DO IT FOR THE SNAP: DIFFERENT METHODS OF AUTHENTICATING SNAPCHAT EVIDENCE FOR CRIMINAL PROSECUTIONS

Maximilian Bungert[*]

TABLE OF CONTENTS

* J.D. 2021, University of Illinois College of Law; B.A., University of Florida. I would like to thank the editors and staff of the *Journal of Law, Technology & Policy* for their time and dedication to this journal. Without them this Note would not be possible. I would also like to specifically my notes editor Ed Wells for his help with edits and ideas, and my friends and family, who have to put up with my frequent use of Snapchat as an outlet for every idea that pops into my head.

I. INTRODUCTION

In September 2014, a 16-year-old teen was sexually assaulted by two of her male classmates at a party in the small town of Saugus, Massachusetts.[1] The rape, which occurred in a dark wooded area, was not witnessed by anyone at the party, and the two perpetrators claimed that the sexual acts performed were consensual.[2] This left the prosecution in a tough position, as they now had to proceed on a case with very little evidence besides the testimony of a victim who was extremely intoxicated at the time of the incident, and therefore couldn't remember much of what happened.[3]

The prospects for conviction looked bleak, until a new critical piece of evidence emerged. The District Attorney's saving grace was a series of screenshots taken from Snapchat recordings of the incident.[4] In these recordings, which had been posted by the defendants shortly before the incident took place, the victim could be observed being pushed around while slurring the word, "stop."[5] These Snapchat recordings proved too much for the defense to overcome, and the two defendants were convicted and sentenced to four to five years in prison.[6]

Cases like this, in which content from the social media profiles of criminal defendants is used to assist in prosecuting them for alleged crimes, are becoming increasingly common throughout the country.[7] Content from Snapchat in particular, an app that allows users to post and share photos and videos which then disappear after a set amount of time, is increasingly being used by police investigators to assist prosecutors in proving their case in chief.[8] With Snapchat's increasing popularity among both teens and adults, its use in criminal trials will likely become increasingly important in the years to come.[9]

However, as with other content gathered from the social media accounts of defendants, pictures and videos can prove problematic for prosecutors when it comes time to introduce them into evidence at trial.[10] Specifically, states frequently run into problems with the authentication process for evidence taken

1. Laura Crimaldi, *Pair Convicted in Snapchat Rape*, BOS. GLOBE (July 20, 2016), https://www.bostonglobe.com/metro/2016/07/19/deliberations-resume-snapshat-sex-assault-case/EJEg1l1tW3KKGcXQeDqOJP/story.html.

2. *Id.*

3. *Id.*

4. *Id.*

5. *Id.*

6. *Id.*

7. *See generally* Justin P. Murphy & Adrian Fontecilla, *Social Media Evidence in Government Investigations and Criminal Proceedings: A Frontier of New Legal Issues*, 19 RICH. J.L. & TECH. 11 (2013) (explaining the proliferation of online evidence in criminal trials).

8. *See, e.g.*, Russell Brandom, *Colorado Police Turned to Snapchat to Solve a Drug Murder*, VERGE (Feb. 23, 2018), https://www.theverge.com/2018/2/23/17045118/snapchat-police-drug-murder-data-request-colorado (showing an example of a case where police were able to rely on Snapchat screenshots to prove that a drug deal had been conducted via Snapchat video).

9. Karissa Bell, *Snapchat is More Popular Than Ever*, MASHABLE (July 23, 2019), https://mashable.com/article/snap-q2-2019-earnings/.

10. Youngjin Choi, *Mobile Instant Messaging Evidence in Criminal Trials*, 26 CATH. U. J. L. & TECH. 1, 4 (2017).

from the Snapchat accounts of defendants.[11] As Snapchat evidence is increasingly used in criminal trials, it will be important for prosecutors to familiarize themselves with the authentication process and to use a system that will ensure that this often crucial evidence can be properly admitted.[12] Though it is by no means the only one in such a position, Illinois does not currently have a uniform set of rules for dealing with the authentication of content taken from the social media profiles of criminal defendants, including their Snapchat accounts.[13]

This Note will explore the ways in which different jurisdictions go about the authentication process for Snapchat evidence in criminal trials. After viewing the authentication process for Snapchat evidence through the lens of the two most common approaches, those used by Texas and Maryland, this Note will make a recommendation that Illinois adopt the Texas approach and accept a more flexible standard for authenticating evidence that comes from the Snapchat accounts of criminal defendants.[14] This is because in an increasingly digital age it is important for the State to have every resource at its disposal to effectively prosecute complicated criminal cases.

Part II of this Note will explore Snapchat's features and its proliferation as a social media form, as well as its importance as a source of evidence in criminal trials. Additionally, it will give examples of problems that prosecutors frequently run into when trying to authenticate Snapchat evidence in criminal trials.[15] Part III will discuss the two most common approaches to authenticating social media evidence at trial and will analyze how the different standards of these two approaches affect the likelihood that Snapchat evidence introduced at trial will be properly authenticated. Part IV will make a recommendation that Illinois adopt the Texas approach to authenticating evidence gathered from the Snapchat profiles of criminal defendants. Given Snapchat's popularity, the Texas approach's more relaxed standard for authentication provides prosecutors a better chance of authenticating and admitting what often amounts to crucial evidence. This becomes especially important for cases where most of the evidence of wrongdoing comes from the Snapchat accounts of defendants.

II. BACKGROUND

A. Snapchat's Popularity and Features

Snapchat was born out of founders Evan Spiegal and Bobby Murphy's vision to create an app that would mimic the impermanent nature of face-to-face

11. *Id.* at 6.
12. *See infra* Part II, B–C.
13. *See* Douglas J. Cummings, Jr., *Authenticating Social Media Evidence at Trial: Instruction from Parker v. State*, 15 DEL. L. REV 107, 107 (2015) (explaining that many states don't have a set of uniform standards for dealing with the authentication process of evidence gathered from the social media accounts of defendants).
14. *See infra* Part IV.
15. Choi, *supra* note 10, at 5.

communication.[16] First presented by Speigal as a final project in a product design class, the app has since grown to become one of the most popular social media platforms in the United States.[17] In 2018, Snapchat surpassed the 90 million active user mark, and the average Snapchatter opens the app more than 20 times per day and spends an average of 30 minutes in the app each day.[18] Perhaps more importantly for those looking to the future, the app is used by 78% of Americans between the ages of 18 and 24.[19]

In order to understand the issues that might arise when attempting to authenticate Snapchat evidence, it is important to understand exactly how the app works in practice. The company itself describes the app in the following, relatively ambiguous, terms: "Enjoy fast and fun mobile conversation! Snap a photo or a video, add a caption, and send it to a friend. They'll view it, and then the Snap disappears from the screen—unless they take a screenshot!"[20] Snapchat attempts to maintain an "in-the-moment example of what's going on" by limiting the amount of time that content can be viewed, as well as the amount of content that users can later revisit.[21] Content on the app can be viewed for a limited amount of time; anywhere from one to ten seconds for direct messages to twenty-four hours for content posted to a User's Snap Story.[22]

One of Snapchat's most important features is that users can select the audience that will view the content that they post.[23] Where direct Snaps allow only an intended recipient to view the content, a Snap Story allows potentially anybody to view the content for up to twenty-four hours.[24] As is the case with most other social media apps, Snapchat has optional privacy settings that allow a user to block selected individuals from viewing their content.[25]

What especially distinguishes Snapchat from other social media platforms, however, is the subject matter of the content generated by its users.[26] Unlike other platforms such as Facebook or Instagram where users share images of special events or important milestones, Snapchat generally features images and

16. Joseph Hanlon, *What Is Snapchat?*, WHISTLEOUT (July 29, 2013), http://perma.cc/BVF3-PC9B.

17. *Id.*

18. Paige Cooper, *140+ Social Media Statistics that Matter to Marketers in 2020*, HOOTSUITE: BLOG (Feb. 20, 2020), https://blog.hootsuite.com/social-media-statistics-for-social-media-managers/#general.

19. *Id.*

20. *App Store Preview: Snapchat*, APPLE INC., https://apps.apple.com/us/app/snapchat/id447188370 (last visited Apr. 26, 2021).

21. Joseph B. Bayer et al., *Sharing the Small Moments: Ephemeral Social Interaction on Snapchat*, 19 INFO. COMM. & SOC'Y 956, 968 (2015).

22. Andrew C. Billings et al., *Permanently Desiring the Temporary? Snapchat, Social Media, and the Shifting Motivations of Sports Fans*, 5 COMM. & SPORT 10, 11 (2015); *Create a Snap*, SNAPCHAT, https://support.snapchat.com/en-US/a/capture-a-snap (last visited Apr. 26, 2021) [hereinafter *Create a Snap*]; *My Story*, SNAPCHAT, https://support.snapchat.com/en-US/article/view-stories (last visited Apr. 26, 2021) [hereinafter *My Story*].

23. *See generally* Elise Moreau, *10 Essential Snapchat Privacy Tips*, LIFEWIRE (Dec. 2, 2020), https://www.lifewire.com/snapchat-privacy-tips-4117444 (describing how to choose who can view a User's content and other privacy options). *See also Create a Snap*, *supra* note 22 (demonstrating the functionality of the app); *My Story*, *supra* note 22 (allowing custom audience options).

24. Billings et al., *supra* note 22, at 11; *Create a Snap*, *supra* note 22; *My Story*, *supra* note 22.

25. *Privacy Settings*, SNAPCHAT, https://support.snapchat.com/en-US/a/privacy-settings (last visited Apr. 26, 2021).

26. Bayer et al., *supra* note 21, at 967.

videos of everyday occurrences.[27] Users are less concerned with artistic expression, and instead focus on documenting mundane tasks or taking pictures of pets, the weather, or common locations such as their place of work or the post office.[28] This type of spontaneous content sets Snapchat apart from a platform such as Instagram, where users generally go to great lengths to produce polished work that will create a certain aesthetic.[29] This type of content also lends itself more than any other platform to the documentation of the commission of crimes, either in direct Snap form or through users posting accounts of their misdeeds on their Snapchat Stories.[30]

B. Social Media Authentication

In order to be admissible in court, documentary evidence generally must be authenticated, meaning that it must be shown to be what its proponent claims it to be.[31] The authentication process is governed by the Federal Rules of Evidence, specifically, rule 901.[32] Rule 901(a) establishes authentication as a condition precedent to the admissibility of nontestimonial evidence, while 901(b) identifies ten examples for how authentication can be accomplished.[33] Rule 901 is generally used in conjunction with Federal Rules of Evidence 104(a) and 104(b) during trial, as these latter two rules dictate that judges ensure evidence is authentic before they can make any type of relevance ruling.[34] This threshold for authentication is generally not particularly rigorous, as the rule favors admission of evidence.[35]

Authentication can be achieved in a number of ways, but the two most common for internet-based communications, like Snapchat, are testimony of a witness with personal knowledge, and distinctive characteristics of the communication.[36] Personal knowledge can most easily be achieved by putting the author of a communication on the witness stand and having them testify that they created it.[37] Alternatively, in instances where a photo or instant message was exchanged, the recipient can authenticate the communication.[38]

---

27. *Id.*

28. *Id.*

29. Anna Guerrero, *How to Establish an Instagram Aesthetic: 10 Brands Doing It Right*, HUBSPOT, https://blog.hubspot.com/marketing/establish-an-instagram-aesthetic (last updated Oct. 31, 2017).

30. *See, e.g.*, United States v. Lewisbey, 843 F.3d 653, 656 (7th Cir. 2016) (illustrating how inculpatory Facebook photos showing the defendant with guns and large sums of money provided conclusive evidence of guilt in a criminal prosecution for gun trafficking); Alyssa Mauk, *Social Media Increasingly Used In Crime Investigations*, J. TIMES (Nov. 24, 2018), https://journaltimes.com/news/local/crime-and-courts/social-media-increasingly-used-in-crime-investigations/article_d545eb34-1c9e-5b14-8373-a75f7dd6000d.html.

31. George L. Blum, *Authentication of Social Media Records and Communications*, 40 A.L.R.7th 1 (Originally published in 2019).

32. FED. R. EVID. 901.

33. *Id.*

34. FED. R. EVID. 104.

35. *Id.*

36. *See* Steven Goode, *The Admissibility of Electronic Evidence*, 29 REV. LITIG. 1, 18 (2009) (explaining that the distinct nature of online communication makes these two methods discussed in the text most useful).

37. Jonathan D. Frieden & Leigh M. Murray, *The Admissibility of Electronic Evidence Under the Federal Rules of Evidence*, 17 RICH. J.L. & TECH. 5, 19 (2011).

38. *Id.*

The personal knowledge requirement becomes somewhat problematic when dealing with Snapchat because it is a medium which primarily features some form of digital photography.[39] This makes it difficult to ensure that the image or video being admitted has not been manipulated or altered to distort the appearance of the events or subjects being featured.[40] Digital alteration in this sense generally means anything from resizing and reframing an image to changing the coloring and applying different filters.[41]

However, unless a digital photo has been enhanced in such a way that it changes the subject matter in a discernable way, authentication can be achieved through personal knowledge.[42] This requires a witness to testify that the image fairly depicts the subjects or locations at the time that it was taken.[43]

If authentication by personal knowledge is unavailable, then content from a user's social media can also be authenticated through distinctive characteristics.[44] To do this, a party must show that, along with the circumstantial evidence already provided in the case, the "appearance, contents, substance, internal patterns, or other distinctive characteristics" are sufficient to make a showing that the evidence being offered is what it purports to be.[45] However, the circumstantial evidence required to authenticate a piece of social media content varies significantly from case to case, and it is therefore difficult to make generalizations about using this method to authenticate.[46]

C. Common Problems with Social Media Authentication

The most common authentication problem related to social media is making a showing that a piece of media was actually sent by the person associated with the user account from which the content was sent.[47] This is true even in situations where a person's name is associated with their user account, as account holders can sometimes remain logged into their accounts on multiple devices and then leave those devices unattended for long periods of time.[48] Furthermore, usernames and passwords associated with accounts are susceptible to attacks from hackers, and it is therefore impossible to authenticate content simply because it is associated with a given user account.[49] Courts have generally agreed that a showing that a piece of content came from a given account without any further authenticating evidence is inadequate proof of authorship.[50]

---

39. Goode, *supra* note 36, at 20.
40. *Id.*
41. *Id.*
42. Goode, *supra* note 36, at 21.
43. *Id.*
44. Frieden & Murray, *supra* note 37, at 12.
45. FED. R. EVID. 901(b)(4).
46. Goode, *supra* note 36, at 21.
47. Honorable Paul W. Grimm et al., *Authentication of Social Media Evidence*, 36 AM. J. TRIAL ADVOC. 433, 448 (2018).
48. *Id.*
49. *Id.*
50. *Id.*

An example of the principles mentioned above can be found in *Tienda v. State*, a 2012 Texas criminal case.[51] Tienda was charged with murder, and at his trial the prosecution attempted to introduce evidence from multiple MySpace pages allegedly belonging to him.[52] Prosecutors put the victim's sister on the stand as a sponsoring witness for the MySpace pages, as well as a detective who could testify that gangs in the area typically used MySpace pages to carry out gang-related activities.[53] Each account stated that it had been created by a nickname typically associated with Tienda, and that the owner of the account lived in Dallas, which is where Tienda was from.[54] The accounts were also all registered to email addresses associated with Tienda and had links to photographs of someone who "strongly resembled" him.[55] Finally, instant messages from the account owner to others referenced details of the murder in question and made reference to the fact that the account owner was being electronically monitored.[56]

Nevertheless, Tienda's attorneys frequently objected to the authentication process for the MySpace accounts.[57] Their primary arguments were that MySpace accounts could be made in someone else's name relatively easily and this would then allow that person to pose as the purported account user to exchange messages and content with others.[58] They further argued that the detective called by the prosecution was not familiar with how MySpace pages were created and therefore couldn't adequately testify.[59] The trial court did not buy these arguments, finding that there was sufficient circumstantial evidence surrounding the authentication process to come to a conclusion that all three accounts were created and used by Tienda.[60] This decision was later upheld by the Texas Court of Appeals.[61]

State v. Assi, a criminal case litigated in the same year, exposed a similar set of problems with the authentication process.[62] Assi, who was being prosecuted for the murder of a rival gang member, allegedly had a MySpace page with the username "Flaco," a well-known nickname of his.[63] The authentication process for this page relied on evidence taken from the page itself, specifically photos of Assi himself.[64] These photos showed Assi posing with weapons and "throwing up gang signs," and the prosecution was able to call witnesses who could testify to the page belonging to him.[65] The court here also

51. Tienda v. State, 358 S.W.3d 633 (Tex. Crim. App. 2012).
52. *Id.* at 634.
53. *Id.* at 635.
54. *Id.*
55. *Id.*
56. *Id.* at 636.
57. *Id.*
58. *Id.*
59. *Id.*
60. *Id.*
61. *Id.* at 637.
62. State v. Assi, No. 1 CA-CR 10-0900, 2012 WL 3580488 (Ariz. Ct. App. Aug. 21, 2012).
63. *Id.* at *3.
64. *Id.*
65. *Id.*

found that there was sufficient circumstantial evidence to corroborate that the page belonged to Assi.[66]

While many of the problems associated with authenticating MySpace profiles can also be applied to Snapchat, there are other problems with authenticating Snaps unique to the platform.[67] Specifically, the transient nature of Snapchat content, both through user behavior and company policy, can occasionally present problems for prosecutors.[68] Photos and videos exchanged on the app are deleted from what the user is able to access, and the content is also deleted by the company from its own servers.[69] The timing of this deletion process depends on the format of the Snapchat content.[70] Direct messages are automatically deleted once they have been viewed by the intended recipient, while Stories are automatically deleted after 24 hours.[71]

The only way for a recipient of Snapchat content to permanently store it is to use their own image-capture software.[72] This process is called screenshotting, which creates an exact copy of the image currently on the screen and saves it to their cell phone.[73] When a recipient of a Snap screenshots it, the sender is accordingly notified.[74] There is, however, a method that some Snapchat recipients use to screenshot a Snap without notifying the sender.[75] Namely, rather than taking a screenshot, the recipient can use another person's phone to record or take a picture of the content being displayed on their own device.[76] This method is commonly used in cases where the recipient is aware that they are receiving Snapchat content that depicts some kind of criminal activity.[77] Authenticating Snapchat content gathered through either of the above approaches generally requires prosecutors to call the recipients of the content to the stand as witnesses, where they can then verify that the content is a fair and accurate depiction of the events that took place.[78]

III. ANALYSIS

The authentication process for content gathered from the Snapchat accounts of criminal defendants still varies significantly on a state-by-state basis. There are currently two states' approaches to the question of authenticating

66. *Id.* at *18.

67. *See When Does Snapchat Delete Snaps and Chats?*, SNAPCHAT, https://support.snapchat.com/en-US/a/when-are-snaps-chats-deleted (last visited Apr. 26, 2021) (explaining that most messages sent on Snapchat are deleted).

68. *Id.*

69. *Privacy Policy*, SNAPCHAT, https://www.snap.com/en-US/privacy/privacy-policy (last modified Nov. 24, 2019).

70. *When Does Snapchat Delete Snaps*, *supra* note 67.

71. *Id.*

72. *Id.*

73. Elise Moreu, *How to Take Snapchat Screenshot*, LIFEWIRE (Nov. 4, 2019), https://www.lifewire.com/capturing-snapchat-screenshots-3485993.

74. *Id.*

75. People v. Gray, 2019 WL 2314572, *2 (Ill. App. Ct. 2019).

76. *Id.*

77. *Id.*

78. Pugh v. State, 270 So. 3d 949, 957 (Miss. App. Ct. 2018).

social media evidence.[79] This section will explore both of these approaches and provide examples of outcomes when either of them is used during the course of criminal trial proceedings. It will also briefly explore the federal precedent for authenticating social media content, as well as the limited precedent for authentication of social media content in the state of Illinois.

A. The Maryland Approach

1. Overview

The Maryland Approach to authenticating social media content in criminal cases comes from the Court of Appeals Decision in *Griffin v. Maryland.*[80] Of the two standards discussed in this Note, the Maryland Approach provides the higher standard. The basic tenets of the Maryland Approach were articulated by the court as follows: to properly authenticate social media posts in Maryland, the admitting party should either (1) ask the purported creator if she created the profile and the post in question, (2) search the internet history and hard drive of the purported creator's computer to determine whether that computer was used to originate the social networking profile and post in question, or (3) obtain information directly from the social networking site to establish the identity of the creator and link the post in question to the person who initiated it.[81] The most important component of the court's rationale in articulating this standard is the concern that social media content may have been fraudulently created by someone other than the purported user.[82]

2. Factual Background

This action arose out of a petition by Antoine Levar Griffin after he was convicted of multiple shooting charges in conjunction with the death Darvell Guest.[83] Guest had been shot to death at Ferrari's Bar, a local hangout in Perryville, Maryland.[84] At trial, the State attempted to introduce the MySpace profile of Griffin's girlfriend Jessica Barber.[85] Printed pages from the Myspage page showed a profile name of "Sistasouljah," a nickname of Barber's, as well as descriptions of her hometown and date of birth.[86] The page also contained a photograph of an embracing couple and a blurb that read as follows: "FREE BOOZY!!!! JUST REMEMBER SNITCHES GET STITCHES!! U KNOW WHO YOUR ARE!!"[87]

---

79. *Compare* Griffin v. Maryland, 19 A.3d 415 (Md. 2011) (using a higher authentication standard for social media evidence), *with* Tienda v. State, 358 S.W.3d 633 (Tex. Crim. App. 2012) (using a more moderate authentication standard for social media evidence).

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

81. *Id.* at 427–28.

82. *Id.*

83. *Id.* at 418.

84. *Id.*

85. *Id.*

86. *Id.*

87. *Id.*

When Barber was called to the stand to testify about her role in the incident involving her boyfriend, the State chose not to question her about the printed pages from her MySpace page.[88] Instead, the prosecution attempted to authenticate the page through the testimony of the lead investigator on the case, Sergeant John Cook, to which defense counsel objected by arguing that the State would not be able to establish that Cook had sufficient personal knowledge to make a showing that the Myspace page actually belonged to Barber.[89] Defense counsel was allowed to voir dire investigator Cook outside the presence of the jury, but this ultimately led the trial judge to rule that Cook could testify in support of redacted portions of the Myspace profile.[90] Griffin was convicted at trial and appealed to the intermediate court where he lost.[91]

When the decision was appealed to the Maryland Court of Appeals, the Court of Appeals held that the prosecution failed to properly authenticate the Myspace pages pursuant to Maryland Rule 5-901, the state equivalent to Rule 901 of the Federal Rules of Evidence.[92] Specifically, it found that the prosecution failed to adequately link both the profile itself and the "snitches get stitches" post to Griffin's girlfriend.[93] The court also found that the trial court failed to acknowledge the possibility that that another user could have created a profile and authored the posts in question.[94]

3. Recent Updates

In the years since the decision in *Griffin* was handed down, the Maryland Court of Appeals has attempted to clarify the standard used for authenticating social media evidence.[95] Five years after the opinion in *Griffin* was written, the court passed a decision in *State v. Sublet*, which recognizes a need for the creation of a standard that aligns more closely with the Maryland Rules of Evidence.[96] Like the decision in *Griffin*, the court recognized that authenticating social media posts presents unique challenges because proving authorship can be complicated by factors relating to anonymity and ease of accessing accounts.[97] This means, the court found, that authentication is linked closely with actual ownership and the ease with which other parties are able to access a given account.[98] In its holding, the court emphasized the need to focus on distinctive characteristics to authenticate social media evidence.[99] This holding

88. *Id.*
89. *Id.* at 422.
90. *See* Cummings, *supra* note 13, at 109 (explaining that the voir dire process established sufficient circumstantial evidence, including investigative knowledge of Barber's nickname and relation to Griffin, to allow Cook to testify in support of the printed Myspace pages).
91. Griffin, 19 A.3d at 428.
92. *Id.* at 422.
93. *Id.* at 423.
94. *Id.* at 427.
95. *Id*. *See* Sublet v. State, 113 A.3d 695, 698 (Md. 2015) (clarifying the standards and procedures associated with authenticating social media accounts).
96. Griffin, 19 A.3d at 428; Sublet v. State, 113 A.3d at 710–11.
97. Sublet, 113 A.3d at 710–11.
98. *Id.* at 712–13.
99. *Id.* at 718.

contributes to the Maryland Approach to authentication being a much stricter standard than the one used by courts in Texas.[100] In the context of Snapchat use, this heightened standard could present problems since the profiles sometimes lack defining characteristics that could allow a jury to distinguish whether a user created the content in question.[101]

B. The Texas Approach

The Texas Approach to authenticating social media content in criminal trials comes from *Tienda v. State*, whose facts have already been discussed above. Courts following the Texas Approach apply a more moderate approach to the admission of social media evidence.[102] The proponent of a piece of evidence must essentially show what a "reasonable juror" would need to by persuaded that a piece of evidence is authentic.[103] The burden then shifts to the objecting party to show that the piece of evidence is not authentic.[104] The *Tienda* court recognized that its approach was a comparatively flexible alternative to the high standard advocated by the court in *Griffin v. Maryland*.[105]

The factual background of *Tienda v. State* has already been provided in an earlier section, so this section will focus on the Texas Court of Appeals response to the authentication issues raised by the defendant.[106] The primary question that the court was forced to grapple with was whether sufficient evidence was presented to establish a *prima facie* showing that the social networking pages offered by the prosecution were actually authored by the defendant.[107] Specifically, prosecutors sought to admit three Myspace profile pages which contained posts that were relevant to the commission of the offense that the defendant allegedly committed.[108] These pages were allegedly registered to and maintained by the defendant.[109] In order to authenticate the pages, the prosecution called the defendant's sister, who could testify to having seen some of the pictures and posts made on the page and could corroborate that they were made by the defendant.[110]

The intermediate Texas appellate court found that there was sufficient "individualization" in the comments and pictures on the Myspace profiles to satisfy Texas Rule of Evidence 901(b)(4).[111] It affirmed the decision of the lower court to admit the evidence, as there was sufficient evidence to support a finding that the person depicted on the Myspace profile had provided the

100. *See generally* George L. Blum, *Authentication of Social Media Records and Communications*, 40 AM. L. REP. 46 (2019) (describing the stricter standard found in the Maryland Approach).
101. Bayer et al., *supra* note 21, at 968.
102. Tienda v. State, 358 S.W.3d 633, 634 (Tex. Crim. App. 2012).
103. *Id.* at 642.
104. *Id.*
105. *Id.*; Griffin v. Maryland, 19 A.3d 415, 426–27 (Md. 2011).
106. Tienda, 358 S.W.3d at 647.
107. *Id.* at 636.
108. *Id.* at 634.
109. *Id.* at 637–38.
110. *Id.* at 634.
111. *Id.* at 637.

information that the State was attempting to enter into evidence.[112] This decision was affirmed by the Texas Criminal Court of Appeals.[113]

The Supreme Court of Texas explained that authentication of social media content requires a baseline showing that the matter in question is what the proponent claims it to be.[114] The court then went on to explain that making this determination is up to trial judges, as it is their "primary gatekeeping function" in dealing with evidentiary matters that gives them the ultimate say when it comes to questions of authentication.[115]

After explaining a judge's important role in the authentication process for social media content, the court went on to stress the flexibility of that process.[116] Specifically, the court suggested that there are many different methods of authenticating evidence that comes from social media sources, including through personal knowledge or by some combination of circumstantial evidence.[117] This flexibility was further illustrated by the suggestion that the authentication process itself should vary based on the previous evidence admitted over the course of the trial.[118] It suggested that, due to nearly constant innovation in different social media platforms and apps, there is no one way to authenticate evidence that comes from one of those sources.[119]

The court concluded its opinion by addressing the decision reached by the Maryland court in *Griffin v. State*—it suggested that the possibility of fraud and deception, the primary rationale behind the high standard advocated for by the Maryland court, is something for a jury to consider once the prosecution has made a *prima facie* showing that the content was maintained by someone with personal knowledge.[120] Ultimately, the court found that a more relaxed standard would be better able to handle the diverse set of problems that might arise when it comes to introducing different forms of social media content.[121]

C. Federal Precedent

Both the Texas and Maryland courts were preceded by a federal case, *Lorraine v. Markel American Insurance Company*.[122] This case is seen as an exhaustive guide to the admissibility of social media evidence in trials, and the case features a lengthy section on authenticating such evidence during the course

112. *Id.*
113. *Id.*
114. *Id.* at 640.
115. *Id.* at 647.
116. *Id.* at 649.
117. *Id.*
118. *Id.*
119. *Id.*
120. *Id.* at 651.
121. *Id.*
122. *See generally* Lorraine v. Markel American Insurance Company, 241 F.R.D. 534 (D. Md. 2007) (determining that proper, authenticated evidence is required for a motion to be successful). *See also* Ed Finkel, *Building Your Case with Social Media Evidence*, 102 ILL. B. J. 276, 279 (2014) (referring to *Loraine* as the "godfather of all cases" when it comes to issues of authentication for social media evidence).

of trial.[123] The opinion was written by Judge Paul Grimm, who is considered to be the leading jurist on the admissibility of social media evidence.[124] In it, Judge Grimm identified several useful tools for authenticating such evidence, including using the distinctive characteristics of specific posting habits to show that a user has a habit of posting in a certain way.[125] This specific characteristics approach has since been used in a number of other federal cases where social media content made up a significant portion of the available evidence.[126]

In *United States v. Vayner*, for example, the Second Circuit found that something beyond a defendant's name, photograph, and other biographical information was needed to properly authenticate their social media profile.[127] The court stated that the bar for authentication of social media evidence is not particularly high, but that it is still necessary to provide enough circumstantial evidence to conclusively suggest that a social media profile is what it purports to be.[128] Essentially, something beyond basic biographical information is required to ensure that a social media profile can be properly authenticated.[129]

This standard has been used by other courts since the *Vayner* decision was passed down, and it seems to be closer to the Maryland Approach to authentication than to the Texas Approach.[130] Requiring something beyond basic levels of biographical information is also important when analyzing how Snapchats should be authenticated, since most Snapchat profiles do not contain any kind of biographical information beyond perhaps the name of the user with whom the account is associated.[131]

D. Illinois Precedent

The seminal case for authenticating social media posts in Illinois is *People v. Kent*, an Appellate Court case that held that an IP address was likely sufficient to authenticate the Facebook post in question, in addition to other biographical information that could be discerned from the post such as name and appearance of the subject in question.[132] In reaching this decision, the Appellate Court relied heavily on the decision in *Vayner*.[133] It found that while the IP addresses provided were a strong signal that the posts could be authenticated, the proponents lacked sufficient additional biographical information to pass the

123. Breanne M. Democko, Comment, *Social Media and the Rules on Authentication*, 43 U. TOL. L. REV. 367, 395 (2012).

124. *Id.*

125. Lorraine, 241 F.R.D. at 548.

126. Linda Greene, *Mining Metadata: The Gold Standard for Authenticating Social Media Evidence*, 68 DEPAUL L. REV. 103, 112 (2017).

127. United States v. Vayner, 769 F.3d 125, 133 (2d Cir. 2014).

128. *Id.*

129. Greene, *supra* note 126, at 112.

130. *See* Vayner, 769 F.3d at 134 (stating the need for circumstantial evidence to authenticate evidence); Griffin, 19 A.3d at 428 (describing the higher standard in Maryland); Tienda v. State, 358 S.W.3d 633, 647 (Tex. Crim. App. 2012) (explaining the authentication standard in Texas).

131. *Privacy Settings*, *supra* note 25.

132. People v. Kent, 81 N.E.3d 578, 595 (Ill. App. Ct. 2017) (holding in dicta that the IP addresses for a Facebook post were sufficient to show that the post was authored by the person who the proponents of the evidence say authored it).

133. *Id.*

standard of admissibility.[134] The court refrained from providing examples of the specific types of evidence it would require to authenticate a piece of social media evidence, but did refer to examples from *Tienda*.[135] Examples included things like:

> [B]usiness records of an internet service provider or cell phone company show[ing] that the communication originated from the purported sender's personal computer or cell phone under circumstances in which it is reasonable to believe that only the purported sender would have had access to the computer or cell phone.[136]

The fact that *Tienda* was cited as an example of the types of authentication strategies that might be used shows that Illinois courts might be open to adopting the more liberal Texas standard when it comes to the authentication of Snapchat evidence.[137] Courts in Illinois have wavered somewhat in a string of unpublished opinions about the standard that should be used for authenticating these types of materials.[138] Creating a common standard could contribute to overall efficiency in the court system by allowing for a more uniform set of rules with respect to the authentication process.

E. Circumstantial Considerations

As a result of the unique nature of social media posts, courts have struggled to find a consistent set of rules when attempting to authenticate evidence that comes from user-generated online sources.[139] It is up to the litigants at trial to provide sufficient circumstantial evidence to prove that the piece of social media being offered is what its proponent purports it to be.[140] Generally speaking, the most common strategy used to authenticate a social media message is to present testimony from the recipient of the social media message.[141] For example, in *Campbell v. State*, a 2012 case from Texas, the court found that a series of Facebook messages, which were printed out and shown to the jury, could be authenticated by having the recipient of the messages testify that she really had received them and that she had not sent them to herself.[142] A majority of courts nationwide, however, have found that simply calling on the recipient of a social media message as a means of authentication is insufficient.[143] The primary rationale behind this trend is that social media accounts are capable of being

134. *Id.*
135. *Id.*
136. *Id.*
137. Greene, *supra* note 126, at 112.
138. *Id.*
139. *See* Paul W. Grimm et al., *Authentication of Social Media Evidence*, 36 AM. J. TRIAL ADVOC. 433, 441 (2013) (explaining the disparity in social media authentication methods among courts nationwide).
140. *See* State v. Eleck, 23 A.3d 818, 822 (Conn. App. Ct.) (giving a general background on the ways in which social media evidence might be authenticated at a criminal trial).
141. *See* Campbell v. State, 382 S.W.3d 545, 551 (Tex. Ct. App. 2012) (finding that in-court testimony from the recipient of a Facebook message was sufficient to establish authentication).
142. *Id.*
143. *See* Smith v. State, 136 So.3d 432, 434 (Miss. 2014) (explaining that additional testimony is sometimes necessary to establish a user's personal knowledge of the account in question).

manipulated by users other than the person whose name is associated with the account.[144]

F. Metadata Approach

Recently, a new approach to the authentication of social media evidence that focuses on metadata has made some headway, and its proliferation could have a substantial effect on the ways in which attorneys go about authenticating Snapchat evidence in criminal trials.[145] Generally speaking, metadata is any data that is generated automatically as a function of the application being used.[146] The metadata contained in a given social media post can vary dramatically based on the platform used, but it generally gives information such as how, when, and where a user posts to their account.[147] In the context of Snapchat, metadata might describe which smartphones were used to access a given account, as well as the IP addresses and mobile numbers of any devices from which posts were made.[148] This information could then be used to identify the originator of a social media post by linking a particular device to the person who had immediate access to it at the time that a post was made.[149] Metadata can be extremely useful for the authentication process of social media in general, especially for Snapchat, which allows users to post from different devices as long as they are logged in with their username and password.[150]

As previously discussed, Rule 901(b)(4) of the Federal Rules of Evidence provides that authentication can be accomplished via distinctive characteristics.[151] The basic biographical information for a person's social media account is provided by their username and any pictures or posts that are sent through the account.[152] Metadata, however, can provide some of the distinctive characteristics that might be crucial to authenticating a given piece of evidence.[153] Metadata provides information such as timestamps and unique identification numbers on posts associated with a given account. In addition, metadata may allow a user to access IP addresses and mobile device identifiers.[154] All of these are distinctive characteristics which might allow a jury to authenticate a piece of evidence with a higher degree of accuracy than they would otherwise be able to without this technology.[155]

---

144. *Id.*

145. *See* Greene, *supra* note 126, at 112 (explaining that this method has gained a fair amount of traction in recent years).

146. Lindsay Wise & Jonathan S. Landay, *Government Could Use Metadata to Map Your Every Move*, MIAMI HERALD (June 20, 2013), http://www.miamiherald.com/latest-news/article1952644.html.

147. Brian Focht, *Metadata Is Key to Getting the "Whole Truth" from Social Media*, CYBER ADVOC. (Jan. 14, 2015), http://www.thecyberadvocate.com/2015/01/14/metadata-is-key-to-whole-truth-in-social-media/.

148. *Id.*

149. Greene, *supra* note 126, at 112.

150. *See id.* at 112 (making a recommendation that metadata be used more frequently in the authentication process for multiple different social media platforms).

151. Nicholas O. McCann, *Tips for Authenticating Social Media Evidence*, 100 ILL. BAR. J. 482, 484 (2012).

152. Greene, *supra* note 126, at 112.

153. *Id.*

154. *Id.*

155. *Id.*

IV. RECOMMENDATION

The state of Illinois has a set of general standards that it applies to authenticating electronically stored information, or "ESI."[156] Generally, courts in Illinois have applied the same set of standards to electronic documents as they would to any other type of evidence when it comes to the authentication process.[157] However, courts in certain jurisdictions within the state have chosen to apply a stricter standard, finding that there are types of social media evidence which lack the necessary indicia of reliability that would allow them to be easily identifiable.[158] This stricter standard has more in common with the Maryland Approach to social media evidence discussed previously.[159] With social media posts, and Snapchat content in particular, becoming more commonly used in criminal trials throughout the state, Illinois should adopt the Texas Approach when dealing with the authentication process for evidence of Snapchat content. This will allow a wider body of evidence to be used when prosecuting a range of crimes and will lead to increased efficiency within a criminal justice system bogged down by the sheer volume of cases it is tasked with administering at any given time.[160]

A. Unique Elements of Snapchat

1. Lack of Permanent Content

One of the elements of the Snapchat operating system that might make the authentication process more difficult as compared to other forms of social media is automatic deletion.[161] As has been previously discussed to some degree, Snaps are deleted after a certain amount of time, and after that point the recipient no longer has access to the content.[162] The only option that recipients have to permanently access Snapchat content sent to them is to take a "screenshot" of the picture or message.[163] The sender is then given a notification that the recipient of the message or picture has taken such an action.[164] Unless recipients take screenshots that could refresh their recollection when testifying, this lack of permanence creates problems when authenticating Snaps because recipients

156. *See generally* McCann, *supra* note 151, at 484 (explaining the similarities between the authentication process for regular and electronic media in the state of Illinois).

157. *Id.* at 485.

158. *Id.* at 482.

159. *See supra* Part III.A.

160. *See generally* Cherly Niro, *Healing and the Criminal Justice System*, 87 ILL. BAR J. 512, 525 (1999) (explaining that the criminal justice system in Illinois is saddled with cases that it does not have the administrative capacity to handle).

161. *When Does Snapchat Delete Snaps and Chats?*, SNAPCHAT, https://support.snapchat.com/en-US/a/when-are-snaps-chats-deleted (last visited Apr. 26, 2021).

162. *Id.*

163. Joseph Hanlon, *What Is Snapchat?*, WHISTLEOUT (July 29, 2013), http://perma.cc/BVF3-PC9B.

164. *Id.*

must rely almost exclusively on their memory of the Snap or Snaps that they received.[165]

One possible solution to this permanence problem is on the horizon. A forensics company in Utah has created a service that allows it to retrieve deleted Snaps.[166] The technology allows the company to hack into the Snapchat app on a user's phone and recreate the Snapchat content which was previously deleted.[167] The technology has not yet been adopted by law enforcement officials, and in the context of litigation, it has only been used in divorce and personal injury cases to prove infidelity or misconduct on the part of a plaintiff.[168] Absent the use of such technology on a larger scale within the criminal trial process, courts must find a more efficient way to allow for the authentication of Snapchat evidence so that it might gain more widespread acceptance.

It becomes necessary to use an approach that allows Snapchat evidence to be authenticated by the jury itself, rather than relying on judges to make an initial determination that enough circumstantial evidence exists to allow it to be brought in at trial.[169] Using the Maryland Approach to authenticate Snapchat materials would give too much weight to a judge's determination of admissibility.[170] For authentication of Snaps, a process which requires testimony from recipients who may no longer have immediate access to the content they are describing, the high threshold created by the Maryland Approach would likely keep out a huge amount of otherwise useful evidence.[171] The Texas Approach, on the other hand, would allow jurors to assess the credibility of the witnesses describing the Snapchat content to be admitted, and then decide whether sufficient evidence of the content's admissibility has been presented.[172] This latter approach would give prosecutors in Illinois the flexibility that they need to authenticate Snapchat evidence that is no longer available in the form in which it was originally sent.

2. Availability of Metadata Use

As mentioned previously, metadata could be useful in the process of authenticating Snaps because of its ability to provide more relevant information about the devices which produce content.[173] The Texas Approach to

165. *See* McCann, supra note 151, at 482 (explaining that one of the primary concerns for attorneys attempting to enter social media content into evidence is that witnesses sometimes lack personal knowledge of the content in question).

166. Kashmir Hill, *Snapchats Don't Disappear: Forensics Firm Has Pulled Dozens of Supposedly-Deleted Photos from Android Phones*, FORBES (May 9, 2013), https://www.forbes.com/sites/kashmirhill/2013/05/09/snapchats-dont-disappear/?sh=5fc6730b2bdd.

167. *Id.*

168. *Id.*

169. *See* Tienda v. State, 358 S.W.3d 633, 642 (Tex. Crim. App. 2012) (holding that the authentication of social media evidence is a question that should be left up to the jury to decide).

170. *See* Griffin v. Maryland, 19 A.3d 415, 418 (Md. 2011) (explaining that judges should have some degree of input in making an initial authenticity determination for social media evidence).

171. *Id.*

172. Tienda, 358 S.W.3d at 642.

173. Greene, *supra* note 126, at 122–24.

authentication might be more useful for allowing the use of such metadata because of the less stringent standard it provides.[174] If attorneys are able to provide metadata in a Texas Approach context, it would increase the likelihood that evidence provided through Snapchat content would be authenticated by a jury and admitted into evidence.[175]

3. Practical Considerations

When attempting to gather evidence against the defendant in a criminal case, the prosecution must still be sure that its methods are complying with the law. Generally, obtaining social media evidence is governed by The Stored Communications Act ("SCA").[176] While the SCA was originally intended to only apply to text message and e-mail communications, it has since been applied to prohibit social media companies such as Facebook and Snapchat from disclosing personal information to the government without the account owner's consent.[177]

The SCA was originally intended to create a zone of privacy for users while also attempting to balance the Fourth Amendment rights of users with the need for law enforcement officials to gain access to information that they could use in the course of criminal prosecutions.[178] Essentially, it requires that law enforcement officials issue subpoenas to Internet Service Providers, which first forces them to disclose who has control over a piece of communication.[179] Once they figure out who has control over the communication, the same officials must go to the court and attempt to compel disclosure.[180]

The process outlined above can also create problems for the later authentication of the evidence obtained, especially as it relates to the Fourth Amendment rights of the owners of the accounts from which the information is drawn.[181] Generally, in order to gain access to the forms of communication that they seek, in this case Snaps or other data from a user's Snapchat account, law enforcement officials must circumvent users by gaining access to content directly from the platform.[182] The Fourth Amendment implications of this are that users are not aware when their information is being accessed, as Snapchat doesn't have to let them know that it is cooperating with law enforcement agencies.[183] This can create problems at trial during the authentication process

174. *Id.* at 110.

175. *Id.*

176. Stored Communications Act, 18 U.S.C. § 2701(a)(1)-(2) (2018).

177. *Id.*

178. *See id.* at 42 (explaining that the Act was a response by Congress to the seeming erosion of privacy rights in the digital age).

179. *See id.* at 41 (outlining the steps necessary to issue a subpoena to an Internet Service Provider and the considerations that have to be made in this process).

180. *Id.*

181. *See generally* Greene, *supra* note 126 (explaining that problems often arise in attempting to authenticate social media evidence that has not been obtained through the proper channels, making it difficult to determine whether it actually is what it purports to be).

182. *Id.*

183. *See* Victoria Cvek, *Policing Social Media: Balancing the Interests of Schools and Students and Providing Universal Protections for Students' Rights*, 121 PA. ST. L. REV. 583, 588 (2016) (describing the ways

for evidence obtained through these methods, as law enforcement officials might have trouble arranging for a representative from the social media platform to attest that a piece of evidence is what it purports to be as required by the Federal Rules of Evidence.[184]

Once again, the Texas Approach to authentication is best equipped to handle this problem. While the Maryland Approach would likely require law enforcement officials to bring at least one or multiple representatives from Snapchat to trial in order to authenticate a given picture or video, the Texas Approach would likely allow for the testimony of the law enforcement officials specifically involved in the investigation as long as they were able to thoroughly outline the steps that they took to recover the evidence, including providing a copy of the subpoena and explaining who they spoke with at Snapchat.[185] In terms of efficient use of court resources, it would certainly be better if the authentication of each picture being admitted required fewer people to attest to its authenticity, as calling multiple people would be much more time consuming.[186]

B. Policy Reasons for Choosing the Texas Approach

1. Overloaded Courts

One of the biggest policy issues currently facing the criminal justice system in the United States is the fact that many courthouses are overloaded with criminal cases without having sufficient resources to handle all of them.[187] This has led to a shift away from jury trials and towards a reliance by both prosecutors and criminal defense attorneys on plea bargaining agreements.[188] When criminal cases do go to trial, however, it is often at significant taxpayer expense, as the salaries of judges, court administrative staff, prosecutors, and public must be paid.[189] This creates an incentive for these trials to be litigated as quickly as possible, ,meaning that evidence should be admitted in an efficient manner.[190] Since significant amounts of evidence in criminal trials today comes from

in which the Fourth Amendment rights of social media platform users are implicated by providers allowing law enforcement officials access to these platforms).

184. *See* McCann, *supra* note 151, at 482 (explaining that one of the main problems with authentication can come from the fact that law enforcement officials struggle to find someone from a social media company who can actually come to trial and properly authenticate a piece of evidence).

185. *See* Grimm et al., *supra* note 47, at 443 (showing that the Texas standard to social media authentication often requires less people to be brought to the witness stand in order to authenticate a piece of evidence).

186. *Id.* at 445.

187. *See* Darryl Brown, *The Perverse Effects of Efficiency in Criminal Process*, 100 VA. L. REV. 183, 185 (2014) (demonstrating that modern courts frequently don't have the resources to adequately handle all the cases that on their dockets).

188. *Id.*

189. *See* Carson Guy, *Court Costs Break Down*, 78 TEX. B. J. 874, 876 (2015) (explaining how court costs are calculated and factored into the final cost scheme for every criminal case that is litigated within the state of Texas).

190. *See* Brown, *supra* note 187, at 186 (detailing the authentication process for evidence, which can often slow down trials to a significant extent).

Snapchat expediting the authenticated process would make the entire trial process more efficient.[191]

As has been explained throughout this Note, the Texas Approach to evidence authentication allows a lower bar for the authentication of Snapchat evidence.[192] Since the use of such evidence in criminal trials by both prosecutors and criminal defense attorneys is increasingly common, allowing for a lower bar for authentication would save a substantial amount of court resources and taxpayer dollars over the course of a year's worth of trials.[193]

V. CONCLUSION

As a social media platform that allows largely unfettered access to the lives of criminal defendants through photos, videos, and messages documenting the commission of crimes with which they are being charged, evidence from Snapchat will increasingly be used in criminal trials going forward. However, such evidence can be difficult to authenticate since it is sometimes unclear who authored a given piece of evidence. Even when it is clear, it can be difficult to have that person to testify in court.[194] Furthermore, the ease with which Snaps can be altered creates further authentication issues as it can be difficult for the proponent of a piece of Snapchat evidence to show that it is what it purports to be.[195] Currently, courts look to the approaches of two states, Texas and Maryland, to determine the appropriate standard for authenticating Snapchat evidence.[196]

The state of Illinois currently has no set standard for the authentication of social media evidence, but it would be wise to adopt an approach similar to the one used in Texas because this lower standard will allow for increased judicial efficiency and handle many of the problems inherent in Snapchat evidence described above. Using the Texas Approach will lead to criminal cases being litigated more quickly and will allow crucial Snapchat evidence to be admitted more easily in an age when it is becoming increasingly available to law enforcement officials and prosecutors.

191. *Id.* at 186; Guy, *supra* note 189, at 876.

192. *See* Grimm et al., *supra* note 47, at 448 (explaining that the Texas Approach is less stringent and allows for Snapchat evidence to be admitted more easily than under the Maryland Approach).

193. *See* Guy, *supra* note 189, at 878 (showing that a court cost breakdown really starts to add up over the course of a year rather than being taken over the course of a single trial).

194. Grimm et al., *supra* note 47, at 443.

195. Goode, *supra* note 36, at 18.

196. *See generally* Tienda v. State, 358 S.W.3d 633 (Tex. Crim. App. 2012) (describing the Texas Approach which is less stringent); Griffin v. Maryland, 19 A.3d 415 (Md. 2011) (detailing the Maryland Approach which is more exclusionary).