ENSURING DIGITAL INTEGRITY: STRENGTHENING AUTHENTICATION REQUIREMENTS FOR ELECTRONIC EVIDENCE IN IOWA CRIMINAL CASES

ABSTRACT

With the rise of electronic evidence introduced at trial, courts have become concerned with the authenticity of social media electronic evidence. Technology has evolved, allowing people to create realistic and authentic-looking messages or social media posts. Due to the ease and accessibility of creating fabricated electronic evidence, Iowa courts should increase the evidentiary standard for authenticating digital communications. The current authentication requirement is low and permits witness testimony about the contents of the digital communication to meet the standard. If a witness has fabricated digital communications evidence, that witness would clearly have enough information regarding the evidence they fabricated to testify to its contents. Iowa courts should adopt the Maryland approach and require electronic evidence to be gathered from the social media organization or cell phone provider directly to ensure authenticity.

TABLE OF CONTENTS

I. INTRODUCTION

As the influence of social media continues to grow and expand, the law must adapt to the ever-changing issues that increased social media use creates for authenticating evidence.[1] With advancements to technological devices such as computers, smartphones, tablets, and smart watches, digital methods of communication have drastically increased.[2] Because of the rapid increase and reliance on digital communication, legal disputes frequently include some form of electronic evidence.[3] Digital communication has its own challenges, however, including increased instances of hacking and the creation of fake accounts, social media posts, and messages.[4]

One method of altering or fabricating digital communications evidence is known as "spoofing."[5]

> Using a spoofing application (app), an individual can falsify a text message and send the message from any phone number they choose. Thus, an alleged victim can enter the accused's phone number and send a message—in which the accused appears to admit his guilt—to the alleged victim's phone.[6]

Another method allows spoofers "to create an entire fake conversation on the user's phone, allowing the user to take a screenshot of the spoofed conversation and represent it as a genuine conversation."[7] Screenshots of spoofed text conversations appear identical to real text message conversations, posing a tremendous risk to courts attempting to authenticate screenshots of electronic evidence.[8] Further, the spoofing applications are moderately user-friendly, and anyone with limited knowledge of technology could spoof an entire text conversation.[9]

1. Siri Carlson, Comment, *When is a Tweet Not an* Admissible *Tweet? Closing the Authentication Gap in the Federal Rules of Evidence*, 164 U. PA. L. REV. 1033, 1035 (2016).

2. *Id.* at 1034.

3. *Id.*

4. *See, e.g.*, *id.* at 1046 (discussing a case where the Maryland Court of Appeals excluded a MySpace profile allegedly created to intimidate a witness, emphasizing the ease with which digital communications can be forged and the necessity for requiring heightened authentication).

5. Eric A. Catto, *The Spoof is in the Evidence: Obtaining Electronic Records to Corroborate Text Message Screenshots*, ARMY LAW., 2020, at 34, 34.

6. *Id.*

7. *Id.*

8. *See id.* at 35.

9. *Id.*

Electronic evidence can also be fabricated through the creation of fake social media profiles.[10] Creating fake or fraudulent profiles is easy, and this is exacerbated by the lack of social media platforms verifying user identity upon creation of a new account.[11] Thus, any individual could create a fake profile using personal information and photographs found online, and fabricate incriminating posts or messages.[12] To further complicate these authentication issues, social media profiles are also susceptible to hacking.[13]

Due to the increasing use of electronic forms of evidence in litigation and the above-mentioned methods of creating fake social media posts and texts, this Note argues that the authentication requirements in Iowa should be heightened to ensure electronic evidence has not been altered or fabricated.[14] Most courts have considered the issue of electronic evidence authentication, but only a minority have adopted a heightened approach thus far.[15] However, as social media grows, reliance on electronic evidence will continue to cause authentication problems that courts must eventually address.[16] The issue of authentication is prevalent in all litigation, including criminal law and civil law matters such as family law, tort law, worker's compensation, and personal injury.[17] Although this Note primarily analyzes criminal law cases, electronic discovery is becoming the dominant form of evidence, and the position of this Note applies to both criminal and civil litigation equally.

II. IOWA'S STANDARD FOR AUTHENTICATING SCREENSHOTS OF ELECTRONIC EVIDENCE

The current authentication requirements for evidence in Iowa are governed by Iowa R. Evid. 5.901.[18] Rule 5.901 requires the proponent of evidence to "produce evidence sufficient to support a finding that the item is what the proponent claims it is."[19] Further, the proponent's authentication burden is not

10. Linda Greene, Comment, *Mining Metadata: The Gold Standard for Authenticating Social Media Evidence in Illinois*, 68 DEPAUL L. REV. 103, 103 (2018).

11. *See id.* at 128.

12. *See id.*; Catto, *supra* note 5, at 34.

13. Greene, *supra* note 10, at 103.

14. *See infra* Part IV.

15. *See infra* Part III.

16. *See* Greene, *supra* note 10, at 103.

17. *Id.* at 108–09.

18. IOWA R. EVID. 5.901. For the analogous federal authentication rule, see FED. R. EVID. 901.

19. IOWA R. EVID. 5.901(a); State v. Acosta, No. 19-0364, 2020 WL 7021516, at *2 (Iowa Ct. App. Nov. 30, 2020) (citation omitted).

high, but rather a mere "prima facie showing is required."[20] The proponent of electronic evidence must "produce evidence sufficient to convince a reasonable juror of its authenticity or authorship."[21] To authenticate a screenshot of electronic evidence, the proponent must "produce evidence sufficient to show that the purported author of the communication, whether it be an email, a Facebook posting, or a text message, actually authored or published the content."[22]

A proponent of electronic evidence has various methods to prove who authored a message, thereby authenticating the evidence.[23] The most direct method is testimony from the author of the message, or testimony by someone who witnessed the author write and send the message; however, most people do not write messages with another person observing.[24] If the alleged author denies writing the message, the proponent has other potential methods to authenticate the evidence.[25]

In the absence of direct testimony, the proponent of electronic evidence can use circumstantial evidence to authenticate the author of a message.[26] Circumstantial evidence includes "appearance, contents, substance, internal patterns, or other distinctive characteristics, taken together with all the circumstances."[27] Other forms of circumstantial evidence include the username or email address of the account that sent or published the message, nicknames associated with the account that few people would know, or any other information that is not commonly known about the author or the recipient.[28] This method of piecing together circumstantial evidence to uncover the author is a common method of authentication in most courts.[29]

20. State v. Goodwin, No. 18-1822, 2020 WL 1551149, at *4 (Iowa Ct. App. Apr. 1, 2020) (quoting United States v. Hassan, 742 F.3d 104, 133 (4th Cir. 2014) (referring to FED. R. EVID. 901)).

21. 7 LAURIE KRATKY DORÉ, IOWA PRACTICE SERIES: EVIDENCE § 5.901:11 (2024–2025).

22. *Acosta*, 2020 WL 7021516, at *2 (quoting DORÉ, *supra* note 21, § 5.901:11).

23. DORÉ, *supra* note 21, § 5.901:11.

24. *Id.*

25. *Id.*

26. *Id.*

27. *Id.* (quoting IOWA R. EVID. 5.901(b)(4)).

28. *See id.*

29. *See id.*

A. *Iowa Courts Interpretation and Application of the Current Authentication Process*

Some Iowa courts have properly authenticated electronic messages, but as discussed below, there are instances where Iowa courts were too lenient with the authentication process—cases involving little circumstantial evidence, that nonetheless resulted in authentication.[30] In all cases discussed below, the courts found that the proponent of the evidence met the burden of authenticating the electronic messages; however, the cases reveal a clear division of authentication methods.[31]

1. *Strong Circumstantial Evidence Caselaw*

In *State v. Brown*, the prosecutor offered Facebook messages allegedly sent by the defendant in a first-degree murder and first-degree robbery case.[32] The defendant allegedly sent Facebook messages to his friend and to his friend's brother regarding the crimes.[33] The defendant deleted the messages off his Facebook account before officers seized his phone, and in response, an investigator sent search warrants to Facebook for the accounts of the defendant, his friend, and his friend's brother.[34] The messages the prosecutor offered in trial for authentication were certified messages from Facebook produced directly in response to the search warrant.[35] The court concluded the Facebook messages were authenticated based on the name of the Facebook account matching the named defendant, the photographs found on the Facebook account being photographs of the defendant, and the certified messages from Facebook.[36]

In *State v. Goodwin*, the prosecutor offered evidence of incriminating text messages in connection with a string of Craigslist robberies.[37] The messages were taken from an individual's phone who was believed to be the defendant's romantic partner.[38] The trial court allowed the messages to be admitted into evidence, and

30. *See* State v. Goodwin, No. 18-1822, 2020 WL 1551149, at *5 (Iowa Ct. App. Apr. 1, 2020); State v. Simpson, No. 18-0666, 2020 WL 4812647, at *2 (Iowa Ct. App. Aug. 19, 2020); State v. Akok, No. 17-0655, 2018 WL 4362065, at *1 (Iowa Ct. App. Sep. 12, 2018).

31. *See Goodwin*, 2020 WL 1551149, at *5; *Simpson*, 2020 WL 4812647, at *3; *Akok*, 2018 WL 4362065, at *1.

32. No. 20-1098, 2022 WL 468960, at *1 (Iowa Ct. App. Feb. 16, 2022).

33. *Id.* at *1–2.

34. *Id.* at *2, *4.

35. *Id.* at *4.

36. *Id.* at *5.

37. No. 18-1822, 2020 WL 1551149, at *4 (Iowa Ct. App. Apr. 1, 2020).

38. *Id.*

the defendant appealed.[39] The appellate court found that the proponent of the messages met the burden of authenticating the screenshotted messages.[40] The appellate court concluded that the messages were properly authenticated due to a number of factors.[41] Even though the phone number associated with the contact could not be connected to the defendant, the contact name of the sender was "Edwin," which matched the defendant's name.[42] Further, the contents of the text messages included specific details about the crimes that someone without knowledge of the crimes would not have been able to recreate.[43] Finally, the court also considered that the messages were sent on the night of the robbery to support a conclusion that the messages were sent from the defendant.[44]

In *State v. Akok*, the defendant, Akuk Akok, appealed his conviction of burglary, felonious assault, and child stealing, arguing the electronic messages were not properly authenticated.[45] The trial court admitted the Facebook messages because they came from an account known as "Akuk Akok" and were sent from an internet address associated with a University of Iowa hospital during a period when the defendant was receiving treatment there.[46] The Court of Appeals affirmed and concluded that the messages were properly authenticated because the username of the Facebook account that sent the messages was the same as the defendant's name and because of the IP address of the messages.[47]

The abovementioned cases provide examples of the types of strong circumstantial evidence used to authenticate electronic messages.[48] In *Brown*, the prosecutor obtained a search warrant for Facebook to gather information from the source directly, rather than relying on circumstantial or testimonial evidence from a witness.[49] The cases used strong circumstantial evidence, such as the specificity

39. *Id.* at *3–4.

40. *Id.* at *5.

41. *Id.* at *4–5.

42. *Id.* at *4.

43. *Id.* at *5 (noting that the text messages included details of defendant stealing two hundred dollars from the victim, whom he met via Craigslist, in the texts between Hodges and defendant).

44. *Id.*

45. No. 17-0655, 2018 WL 4362065, at *1 (Iowa Ct. App. Sep. 12, 2018).

46. *Id.*

47. *Id.*

48. *See* State v. Brown, No. 20-1098, 2022 WL 468960, at *4–5 (Iowa Ct. App. Feb. 16, 2022); *Goodwin*, 2020 WL 1551149, at *4–5; *Akok*, 2018 WL 4362065, at *1.

49. *Brown*, 2022 WL 468960, at *4.

of detail in the messages and the internet addresses of the messages, to authenticate without unduly burdening prosecutors.[50]

2. *Minimal Circumstantial Evidence Caselaw*

In *State v. Simpson*, the defendant was charged with third-degree harassment based on a public Facebook post and comments reviewing a particular massage therapist at a salon.[51] The salon owner offered screenshots of the Facebook post and comments.[52] The authentication method used in *Simpson* was proponent testimony, with the salon owner testifying about taking the screenshots and the contents of the screenshotted post and comments.[53] However, the owner failed to identify the last four pages of the five-page screenshot exhibit.[54] The court noted, "The salon owner identified the first page of Exhibit 1, named the author of the review, examined the contents of the post on Simpson's public Facebook page, identified the therapist partially named in the review, and took the screenshot of the post," and therefore determined that the proponent met the authentication requirements.[55]

Although the screenshotted evidence in *Simpson* was deemed properly admitted, this case exemplifies the low standard of proof proponents of electronic evidence must satisfy.[56] An unfair advantage exists for the proponent of the evidence when the proponent's testimony is enough to satisfy the authentication burden.[57] As evident in *Simpson*, gaps may exist in the proponent's knowledge of the electronic messages.[58] Further, the current Iowa standard for authenticating electronic messages provides no safeguards to the opponent of the evidence to ensure the proponent did not falsify the proffered evidence.[59]

Another notable Iowa case is *State v. Acosta*.[60] In this case, the evidence in question included screenshots of Snapchat messages between the defendant and the victim of sexual assault.[61] The State offered the screenshots as evidence

50. *See id.* at *5; *Goodwin*, 2020 WL 1551149, at *5; *Akok*, 2018 WL 4362065, at *2.
51. No. 18-0666, 2020 WL 4812647, at *1 (Iowa Ct. App. Aug. 19, 2020).
52. *Id.*
53. *Id.* at *1–2.
54. *Id.* at *2.
55. *Id.*
56. *See id.*
57. *See, e.g.*, *id.*
58. *Id.*
59. *See* IOWA R. EVID. 5.901(a).
60. No. 19-0364, 2020 WL 7021516, at *1 (Iowa Ct. App. Nov. 30, 2020).
61. *Id.* at *1–3.

between "Tio" and the victim.[62] The victim testified regarding the contents of the messages, the timing of the defendant adding her Snapchat account (after the assault occurred), and the defendant's Snapchat username and contact name.[63] The victim took a screenshot of the messages and accurately identified all eleven pages of the exhibit.[64] The court found that the messages were properly authenticated and admitted based on the victim's testimony regarding the content and timing.[65]

Acosta seems to fit somewhere in the middle between the strong authentication cases of *Brown*, *Goodwin*, and *Akok*, and the weak standard relied on in *Simpson*.[66] One distinction is abundantly clear: the testimony of the evidence in *Acosta* was much stronger than in *Simpson*. The victim in *Acosta* testified to all pages of the exhibit, whereas the witness in *Simpson* failed to identify 80 percent of the exhibit.[67] However, another distinction must be made between *Acosta* and the higher standard authentication cases. In *Brown*, *Goodwin*, and *Akok*, outside evidence aided the court in finding the authentication requirements were met.[68] Stated another way, authentication in *Brown*, *Goodwin*, and *Akok* were not solely based on testimonial evidence from the proponent that offered the evidence.[69] A heightened authentication standard that requires some outside evidence, such as a certification from a social media platform or a corroborating internet address,

62. *Id.* at *2.

63. *Id.* at *1–3.

64. *Id.* at *2.

65. *Id.* at *3.

66. *See id.* at *2–3; State v. Brown, No. 20-1098, 2022 WL 468960, at *4–5 (Iowa Ct. App. Feb. 16, 2022); State v. Goodwin, No. 18-1822, 2020 WL 1551149, at *4–5 (Iowa Ct. App. Apr. 1, 2020); State v. Akok, No. 17-0655, 2018 WL 4362065, at *1 (Iowa Ct. App. Sep. 12, 2018); State v. Simpson, No. 18-0666, 2020 WL 4812647, at *2 (Iowa Ct. App. Aug. 19, 2020).

67. *Contrast Acosta*, 2020 WL 7021516, at *3 ("D.R. identified Exhibit 16 as the username of the person who sent the messages, took screenshots of the messages, stated the timing the messages took place, and explained the context of the messages. We conclude the district court did not abuse its discretion in finding D.R.'s testimony sufficient to establish that the messages were what she claimed them to be."), *with Simpson*, 2020 WL 4812647, at *2 (noting that the evidence was properly authenticated, even when considering the owner could not identify the last four pages of the exhibit).

68. *Contrast Acosta*, 2020 WL 7021516, at *2–3 (relying only on the testimony of the victim to authenticate the messages), *with Brown*, 2022 WL 468960, at *4–5 (relying, in part, on the certified copy of messages received from Facebook), *and Goodwin*, 2020 WL 1551149, at *4–5 (relying on the timing of the messages to connect them to the defendant), *and Akok*, 2018 WL 4362065, at *1 (relying on the IP address the messages were sent from to connect them to the defendant).

69. *See Brown*, 2022 WL 468960, at *4–5; *Goodwin*, 2020 WL 1551149, at *4–5; *Akok*, 2018 WL 4362065, at *1.

should be required of proponents of electronic evidence to ensure evidence has not been falsified or tampered with, especially as technology continues to develop and evolve.[70]

III. ELECTRONIC MESSAGE AUTHENTICATION REQUIREMENTS IN OTHER JURISDICTIONS

Analysis into the authentication requirements of other states should persuade Iowa courts to heighten the authentication standard. Even if Iowa does not adopt a different approach, commentary from other jurisdictions will inform Iowa courts of the ease of recreating or falsifying electronic evidence.

A. *The Maryland Approach*

A Maryland court first recognized the potential for fabricating electronic evidence in 2011.[71] In *Griffin v. State*, the defendant was convicted of second-degree murder and other related charges.[72] The prosecutor offered evidence from the defendant's girlfriend's MySpace page, which was authenticated by the investigator who screenshotted the profile.[73] The investigator testified that the profile picture and birthday associated with the MySpace account matched the picture and information of the girlfriend.[74] The defendant appealed, arguing the screenshots did not meet the authentication requirements.[75] The court agreed and reversed the verdict.[76] The court noted, "The identity of who generated the profile may be confounding, because 'a person observing the online profile of a user with whom the observer is unacquainted has no idea whether the profile is legitimate.'"[77] Further, the court commented on the rapidly changing technological advancements along with the "complexity" and "novelty" of electronically stored information as evidence.[78] Finally, the court compared methods of authenticating electronic information to authentication of other forms of evidence and noted that the "potential for manipulation [of electronically stored information], requires

70. *See Brown*, 2022 WL 468960, at *4–5; *Akok*, 2018 WL 4362065, at *1.

71. Griffin v. State, 19 A.3d 415 (Md. 2011); *see* Carlson, *supra* note 1, at 1046.

72. *Griffin*, 19 A.3d at 418.

73. *Id.*

74. *Id.*

75. *Id.*

76. *Id.*

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

78. *Id.* at 423 (quoting Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 543–44 (D. Md. 2007)).

greater scrutiny of 'the foundational requirements' than letters or other paper records . . . ."[79]

The Maryland court created a heightened standard for authenticating electronic messages and held that "social media evidence may only be authenticated through the testimony of the creator, documentation of the internet history or hard drive of the purported creator's computer, or information obtained directly from the social networking site."[80] *Griffin*'s holding is known as the "Maryland approach" and has been adopted by some jurisdictions that are concerned with the fabrication issues that electronic evidence may pose.[81]

B. *The Texas Approach*

Conversely, other courts have validated their respective rules of evidence (either the Federal Rules of Evidence Rule 901 or analogous state versions of Rule 901) and upheld the low threshold for authentication.[82] Shortly after *Griffin*, Texas was faced with a similar question regarding the authenticity of electronic social media evidence.[83]

Tienda v. State was an appeal concerning evidence from the defendant's alleged MySpace social media page.[84] The defendant was convicted of a murder stemming from a gang caravan that exchanged gunfire with rival gang members.[85] Conflicting testimony was presented regarding which vehicle the shots were fired from, which car the defendant was in, and whether the defendant fired the fatal shots.[86] The victim's sister provided law enforcement officials with information about a MySpace page allegedly belonging to the defendant.[87] The MySpace page used a nickname that the victim's sister testified was associated with the defendant.[88] Other factors the State relied on for authentication included photographs resembling the defendant's tattoos—even though his face was not present in the pictures—the birth year, location ("D TOWN" suggesting Dallas,

79. *Id.* (quoting *Lorraine*, 241 F.R.D. at 543–44).

80. Parker v. State, 85 A.3d 682, 683 (Del. 2014) (discussing the Maryland approach outlined in *Griffin*).

81. *See id.*

82. *See* FED. R. EVID. 901; *Parker*, 85 A.3d at 686–87.

83. *See* Tienda v. State, 358 S.W.3d 633, 634 (Tex. Crim. App. 2012).

84. *Id.* at 634–35.

85. *Id.* at 634.

86. *Id.*

87. *Id.*

88. *Id.* at 635.

Texas), gang-related gestures, and a link to a song played at the victim's funeral.[89] The relevant postings on the MySpace page incriminated the purported author as the victim's murderer.[90] The trial court found that the testimony of the decedent's sister regarding the MySpace printouts satisfied the applicable Texas rule of evidence standard for authenticating electronic evidence, and a jury convicted the defendant of murder.[91]

The defendant argued on appeal that the trial court erred by admitting the MySpace printouts into evidence.[92] The defendant urged the court to implement the Maryland approach from *Griffin* and argued that the MySpace screenshots were improperly authenticated.[93] The State opposed, arguing that enough circumstantial evidence was available to allow the MySpace evidence to be submitted to the jury for factual determinations.[94]

The Texas Court of Criminal Appeals stated,

> Courts and legal commentators have reached a virtual consensus that, although rapidly developing electronic communications technology often presents new and protean issues with respect to the admissibility of electronically generated, transmitted, and/or stored information, including information found on social networking web sites, the rules of evidence already in place for determining authenticity are at least generally "adequate to the task."[95]

Thus, Texas declined to adopt the Maryland approach.[96] Further, the court noted that "jurisdictions across the country have recognized that electronic evidence may be authenticated in a number of different ways consistent with Federal Rule 901 and its various state analogs."[97] Texas admonished the Maryland approach, suggesting that the jury should, upon satisfaction of the low-threshold authentication requirement, determine whether social media evidence is fraudulent or authentic.[98] Finally, the court noted that even if it decided to adopt *Griffin*'s

89. *Id.*
90. *Id.* at 635–36.
91. *Id.* at 634–35, 637; *see* TEX. R. EVID. 901.
92. *Tienda*, 358 S.W.3d at 637.
93. *Id.* at 637, 646.
94. *Id.* at 637.
95. *Id.* at 638–39 (quoting Steven Goode, *The Admissability of Electronic Evidence*, 29 REV. LITIG. 1, 7 (2009)).
96. *Id.* at 638–39, 647.
97. *Id.* at 639; *see* FED. R. EVID. 901.
98. *Tienda*, 358 S.W.3d at 647.

authentication test, the circumstantial evidence in *Tienda* was enough to overcome the heightened authentication standard.[99]

C. *Comparing the Maryland Approach and the Texas Approach*

As shown in *Griffin* and *Tienda*, two approaches to authentication requirements for electronic evidence have emerged.[100] The Maryland approach is regarded as "setting a higher bar for authenticating social media evidence than is required for other types of evidence under the Rules [of Evidence]," whereas the Texas approach is coined as the liberal approach to evidence, allowing the finder of fact to make determinations of authenticity versus fabrication.[101]

The Maryland approach hinges upon whether the trial court has "definitively determine[d] that the evidence is authentic."[102] In contrast, the Texas approach is "whether the proponent has produced sufficient evidence for a reasonable jury to find that the proffered evidence is authentic."[103]

A Delaware Supreme Court decision summarized the alternative approaches to electronic authentication.[104] In *Parker v. State*, the defendant appealed a conviction of second-degree assault, arguing that the Facebook evidence used against her was not properly authenticated.[105] The trial court found that the authentication standard was properly met for the Facebook evidence based on victim testimony and circumstantial evidence found within the Facebook posts and messages.[106]

Parker noted how the Maryland approach is concerned with evidence that may be "fake, a digital alteration of an alleged creator's profile, or a posting by another using the alleged creator's profile."[107] The Maryland approach would circumscribe different evidentiary rules to electronic evidence, namely social

99. *Id.*

100. *Contrast id.* at 633 (applying a liberal standard of authentication), *with* Griffin v. State, 19 A.3d 415, 423 (Md. 2011) (applying a heightened standard of authentication).

101. *See* Carlson, *supra* note 1, at 1046–47.

102. *Id.* at 1046 (quoting Paul W. Grimm, Lisa Yurwit Bergstrom & Melissa M. O'Toole-Loureiro, *Authentication of Social Media Evidence*, 36 AM. J. TRIAL ADVOC. 433, 441 (2013)).

103. *Id.* at 1047.

104. *See* Parker v. State, 85 A.3d 682, 686–87 (Del. 2014).

105. *Id.* at 683–84.

106. *Id.* at 684.

107. *Id.* at 686.

media and text messages.[108] The *Parker* court considered both alternatives but ultimately maintained the status quo of Delaware Rule of Evidence 901, siding with the Texas approach.[109]

D. *Eighth Circuit Approach*

Although questions of authentication requirements arose in the early 2010s, the Eighth Circuit did not address this issue until 2021.[110] In *United States v. Lamm,* a grand jury found the defendant guilty of distribution, production, and possession of child pornography.[111] The defendant allegedly used two Facebook accounts, one bearing his name and one with a fake name, to engage in the crimes.[112] The Government authenticated Facebook evidence of the crimes using corroborating photos, screenshots of messages, and the email address that was linked to the accounts.[113] The district court admitted the Facebook accounts into evidence.[114]

The defendant appealed, arguing that the Facebook evidence was improperly admitted.[115] The Eighth Circuit noted, "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."[116] Sufficient evidence includes witness testimony or circumstantial evidence taken together, such as contents, appearance, patterns, or other distinctive characteristics.[117] Once the low-threshold requirement is met, the Eighth Circuit noted that the question of authenticity becomes one for the fact-finder.[118]

Although the court did not adopt a heightened standard of authentication, it did note: "[A]uthentication of social media evidence . . . presents some special challenges because of the great ease with which a social media account may be

108. *See id.* at 683; *see also* Carlson, *supra* note 1, at 1046 ("In courts that follow the *Griffin* approach, evidence from digital communications is not admissible 'unless the court definitively determines that the evidence is authentic.'" (quoting Grimm, Bergstrom & O'Toole-Loureiro, *supra* note 102, at 441)).

109. *Parker*, 85 A.3d at 687.

110. *See* United States v. Lamm, 5 F.4th 942, 947 (8th Cir. 2021).

111. *Id.* at 946.

112. *Id.* at 944.

113. *Id.* at 945.

114. *Id.* at 946.

115. *Id.*

116. *Id.* (quoting FED. R. EVID. 901(a)).

117. *Id.*

118. *Id.* at 947.

falsified or a legitimate account may be accessed by an imposter."[119] However, the court did not elaborate further on the challenges that screenshots of social media evidence presents.[120]

The Eighth Circuit was presented with the same issue again in 2024 in *United States v. Boykins*.[121] The defendant was convicted of sex trafficking, sex trafficking of a minor, and production and distribution of child pornography.[122] The defendant appealed the charges, arguing "that the district court erred by admitting insufficiently authenticated electronic-communication and social-media evidence obtained from [his] phone."[123] One important caveat is that the parties stipulated to the admission of the evidence.[124]

Although the court did not need to discuss admission of the Facebook and Instagram evidence because the parties stipulated to its admission, the court analyzed the evidence anyway.[125] The Government provided witness testimony from the victim and a special agent regarding the phone's ownership and number, the defendant's admission to arresting officers regarding ownership of the phone, and the fact that neither the victim nor anyone else had access to the phone.[126] Additional circumstantial evidence included an account reference to the defendant's known nickname and the registered email on the account belonging to the defendant.[127] The court held that, absent a stipulation, the Facebook and Instagram evidence would have been admissible anyway as it clearly met the threshold requirement for authentication of electronic communications.[128]

The court also acknowledged the "special challenges" of social media evidence "because of the great ease with which a social media account may be falsified or a legitimate account may be accessed by an imposter."[129] Although there may have been clear evidence in *Boykins* supporting authentication, the Eighth Circuit may not have been fully aware of the precedent set in future cases

119. *Id.* (alteration in original) (quoting United States v. Browne, 834 F.3d 403, 412 (3d Cir. 2016)).

120. *See id.* at 947–48.

121. No. 23-1652, 2024 WL 208346, at *1 (8th Cir. Jan. 19, 2024).

122. *Id.*

123. *Id.*

124. *Id.*

125. *Id.* at *1–2.

126. *Id.* at *2.

127. *Id.*

128. *Id.* at *1.

129. *Id.* at *2 (quoting United States v. Lamm, 5 F.4th 942, 947 (8th Cir. 2021)).

potentially involving minimal circumstantial evidence to support admission of social media accounts.[130]

IV. RECOMMENDATIONS

While the current Iowa Rules of Evidence and the Federal Rules of Evidence only require *some* authentication of electronic social media evidence, courts and legislatures should consider adopting a heightened standard for authenticating electronic evidence.[131] As technology evolves and the fabrication of social media evidence becomes easier, every court will eventually be forced to confront this issue. The justice system should not wait for someone to be wrongfully incarcerated based on fake social media messages to enact heightened authentication requirements.

The Iowa judicial system should consider an approach similar to the Maryland approach, which is skeptical of the authenticity of social media platforms and the evidence collected from them.[132] Under a heightened approach, Iowa should require some form of authenticating evidence beyond witness testimony regarding the contexts of a social media post or communication.

One potential authentication requirement could be requiring social media evidence to be accompanied by its digital footprint.[133] A digital footprint can be obtained from the device itself, such as a cellphone or computer, or by records from a service provider.[134] Text messages produce a special type of record, known as a transactional record, that could also be used to authenticate the message.[135]

Metadata also proves to be a form of authenticating social media records that can be admitted into evidence under a business record exception.[136] Metadata is a practical authentication tool as it provides electronic records with "distinctive characteristics."[137] Metadata is "'neither created by nor normally accessible to the computer user' but is often generated automatically as a function of the application

130. *See id.* at *2.

131. *See* FED. R. EVID. 901; IOWA R. EVID. 5.901; *see* Catto, *supra* note 5, at 35.

132. *See* Griffin v. State, 19 A.3d 415, 424 (Md. 2011).

133. *See* Catto, *supra* note 5, at 35.

134. *Id.*

135. *Id.*

136. *See* Greene, *supra* note 10, at 112; Carlson, *supra* note 1, at 1054–55.

137. Greene, *supra* note 10, at 112 (quoting Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 548 (D. Md. 2007)).

being used."[138] Metadata can provide the device location, phone number, IP address, and other records associated with the account.[139] This information is especially useful for authentication purposes because "unlike social media users, metadata does not lie."[140] As for admitting metadata, social media platforms could provide a certificate, which is a signed record signifying the metadata's authenticity, instead of requiring live testimony.[141] Certification is efficient and also provides fair notice to the opposing party.[142] Another benefit to utilizing metadata is that "[d]elineating a cohesive approach will help courts avoid over-consideration of the potential for forgery in the threshold authentication analysis."[143] Using metadata to authenticate electronic evidence saves time and money while ensuring true authenticity for some of the most imperative evidence in many cases.[144]

V. CONCLUSION

The Iowa judicial system should analyze the multiple ways social media and text message evidence can be altered and forged, and Iowa should implement special requirements for these forms of electronic evidence. At minimum, Iowa courts should require more than witness testimony regarding the contents of the messages to ensure that the testifying witness does not have knowledge of the contents simply because they fabricated the post or message.[145] There is a clear conflict of interest that should be addressed more formally than the method provided by the current, more lenient rules of authentication.[146] Further, the authentication issue will continue to grow as technology continuously evolves, and Iowa courts should face the issue head-on rather than wait for a wrongful conviction based on fake evidence. The Iowa court system has the opportunity to be a digital trailblazer by adopting an approach recommended above or by creating a new approach to social media evidence. While this Note does not fully encapsulate all the issues regarding social media evidence, an increased awareness of the issues of authentication should encourage the legal community to consider

138. *Id.* at 104 (citation omitted).
139. *Id.* at 104–05.
140. *Id.* at 104.
141. *See id.* at 119.
142. *Id.* at 119–20.
143. Carlson, *supra* note 1, at 1060.
144. *See* Greene, *supra* note 10, at 147.
145. *See supra* Part IV.
146. *See supra* Part IV.

ways that the judicial system can evolve alongside technology and ensure fair trials for all based on truly authentic evidence.

*Kayla Hruska**

* Kayla Hruska, B.A. & B.S.E., Drake University, 2022; J.D., Drake University Law School, 2025.