–24 (2011).

174. *Id.* at 361 n.13, 19 A.3d at 426 n.13.

175. *See* MD. R. 5-901(b) ("By way of illustration only, and *not by way of limitation*, the following are examples of authentication or identification conforming with the requirements of this Rule.") (emphasis added). There are rules which allow additional means of au-

mary risk considered by the court, "manipulation . . . by someone other than [the] purported creator and/or user," is shared equally between email and social networking sites.[176] There are numerous cases dealing with the authentication of emails, and despite almost identical security and access mechanisms between the two platforms, courts have generally applied the traditional authentication rules, without modification, to email authentication questions.[177]

While the court is correct that text messages are more difficult to falsify,[178] since they are always associated with a phone number that can usually be connected to an owner,[179] there still exists the possibility that a given message could be fraudulent if the phone is shared among multiple individuals, stolen, or left unattended—a fact not suggested in the consideration of the authentication of text messages in *Dickens v. State*.[180] The risk of fraudulent or falsified communications being presented at trial exists regardless of the medium of communication; for example, text messages can be faked, online accounts can be hacked, and signatures can be forged.[181] The suggestion that social media and only social media requires a higher level of scrutiny reinterprets the rules of evidence in a way that is not consistent with their plain meaning and application.[182]

thentication based on the source of the evidence, but these rules do not limit authentication of that type of evidence to that method. *See, e.g.*, MD. R. 5-901(b)(5) (allowing identification of a voice by a witness who has previously heard the voice "at any time under circumstances connecting it with the alleged speaker," without differentiating between public and private contexts).

176. *Griffin*, 419 Md. at 357, 19 A.3d at 424; see *supra* note 158 and accompanying text.

177. *See* United States v. Safavian, 435 F. Supp. 2d 36, 38–40 (D.D.C. 2006) (discussing the admissibility of emails in a motion in limine prior to a wire fraud and corruption case and finding that the emails had been properly authenticated under the Federal Rules of Evidence where there were distinctive characteristics, such as email addresses and signatures, for the sender to be identified).

178. *Griffin*, 419 Md. at 361 n.13, 19 A.3d at 426 n.13.

179. *See* Dickens v. State, 175 Md. App. 231, 238, 927 A.2d 32, 36 (2007) (authenticating text messages based on the sender's telephone number).

180. 175 Md. App. 231, 238–40, 927 A.2d 32, 36–37 (2007).

181. For a recent example of the threat posed by falsification of electronic evidence on phone, see Mike Scarcella, *Defense Lawyers Seek iPhone 3G in Conspiracy Prosecution*, L. TECH. NEWS (Jan. 11, 2012), http://www.law.com/jsp/lawtechnologynews/PubArticleFriendlyLTN.jsp?id=1202537995906#.

182. Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 538 n.5 (D. Md. 2007) (noting that the Federal Rules of Evidence "apply to computerized data" and that Rule 102 contemplated flexibility to address technological developments) (quoting MANUAL FOR COMPLEX LITIGATION § 11.447 (4th ed. 2004))).

2. The New Methods of Authentication for Social Media Evidence Proposed by the Court Could Be Applied Easily Within Existing Authentication Standards

The *Griffin* court's suggested means for the authentication of social media—testimony from the purported creator, searching the computer of the purported creator of the social media account, and obtaining information directly from the social networking website—are valid suggestions for possible methods of authentication.[183] The rules of evidence do not posit an exclusive list of possible methods for authentication.[184] Indeed, the methods suggested in *Griffin* fit well within the established guidelines in the rules. Statements by either the purported creator or an individual from the social networking website are testimony of a witness with knowledge,[185] and any data recovered from the purported creator's computer or the social networking site itself is circumstantial evidence that the evidence is what the party presenting the evidence purports it to be.[186]

Furthermore, the methods outlined by the court are unnecessarily specific and fail to discuss other traditional methods of authentication that could be sufficient to meet the burden of authentication imposed by the rules.[187] Testimony from the alleged creator of the social media content would certainly be sufficient for authentication.[188] In many circumstances, however, testimony from another individual could be just as valuable, especially where, as in *People v. Clevenstine* and *In Re F.P.*, the individual is familiar with the writing style of the alleged creator of the content. Therefore, this individual can verify independently that the alleged poster did in fact post the con-

183. *Griffin*, 419 Md. at 363–65, 19 A.3d at 427–28.

184. MD. R. 5-901(b) (stating "[b]y way of illustration only, and not by way of limitation, the following are examples of authentication or identification conforming with the requirements of this Rule").

185. MD. R. 5-901(b)(1).

186. MD. R. 5-901(b)(4). For a discussion of the use of hash tags and metadata in authentication decisions, see Chief Magistrate Judge Grimm's discussion in *Lorraine*, 241 F.R.D. at 546–48, which explains how data from a computer or website can be used to demonstrate the "distinctive characteristics" of the electronic evidence.

187. Griffin v. State, 419 Md. 343, 363–64, 19 A.3d 415, 427–28 (2011). The court notes that *Griffin* should not be read to "suggest that printouts from social networking sites should never be admitted," stating that possible avenues of authentication will "continue to develop" and suggesting three "authentication opportunities" for social media evidence. *Id.* at 363, 19 A.3d at 427.

188. MD. R. 5-901(b)(1).

tent because he witnessed the posting first hand, or the posting is consistent with other statements or actions by the poster.[189]

In addition to testimonial evidence, as the court notes, physical evidence could be used to authenticate the posting, whether from the website host, Internet service provider, or the hard drive of the computer from which the information was posted.[190] This physical evidence could be supplemented or replaced by circumstantial evidence surrounding the posting or page, such as photos, other communications with friends around the same time, non-social media communications which support the assertion that the poster would have been likely to make those comments, or evidence that the postings were in fact made from the same physical location.[191]

3. The Historical Precedents for Authentication Do Not Support the Addition of Restrictive Standards Proposed by the Court

The authentication rules are rooted in common-law precedent that allows relatively lax standards to show whether the evidence in question is what its proponent claims.[192] The standards are purposefully lax because authentication is a threshold issue, and the ultimate determination as to the trustworthiness of the evidence is made by the jury who decides how much weight to give to the evidence presented by the parties.[193] A long history of Maryland case law from prior to the adoption of the Federal Rules of Evidence supports the treatment of authentication as a threshold issue, with only a minimal burden of proof required.[194] In *Lauder v. State*,[195] the Court of Appeals allowed a price tag, which was not attached to merchandise at the time of trial,

189. *People v. Clevenstine*, 891 N.Y.S.2d. 511, 514 (N.Y. App. Div. 2009), provides an example of the value of testimony from individuals other than the creator. In that case, the court found that sexually explicit communications between the defendant and two minor children defendant was alleged to have raped was properly authenticated where there was testimony from both victims and the defendant's wife as to the communications at issue. *Id.* This was also the case in *In Re F.P.*, 878 A.2d 91, 94–95 (Pa. Super. Ct. 2005), in which the court found that testimony from the victim stating he had engaged in online communications with the defendant was properly authenticated where the victim explained that the defendant identified himself to the victim, referenced personal interaction between the two boys, and mentioned the high school they both attended. *Id.*

190. *Griffin*, 419 Md. at 363–64, 19 A.3d at 427–28.

191. *See* MD. R. 5-901(b)(4) (stating "[c]ircumstantial evidence, such as appearance, contents, substance, internal patterns, location, or other distinctive characteristics" that demonstrate the validity of the evidence are acceptable means of authentication).

192. *See supra* Part II.A.1.

193. United States v. Nolan, 818 F.2d 1015, 1017 (1st Cir. 1987), *overruled on other grounds by* United States v. Hilton, 363 F.3d 58, 64 (1st Cir. 2004).

194. *See supra* Part II.A.1.

195. 233 Md. 142, 144, 195 A.2d 610, 611 (1963).

to be admitted into evidence as proof of the price of a stolen object despite a lack of supporting evidence as to its trustworthiness.[196] *Propst v. State*,[197] which held that writings taken from a person's home are authentic by virtue of the fact that they were recovered from that individual without "any further proof of genuineness," further demonstrates the lax authentication standards in Maryland's common law.[198]

These lax standards have carried forward into the modern era and been applied by Maryland courts in cases dealing with electronic evidence.[199] In both Maryland appellate decisions addressing the admissibility of electronic evidence prior to *Griffin*, specifically *Dickens v. State* and *Carpenter v. State*, the Court of Special Appeals reiterated authentication's role as a threshold issue at trial.[200] While this standard has not been adopted formally by the Maryland Court of Appeals, such a standard has been adopted in federal cases,[201] and such a standard is "almost direct authority impacting our construction of a Maryland analog rule."[202] By suggesting that social media evidence exclusively should be subjected to higher standards and limited methods of authentication, the court failed to consider the role of the jury in judging the relative value of evidence and imposed an unnecessary burden on parties seeking to prove the authenticity of social media evidence by forcing litigants to follow separate rules for this narrow, but increasingly important,[203] source of evidence.[204]

196. *Id.*

197. 5 Md. App. 36, 43, 245 A.2d 88, 92 (1968).

198. *Id.*

199. *See supra* Part II.B.1.

200. Carpenter v. State, 196 Md. App. 212, 228, 9 A.3d 99, 108 (2010) (reiterating the position adopted in *Dickens* and stating that, where "the jury 'could infer, legitimately,' that [the defendant] made the calls missed and received by the cell phone," the evidence was admissible at trial); Dickens v. State, 175 Md. App. 231, 239, 927 A.2d 32, 37 (2007) (analogizing to the comparable federal rule, stating that the burden for authentication under Federal Rule 901 is "slight").

201. *See, e.g.*, United States v. Safavian, 435 F. Supp. 2d 36, 38 (D.D.C. 2006) (quoting United States v. Reilly, 33 F.3d 1396, 1404 (3d Cir. 1994)) (explaining that the standard for authentication of evidence at trial is "slight" and intended as a threshold issue).

202. Griffin v. State, 419 Md. 343, 365–66, 19 A.3d 415, 428–29 (2011) (Harrell, J., dissenting) (citing Higgins v. Barnes, 310 Md. 532, 543, 530 A.2d 724, 729 (1987)).

203. For a discussion of the rise of social media evidence in lawsuits, see Michelle Sherman, *The Anatomy of A Trial With Social Media and the Internet*, 11 J. INTERNET L. 1, 9 (2011).

204. *See* Paul W. Grimm et al., *Back to the Future:* Lorraine v. Markel American Insurance Co. *and New Findings on the Admissibility of Electronically Stored Evidence*, 42 AKRON L. REV. 357, 366–68 (2009) (discussing the low bar for authentication of evidence at trial, regardless of the source of the evidence but noting that "[a]s electronic evidence becomes more ubiquitous at trial, it is critical for courts to start demanding that counsel give more in terms of authentication").

B. The Court's Decision to Exclude the MySpace Post Is Not Supported by Existing Rules of Evidence or Traditional Authentication Procedures

The *Griffin* court excluded the MySpace printout from evidence because the "potential for abuse and manipulation of a social networking site by someone other than its purported creator and/or user . . . requires a greater degree of authentication" than was provided at trial.[205] This holding is not supported by a plain reading of the Maryland Rules of Evidence,[206] nor does persuasive authority from other jurisdictions support such a holding in a manner that comports with established evidentiary principles in Maryland.[207]

1. A Plain Reading of the Maryland Rules of Evidence Does Not Support the Majority's Holding That the MySpace Printout Was Not Properly Authenticated at Trial

The Maryland Rules of Evidence state that "[t]he requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims."[208] This showing can be made through multiple methods.[209] In *Griffin*, the parties stipulated to facts that constituted circumstantial evidence that the posting was made by Barber.[210] Circumstantial evidence is sufficient for showing evidence authenticity when its "appearance, contents, substance, internal patterns, location, or other distinctive characteristics" show that "the offered evidence is what it is claimed to be."[211] In this case, the parties stipulated that a police sergeant would testify that the MySpace page contained a photograph which was recognizably Jessica Barber, a date of birth that matched Barber's, the statement "FREE BOOZY!!!! JUST REMEMBER SNITCHES GET STITCHES!! U KNOW WHO YOU ARE!!," and that Barber is the defendant's live-in fiancée.[212] These identifying and distinctive characteristics are sufficient to meet the minimal burden of authentication required in Mary-

205. *Griffin*, 419 Md. at 357–58, 19 A.3d at 424 (majority opinion).

206. *See infra* Part IV.B.1.

207. *See infra* Part IV.B.2.

208. MD. R. 5-901(a).

209. MD. R. 5-901(b).

210. *Griffin*, 419 Md. at 350–51, 19 A.3d at 419–20.

211. MD. R. 5-901(b)(4).

212. *Griffin*, 419 Md. at 350–51, 19 A.3d at 419–20. The page also listed the account owner's hometown as "Port Deposit, Maryland," which is the location Barber gave as her home, but that fact was not in the sergeant's stipulated testimony or presented to the jury. *Id.*

land because the circumstantial evidence demonstrates "that the evidence is what it is claimed to be."[213] Indeed, the majority does not dispute these facts, but rather assumes facts about the possible "abuse and manipulation" of the MySpace posting which were not part of the appellate record in this case.[214] Even if such evidence of manipulation were offered at trial, the determination of authenticity then would become an issue of fact to be decided by the jury under the rules for conditional relevance.[215] While the Court of Appeals noted that it was not asked to consider conditional relevance in this case,[216] it could have ruled *sua sponte* that conditional relevance was the proper means to resolve this evidentiary discrepancy.

2. *Persuasive Authority Suggests That the MySpace Printout Was Properly Admitted at Trial*

Federal and state courts that have addressed the admissibility of electronic evidence generally have applied the same rules of authentication to the electronic evidence as used for non-electronic evidence.[217] In the cases in which the party seeking to introduce the evidence at trial provided supporting facts showing that the offered evidence is what it purports to be, courts allowed the evidence to be admitted at trial.[218] Where courts determined that the evidence was not properly authenticated, lack of authentication was generally pre-

213. MD. R. 5-901(b)(4).

214. *See* Brief for the Petitioner, at 10–20, Griffin v. State, 419 Md. 343, 19 A.3d 415 (2011) (No. 74), 2010 WL 5096820, at *10–20 (Md. Nov. 4, 2010) (failing to provide specific evidence that the page was falsified or "hacked," but stating that the State had not met its burden of persuasion and failed to cite evidence in the record that showed or argued the page was a fake).

215. MD. R. 104(b) ("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.").

216. *Griffin*, 419 Md. at 365 n.15, 19 A.3d at 428 n.15.

217. *See, e.g.*, Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 538 n.5 (D. Md. 2007) (explaining that electronic evidence does not require new authentication standards); *In Re* F.P., 878 A.2d 91, 95–96 (Pa. Sup. Ct. 2005) (declining to apply new evidentiary standards to electronic evidence).

218. *See, e.g.*, Dickens v. State, 175 Md. App. 231, 239, 927 A.2d 32, 37 (2007) (finding that text messages admitted at trial were properly authenticated by a showing that the phone number belonged to the defendant and that the content of the messages were consistent with the proposition that they were sent by the defendant); People v. Clevenstine, 891 N.Y.S.2d 511, 514 (N.Y. App. Div. 2009) (finding that authentication standards were met as to MySpace chat records in a rape case in which both victims testified that they had chatted with the defendant on MySpace, the message records were retrieved from the victims' hard drive, a MySpace representative testified that the messages had been exchanged on the MySpace network, and the defendant's wife recalled seeing a sexually explicit message when viewing the defendant's MySpace account).

mised on one of two grounds: either the court finding that the evidence was not sufficient to meet the low burden of authentication[219] or the court assuming that the risk of falsification of electronic evidence requires a higher standard of proof from evidence offered from such sources.[220] The cases premised on falsification risk, however, do not comport with authentication standards in the Maryland Rules of Evidence, which do not provide for higher authentication standards based on a higher possibility of falsification.[221] The majority in *Griffin* held that the information presented by the prosecution was insufficient to meet authentication standards on its own, and further ruled that because of the greater risk of "abuse and manipulation" inherent in social networking sites, the evidence was not sufficiently authentic.[222] This holding and the subsequent extension of authentication standards are not supported by the existing rules of evidence and common law authentication standards in Maryland.

V. CONCLUSION

In *Griffin v. State*, the Court of Appeals of Maryland enunciated a new standard for the authentication of evidence from social networking websites.[223] The court created three authentication methods for social networking evidence that are not supported by the existing rules of evidence in Maryland.[224] Nor is the result in *Griffin* supported by a plain reading of the existing rules of evidence, Maryland case law, or persuasive authority from other jurisdictions.[225] The court over-

219. *See, e.g.*, Chaney v. Family Dollar Store of Md., No. 24-C-06-11462 OT, 2007 WL 5997994, at *1 (Md. Cir. Ct. Dec. 26, 2007) (finding that evidence from a weather website was not properly authenticated because it contained no relevant identifying characteristics other than a URL printed on the page and no additional "information about the source" was provided to the court).

220. *See* State v. Eleck, 23 A.3d 818, 824–25 (Conn. App. Ct. 2011) (finding that messages sent via Facebook were not properly authenticated after citing the inherent risks of falsification or fraud in online communication); Commonwealth v. Williams, 926 N.E.2d. 1162, 1171–73 (Mass. 2010) (finding that the authentication of chat records from MySpace was insufficient in a murder case because there was no evidence that the owner of the MySpace account sent the messages, despite testimony from a witness stating that she knew it was the owner of the account who sent the messages).

221. MD. R. 5-901(a). This can be compared to relevancy, for which the rules specifically define certain types of evidence which is admissible for one purpose and not another. See, for example, MD. R. 5-408, which does not allow settlement offers in civil matters to be admitted into evidence to prove the validity, invalidity, or amount of civil damages, but allows settlement offers to be admitted for other reasons, such as witness bias.

222. Griffin v. State, 419 Md. 343, 358, 19 A.3d 415, 424 (2011).

223. *Id.* at 357–58, 363–64, 19 A.3d at 423–24, 427–28.

224. *See supra* Part IV.A and note 134.

225. *See supra* Part IV.B.

reached in treating social media evidence as different from other forms of evidence and, in so doing, disregarded state and federal rules of evidence.