DePaul Law Review

Volume 68
Issue 1 *Fall 2018*

Article 5

Mining Metadata: The Gold Standard for Authenticating Social Media Evidence in Illinois

Linda Greene

MINING METADATA: THE GOLD STANDARD FOR AUTHENTICATING SOCIAL MEDIA EVIDENCE IN ILLINOIS

I. INTRODUCTION

From fake news[1] to catfish,[2] it is no wonder why social media is perceived to be untrustworthy.[3] As a result, many jurists continue to be skeptical of social media evidence.[4] The ease with which fake profiles can be created[5] and genuine profiles can be hacked poses significant difficulty in establishing authorship of social media posts.[6] Because social media is so vulnerable to exploitation, proving who authored a communication is vital to properly authenticating social media evidence.[7] For this reason, authentication is arguably the biggest hurdle to admission of social media evidence.[8] Authentication, or the process of identifying an item of evidence as what the proponent claims it to be, is a condition precedent to the admission of the evi-

1. A new poll suggests that Americans believe social media is responsible for the proliferation of fake news. *See* Alex Roarty, *Americans Blame Facebook for Fake News, a New Poll Finds*, MCCLATCHY DC BUREAU (Sept. 29, 2017), http://www.mcclatchydc.com/news/nation-world/national/article175970831.html.

2. The term "catfish" is used to describe "a person who sets up a false personal profile on a social networking site for fraudulent or deceptive purposes." *Catfish,* MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/catfish (last updated Sept. 27, 2018).

3. *See, e.g.,* Mark A. Cohen, *Law In The Age Of Social Media*, FORBES (Nov. 27, 2016, 11:50 AM), https://www.forbes.com/sites/markcohen1/2016/11/27/law-in-the-age-of-social-media/#6d8352981db8; Allison L. Pannozzo, Note, *Uploading Guilt: Adding A Virtual Records Exception to the Federal Rules of Evidence*, 44 CONN. L. REV. 1695 (2012).

4. Deborah Jones Merritt, *Social Media, the Sixth Amendment, and Restyling: Recent Developments in the Federal Law of Evidence*, 28 TOURO L. REV. 27, 51 (2012) ("The anonymity of the internet, combined with the ephemeral nature of some communications, makes some judges wary of accepting social media statements at face value."); Breanne M. Democko, Comment, *Social Media and the Rules on Authentication*, 43 U. TOL. L. REV. 367, 369 (2012).

5. At one point, it was estimated that 83 million Facebook accounts were either duplicate or fake accounts. Heather Kelly, *83 Million Facebook Accounts Are Fakes and Dupes*, CNN (Aug. 3, 2012, 5:27 AM), http://www.cnn.com/2012/08/02/tech/social-media/facebook-fake-accounts/index.html.

6. Nicole A. Keefe, *Dance Like No One Is Watching, Post Like Everyone Is: The Accessibility of "Private" Social Media Content in Civil Litigation*, 19 VAND. J. ENT. & TECH. L. 1027, 1047 (2017).

7. Ira P. Robbins, *Writings on the Wall: The Need for an Authorship-Centric Approach to the Authentication of Social-Networking Evidence*, 13 MINN. J.L. SCI. & TECH. 1, 5, 29 (2012).

8. Pannozzo, *supra* note 3, at 1709; Paul W. Grimm et. al., *Authentication of Social Media Evidence*, 36 AM. J. TRIAL ADVOC. 433, 439 (2013) [hereinafter Grimm 2013].

dence.[9] This requirement "advances one of the major goals of the rules of evidence: to ensure that, in the end, the 'truth may be ascertained and proceedings justly determined.'"[10] Unfortunately, the current evidentiary rules provide little guidance and courts are divided in their interpretation.[11] Considering the increasing role social media plays in litigation, the need for a streamlined approach is ever-pressing.[12]

To illustrate, suppose the Assistant State's Attorney has found the smoking gun in a murder case: an inculpatory statement posted on what appears to be the defendant's Facebook profile.[13] The problem is that the defendant denies that she authored the statement—her account must have been hacked.[14] Fortunately, Facebook records reveal the internet protocol (IP) address of the computer used to create the post, which is then linked to a device within the defendant's exclusive control.[15] In this instance, metadata—the data describing the Facebook transmission—becomes an "elegant weapon" to defeat an otherwise irrebuttable claim.[16] And unlike social media users, metadata does not lie.[17]

Metadata, as distinguished from the data it describes, is "neither created by nor normally accessible to the computer user" but is often generated automatically as a function of the application being used.[18] For instance, as a matter of practice, Facebook records metadata such as device identifiers, device locations, mobile phone numbers, and IP

9. *See* Fed. R. Evid. 901(a); Grimm 2013, *supra* note 8, at 439.

10. Robbins, *supra* note 7, at 5 (quoting Fed. R. Evid. 102).

11. Andy Radhakant & Matthew Diskin, *How Social Media Are Transforming Litigation*, 39 LITIG., Spring 2013, at 17, 20.

12. Pannozzo, *supra* note 3, at 1709; Paul W. Grimm et. al., *Authenticating Digital Evidence*, 69 BAYLOR L. REV. 1, 55 (2017) [hereinafter Grimm 2017].

13. The illustrative example is based on the facts of *People v. Kent*, 81 N.E.3d 578 (Ill. App. Ct. 2017).

14. Keefe, *supra* note 6, at 1047.

15. *Kent*, 81 N.E.3d at 591.

16. Brian Focht, *Metadata – Elegant Weapon of a More Civilized Attorney*, CYBER ADVOC. (Nov. 19, 2014) [hereinafter *Elegant Weapon*], http://www.thecyberadvocate.com/2014/11/19/metadata/; *see also* John Patzakis, *Judge Grimm's Important Guidance on Social Media Evidence Authentication*, X1 DISCOVERY: EDISCOVERY LAW & TECH BLOG (July 31, 2013, 12:46 PM), https://blog.x1discovery.com/2013/07/31/judge-grimms-important-guidance-on-social-media-evidence-authentication./.

17. Alan Rusbridger & Ewan MacAskill, *I, Spy: Edward Snowden in Exile,* GUARDIAN (July 19, 2014), https://www.theguardian.com/world/2014/jul/18/-sp-edward-snowden-interview-rusbridger-macaskill.

18. THE SEDONA CONFERENCE® WORKING GRP. ON ELEC. DOCUMENT RETENTION & PROD., THE SEDONA PRINCIPLES: BEST PRACTICES, RECOMMENDATIONS & PRINCIPLES FOR ADDRESSING ELECTRONIC DOCUMENT PRODUCTION 3 (2d ed. 2007) [hereinafter THE SEDONA PRINCIPLES].

addresses associated with a user profile and the posts therein.[19] Therefore, while the evidentiary rules are still adapting in their approach to computer-generated data, it is generally viewed as reliable.[20]

This Comment aims to demonstrate how using metadata can be a reliable and efficient method of addressing the challenges in authenticating social media evidence. It argues that metadata provides sufficient circumstantial evidence of authorship by establishing the device, the location from which a communication originated, or both.[21] More specifically, this Comment recommends that using metadata to authenticate social media evidence should be adopted as the standard practice in Illinois. By examining the influential cases, distilling the guidance provided by Illinois courts, and considering how evidentiary rules have responded to electronically stored information (ESI), this Comment concludes that courts are not only receptive but also endorse the use of metadata as a method of authentication.

This Comment begins by providing the relevant background information, by first describing metadata and its value to litigators.[22] Part II goes on to discuss the use of social media evidence in litigation and how courts have addressed challenges to its authenticity thus far.[23] Part II concludes by outlining how social media evidence may be authenticated under the rules of evidence.[24] Part III provides an analysis of how metadata can be used to address the most significant challenges associated with authenticating social media evidence: proving it is an accurate representation of what appeared online and proving who authored the communication in question.[25] The analysis then turns to address Illinois law specifically, demonstrating how using metadata is the best method of authentication based on the guidance provided by Illinois courts.[26] Finally, Part IV considers the feasibility of using metadata as the standard practice given the relevant privacy and cost concerns.[27] It outlines the collateral benefits of using

19. *Data Policy*, FACEBOOK, https://www.facebook.com/policy.php (last updated Sept. 29, 2016).

20. *See infra* Parts II.D.1–II.D.2 and the discussion of the new federal rules; *see also infra* notes 280–85 and accompanying text for an analysis of the Illinois approach to computer-generat ed data.

21. *See infra* Part III.A.2.

22. *See infra* Part II.A.

23. *See infra* Part II.B–II.C.

24. *See infra* Part II.D.

25. *See infra*, Part III.A.

26. *See infra* Part III.B.

27. *See infra* Part IV.A.

metadata, ultimately determining that it is not only a feasible but also an efficient means of admitting social media evidence.[28]

II. Background

Besides authentication, metadata has played a part in litigation since the rise of e-discovery.[29] Thanks to Edward Snowden, metadata became the topic of everyday conversation in 2013.[30] Still, it is arguable whether metadata is a commonly understood term. Therefore, this section begins by describing what metadata is and its utility in litigation. The section proceeds to acknowledge the impact social media has on litigation and presents the challenges with authenticating it. Next, it provides background on how courts have addressed these challenges, followed by strategies for authenticating social media with metadata under the rules of evidence.

A. What is Metadata?

Simply put, metadata is data about data.[31] A useful analogy is the Dewey Decimal System once used by libraries to catalog books.[32] Information such as the title, author, and genre contained in the card catalog is metadata that describes a book.[33] Similarly, the Exchangeable Image File Format (EXIF) data embedded in a digital photograph describes the time, date, and GPS coordinates of the photo.[34] The

28. *See infra* Part IV.B.

29. James E. Bibart, Comment, *Metadata in Digital Photography: The Need for Protection and Production of this Silent Witness*, 44 Cap. U. L. Rev. 789, 792 (2016). E-discovery, which is short for electronic discovery, is simply the term applied to the discovery of electronically stored information. *The Sedona Conference Glossary: E-Discovery & Digital Information Management (Fourth Edition)*, 15 Sedona Conf. J. 305, 323 (2014) [hereinafter *Sedona Glossary*] (defining e-discovery as "[t]he process of identifying, locating, preserving, collecting, preparing, reviewing, and producing Electronically Stored Information (ESI) in the context of the legal process."). As the use of ESI as evidence has become increasingly prevalent, the procedures by which attorneys engage in discovery has necessarily adapted.

30. *See* Matthew Heller, *Government Downplaying Sensitivity Of Metadata Collected By NSA*, MintPress News (June 24, 2014), http://www.mintpressnews.com/government-downplaying-sensitivity-of-metadata-collected-by-nsa/192810/.

31. 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.

32. *Id.*

33. *Id.*

34. Heidi Redlitz, *Your Online Photos Can Expose Your Private Data. Here's How to Stop It*, TruthFinder (Aug. 23, 2016), https://www.truthfinder.com/infomania/safety/remove-exif-data-geotag/. Not all photos posted online reveal GPS location information as this feature can be disabled and some—but not all—social media sites strip EXIF data from uploaded photos. Chris Hoffman, *How to See Exactly Where a Photo Was Taken (and Keep Your Location Private)*,

metadata contained in a social media post varies by platform,[35] but generally, it reveals how, when, and where a user posted to her account.[36] For instance, Facebook collects information about the computers and smartphones used to access its services, including device identifiers, location information, IP addresses,[37] and mobile numbers.[38] Such information could then be used to identify the originator of a social media post by linking the particular computer to the person who had access to it at the specific time and place.[39]

Metadata has proven useful to litigants in other ways. Most prevalently, metadata is used to facilitate the discovery of ESI.[40] Metadata is valuable when utilized by e-discovery technology to search, cull, and analyze large amounts of data more efficiently.[41] For instance, timestamps can be used to identify the data pertinent to the particular time period in question.[42] Likewise, location data can be used to identify the data originating from the scene of the accident.[43] Metadata is essential to the de-duplication process whereby excess copies of a file are excluded from the dataset.[44]

How-to Geek (May 17, 2017), https://www.howtogeek.com/211427/how-to-see-exactly-where-a-photo-was-taken-and-keep-your-location-private/.

35. *Elegant Weapon*, *supra* note 16 (listing the metadata available from several platforms).

36. 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/.

37. Internet Protocol (IP) addresses are assigned to every computer on the internet. Tim Fisher, *What Is an IP Address?: Definition of IP Address and Why All Computers and Devices Need One*, Lifewire, https://www.lifewire.com/what-is-an-ip-address-2625920 (last updated Sept. 5, 2018). Just like license plates, IP addresses are unique serial numbers used for identification. *Id.*

38. *Data Policy*, *supra* note 19. Facebook's data policy expressly states that it will "access, preserve and share your information . . . [i]n response to a legal request (like a search warrant, court order or subpoena) if [it has] a good faith belief that the law requires [it] to do so." *Data Policy*, *supra* note 19. Whether a warrant or subpoena is required depends on a number of considerations governed by the Stored Communications Act, 18 U.S.C. § 2701 et seq. (2012), and the operation the third-party doctrine as limited by the Supreme Court's decision in *Carpenter v. United States*, 138 S. Ct. 2206 (2018). *See infra* Part IV.A.

39. Richard S. Kling et al., *Admissibility of Social Media Evidence in Illinois*, 105 Ill. B.J. 38, 41 (2017).

40. The Sedona Conference, *The Sedona Principles, Third Edition: Best Practices, Recommendations, & Principles for Addressing Electronic Document Production,* 19 Sedona Conf. J. 1, 170 (2018).

41. *Id.*

42. Tom Turner, *How Metadata Can Affect a Case*, Today's Gen. Couns., June/July 2014.

43. *See* Mark D. Hansen & Tyler J. Pratt, *Follow the Audit Trail: The Impact of Metadata in Litigation*, Def. Couns. J., July 2017, at 3, 6.

44. *Sedona Glossary*, *supra* note 29, at 319. De-duplication is typically achieved by calculating a file's hash value using a mathematical algorithm. *Sedona Glossary*, *supra* note 29, at 319. Because hash values are unique to the file, if file Y were to return the same hash value as file X,

Sometimes, metadata bears directly on the merits of a case.[45] Not surprisingly, metadata is "smoking gun" evidence in a claim for negligent spoliation of evidence.[46] This is because computer forensic technicians can use metadata to detect manipulation[47] and metadata can reveal activity associated with records the user believed to be deleted.[48] Metadata has become increasingly relevant in medical malpractice suits because of its utility in creating an audit trail of the patient's medical records.[49] It is also indispensable in trucking litigation, where Event Data Recorders that log driver reaction times through braking, acceleration, and vehicle movement data are compared to cell phone use.[50] The increasing use of metadata in litigation is not surprising given the prevalent use of ESI, and especially social media, in litigation.[51]

B. Social Media in Litigation

Not only does social media usage form the basis of many lawsuits and criminal prosecutions today, but it is also often outcome determinative.[52] There are many examples of instances where criminal defendants have posted inculpatory pictures or admissions.[53] On the other hand, a criminal defendant may offer social media posts to prove the victim was the first aggressor.[54] In the civil context, social media provides evidence of torts such as harassment and defama-

---

then file X and Y are identical copies and only one of them need be retained. For more information on hash values, see notes 151–157 and accompanying text *infra*.

45. The Sedona Conference, *supra* note 40, at 170.

46. Turner, *supra* note 42. Illinois law has recognized a cause of action for negligent spoliation where a defendant has breached her duty to preserve evidence. While there is no general duty to preserve evidence, such a duty "may arise through an agreement, a contract, a statute or another special circumstance." Boyd v. Travelers Ins. Co., 652 N.E.2d 267, 270–71 (Ill. 1995) (internal citations omitted).

47. Michael J. Hannon, *An Increasingly Important Requirement: Authentication of Digital Evidence*, 70 J. MO. B. 314, 318 (2014).

48. Turner, *supra* note 42, at 21.

49. *See* Hansen & Pratt, *supra* note 43, at 4.

50. Hansen & Pratt, *supra* note 43, at 6.

51. Hannon, *supra* note 47, at 319.

52. Justin P. Murphy & Adrian Fontecilla, *Social Media Evidence in Government Investigations and Criminal Proceedings: A Frontier of New Legal Issues*, 19 RICHMOND J.L. TECH., no. 3, 2013, at 11, 28; *see also* Grimm 2013, *supra* note 8, at 437–38.

53. *See infra* Part II.C; *see, e.g.*, United States v. Lewisbey, 843 F.3d 653, 656 (7th Cir. 2016) (illustrating how inculpatory Facebook photos showing the defendant with lots of guns and large sums of money provided conclusive evidence of guilt in a criminal prosecution for gun trafficking).

54. *See, e.g.*, People v. Nunn, No. 3–14–0137, 2016 WL 2866361 at *8 (Ill. App. Ct. May 16, 2016).

tion.[55] It may prove useful in defending against personal injury and workers' compensation suits.[56] Furthermore, the use of social media has become exceedingly prevalent in family law.[57] More generally, online profiles are treasure troves of personal information that provide excellent fodder for impeachment on cross-examination, especially given the level of candor on social media.[58]

But social media evidence is susceptible to a host of evidentiary challenges, including authenticity, relevancy, hearsay, and best evidence.[59] Arguably, the most confounding of these issues is authenticity.[60] The authentication of social media evidence can be accomplished under the traditional rules; however, their application presents difficulty in two respects.[61] First, vulnerability to hackers and even innocent alteration since the original post raises potential doubts as to whether the evidence is an accurate representation of the social media content.[62] Second, proving authorship is complicated by the fact that social media communications are stored on remote servers, are ephemeral and collaborative in nature, and are vulnerable to manipulation and fabrication.[63] Although there are many methods for authenticating social media evidence, there is no consensus among jurisdictions.[64] This confusion gives rise to arguments of error on appeal and leaves lawyers vulnerable to malpractice actions.[65]

C. Caselaw to Date

State cases that address the authentication of social media evidence essentially fall into two camps: the Maryland approach or the Texas approach.[66] Skeptical of social media, the Maryland approach imposes a heightened standard for admitting evidence.[67] Under this approach, proponents must affirmatively disprove the possibility that someone

55. Aviva Orenstein, *Friends, Gangbangers, Custody Disputants, Lend Me Your Passwords*, 31 Miss. C. L. Rev. 185, 193 (2012).

56. *Id.*

57. *Id.*

58. Radhakant & Diskin, *supra* note 11, at 18–19.

59. Pannozzo, *supra* note 3, at 1698.

60. *Id.*

61. David I. Schoen, *The Authentication of Social Media Postings*, 19 Trial Evidence, May 17, 2011, at 6.

62. *Id.*

63. Kling et al., *supra* note 39, at 40.

64. *Id.*

65. *Id.*

66. Wendy Angus-Anderson, *Authenticity and Admissibility of Social Media Website Printouts*, 14 Duke L. & Tech. Rev. 33, 37 (2015).

67. *Id.*

other than the putative author created the social media content.[68] By contrast, under the Texas approach, once the proponent has made a prima facie showing of authorship, the burden shifts to the objecting party to prove a third-party created the content.[69] After examining these two approaches, this section follows up by highlighting influential federal cases, before turning to Illinois precedent.

1. The Maryland Approach

The Maryland approach was first articulated in *Griffin v. State*.[70] In *Griffin*, the State sought to admit printouts from a Myspace profile allegedly belonging to the defendant's girlfriend to prove that she had threatened another witness.[71] The profile contained her birthdate, location, a photograph of the couple, and a caption: "FREE BOOZY!!! JUST REMEMBER SNITCHES GET STITCHES!! U KNOW WHO YOU ARE!!"[72] The intermediate appellate court found that the photograph, location, and birthdate provided sufficient circumstantial indicia of reliability.[73] The Maryland Court of Appeals, the highest court in the State, found that the lower court failed to consider the possibility that another user could have created the profile or written the "snitches get stitches" comment and thus, held the printouts were inadequately authenticated.[74]

The court reasoned that the "potential for abuse and manipulation of a social networking site by someone other than its purported creator" calls for a higher degree of scrutiny.[75] The court then identified three means by which social media evidence could be properly authenticated: (1) asking the putative author to admit to creating the content at issue; (2) examining the internet history and hard drive of the computer of the putative author; or (3) obtaining information directly from the social network provider that links the profile and its content to its alleged creator.[76]

---

68. *Id.*
69. *Id.*
70. 19 A.3d 415 (Md. 2011); Angus-Anderson, *supra* note 66, at 37.
71. *Griffin,* 19 A.3d at 418.
72. *Id.*
73. *Id.* at 423.
74. *Id.*
75. *Id.* at 424.
76. *Id.* at 428.

2. The Texas Approach

The more lenient Texas approach was first articulated by *Tienda v. State*.[77] Similar to *Griffin*, the State in *Tienda* introduced printouts of three Myspace profiles belonging to the defendant.[78] The profiles contained numerous photographs of the defendant displaying his unique gang-affiliated tattoos, several boastful references to the shooting in question, and a link to the music played at the victim's funeral.[79] Additionally, the State offered "subscriber reports" and accompanying affidavits subpoenaed from Myspace.[80] According to the subscriber reports, the accounts were registered to email addresses containing the defendant's name or widely-known nickname.[81]

In a footnote, the court noted that the subscriber reports also contained the IP addresses associated with each account.[82] However, no testimony was elicited as to whether these IP addresses corresponded to a device belonging to the defendant or to which he had access.[83] Recognizing that the State had failed to utilize any authentication method described in *Griffin*,[84] the court nevertheless held that the profiles were sufficiently authenticated via circumstantial evidence.[85] The court distinguished *Griffin*, finding that the numerous photographs portraying the distinctive features of the defendant and detailed knowledge of the circumstances surrounding the shooting were enough to justify admission.[86] Although there is some disagreement as to whether the Maryland or Texas approach is more effective,[87] both *Griffin* and *Tienda* contemplate using metadata provided by social media companies.[88]

---

77. 358 S.W.3d 633 (Tex. Crim. App. 2012); Angus-Anderson, *supra* note 66, at 41.

78. *Tienda*, 358 S.W.3d at 634–35.

79. *Id.*

80. *Id.* at 645.

81. *Id.* at 635.

82. *Id.* at 635 n.4.

83. *Id.*

84. The *Tienda* court observed that the first method offered in *Griffin*, asking the user to admit they created the social media profile or authored the content therein, was simply not viable when the purported author is a criminal defendant. *Tienda,* 358 S.W.3d at 647.

85. *Id.*

86. *Id.*

87. *See* Grimm 2013, *supra* note 8, at 456 ("The approach adopted by [Texas] is better reasoned, as it affords appropriate deference to the interplay between the evidence rules that govern the admissibility of social media evidence . . . .").

88. Griffin v. State, 19 A.3d 415, 428 (Md. 2011); *Tienda*, 358 S.W.3d at 647.

3. Federal Precedent

Neither case was the first to consider metadata as a method of authentication. Any discussion of the caselaw concerning the authentication of social media evidence would be remiss without mentioning the "godfather of all cases," *Lorraine v. Markel American Insurance Company*.[89] *Lorraine* is recognized as an exhaustive guide on the admissibility of ESI evidence.[90] The opinion was written by the Honorable Paul Grimm, who is now considered to be "the leading jurist on [the] subject."[91] The oft-cited decision explains how several evidentiary rules are properly applied to ESI.[92] In *Lorraine*, Judge Grimm identified metadata as "a useful tool for authenticating electronic records by use of distinctive characteristics."[93] Since then, several other federal cases have specifically examined the use of metadata to authenticate social media evidence.

For instance, in *United States v. Hassan* the Fourth Circuit affirmed the district court's ruling that Facebook pages and YouTube videos were properly authenticated.[94] First, the district court ruled that the pages and videos were self-authenticating as business records based on certifications of record custodians at Facebook and Google.[95] Second, the court found the prosecution successfully linked the pages to the defendants by tracking the Facebook accounts to the defendants' mailing addresses via IP addresses.[96]

By contrast, in *United States v. Browne* the Third Circuit disagreed with the *Hassan* court that Facebook chat logs could be self-authenticated as business records.[97] Although the Facebook record custodian confirmed that the communications took place between certain Facebook accounts on particular dates and times, the court required evidence that the defendant authored such communications.[98] Nonetheless, the court recognized that by obtaining the logs directly from

89. 241 F.R.D. 534 (D. Md. 2007); Ed Finkel, *Building Your Case with Social Media Evidence*, 102 ILL. B.J. 276, 279 (2014).

90. Democko, *supra* note 4, at 395.

91. Hannon, *supra* note 47, at 314.

92. *See* Democko, *supra* note 4, at 380; Siri Carlson, *When Is A Tweet Not an Admissible Tweet? Closing the Authentication Gap in the Federal Rules of Evidence*, 164 U. PA. L. REV. 1033, 1065 (2016). According to Westlaw, *Lorraine* has been cited by 185 cases and in many jurisdictions (last viewed Oct. 31, 2018).

93. *Lorraine*, 241 F.R.D. at 548.

94. United States v. Hassan, 742 F.3d 104, 133 (4th Cir. 2014).

95. *Id.*

96. *Id.*

97. United States v. Browne, 834 F.3d 403, 410 (3d Cir. 2016).

98. *Id.* Ultimately the court found that the government had otherwise produced enough circumstantial evidence for a reasonable jury to find the chat records authentic. *Id.* at 413.

Facebook, along with a certificate attesting to their maintenance by automated systems, the Government bolstered confidence in their accuracy.[99]

The Second Circuit declined to opine as to "what kind of evidence *would* have been sufficient to authenticate the [social media] page and warrant its consideration by the jury" in *United States v. Vayner*.[100] The court instructed that "[t]he bar for authentication of evidence is not particularly high" and "[t]he proponent need not rule out all possibilities inconsistent with authenticity."[101] The court held that although the defendant's name, photograph, and some details about him were present on the page, this information was insufficient evidence that the defendant created the page.[102] The court's pronouncement that something beyond biographical information is required, while at the same time acknowledging that conclusive proof is not required, has been influential to other courts.[103]

4. Illinois Precedent

The Illinois Appellate Court relied heavily on *Vayner* when it decided its seminal case "addressing the admissibility of a Facebook post allegedly attributable to a criminal defendant."[104] In *People v. Kent*, the Illinois Appellate Court hinted in dicta that an IP address might have been sufficient to authenticate the Facebook post in question.[105] The State offered a screenshot of a Facebook page containing a photograph resembling the defendant, the defendant's name and nickname, and a post stating, "its my way or the highway . . . . . leave em dead n his driveway."[106] The trial court admitted the post based on the State's claim that Facebook records would reveal that the post was associated with an IP address belonging to the defendant's girlfriend.[107] How-

99. *Id.* at 415–16.

100. 769 F.3d 125, 133 (2d Cir. 2014) (emphasis in original).

101. *Id.* at 130 (quoting United States v. Gagliardi, 506 F.3d 140, 151 (2d Cir. 2007)).

102. *Id.* at 132 ("[T]here was no evidence that [the defendant] himself had created the page or was responsible for its contents.").

103. *See* People v. Kent, 81 N.E.3d 578, 592 (Ill. App. Ct. 2017) ("[W]e conclude that *United States v. Vayner* . . . best represents a line of cases that is on point and persuasive.") (internal citation omitted); Sublet v. State, 113 A.3d 695, 714 (Md. 2015) ("[W]e find succor in the standard articulated by the United States Court of Appeals for the Second Circuit in *United States v. Vayner*.").

104. *Kent*, 81 N.E.3d at 592.

105. *Id.* at 595.

106. *Id.* at 591.

107. *Id.*

ever, the State failed to produce any extrinsic evidence of authorship at trial.[108]

As a result, the Illinois Appellate Court reversed the verdict.[109] The court held that "more than a 'simple name and photograph'" is needed to sufficiently link the communication to the putative author.[110] Although the court refrained from deciding the specific type and quantum of evidence necessary to authenticate a Facebook post, it referred to the examples provided in *Tienda* for guidance.[111] Among these were:

> [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.[112]

The court went on to observe that allowing the prosecution "to argue that the Facebook post was tantamount to an admission" without "'some basis' on which a reasonable juror could conclude that the post was not just any Internet post, but was in fact created by defendant or at his direction" was not harmless, but reversible error.[113]

On the other hand, in a previous unpublished opinion, another Illinois Appellate Court ruled that it was reversible error to exclude a Facebook printout proffered by a criminal defendant.[114] In *People v. Nunn*, the trial court allowed the defendant to testify about the Facebook messages exchanged between himself and the victim but refused to admit printouts of the same.[115] The defense aimed to use the Facebook messages to support its theory of the case and its self-defense claim: that the defendant met with the victims to sell them a gun, rather than to rob them during a drug deal.[116] Although the court ruled that the Facebook messages could be authenticated, it ultimately sided with the State in deciding that the printout was evidence of a collateral matter and thus was not relevant.[117]

The appellate court disagreed, finding that the Facebook messages "pertained to defendant's state of mind and intent, an essential ele-

---

108. *Id.*
109. *Id.* at 599.
110. *Kent*, 81 N.E.3d at 598 (Ill. App. Ct. 2017) (quoting Smith v. State, 136 So. 3d 424, 433 (Miss. 2014)).
111. *Id.* at 598–99.
112. *Id.* at 598 (quoting *Smith*, 136 So. 3d at 433).
113. *Id.* at 599 (internal quotations omitted).
114. People v. Nunn, No. 3–14–0137, 2016 WL 2866361 at *9 (Ill. App. Ct. May 16, 2016).
115. *Id.* at *4.
116. *Id.*
117. *Id.*

ment of the underlying charges and defendant's claim of self-defense."[118] The court held that because "[t]he printout was arguably the most probative evidence available on that issue—even more probative tha[n] the defendant's own testimony"—it was an abuse of discretion for the trial court to exclude it.[119] Thus, consistent with the court's ruling in *Kent*, the *Nunn* court considered an error regarding the admissibility of social media evidence attributable to a criminal defendant dispositive on the verdict.[120]

Most recently, an Illinois Appellate Court again considered the admissibility of Facebook messages, but this time under the rules for hearsay.[121] In *People v. Maya*, the appellate court upheld the admission of Facebook messages under the business records exception.[122] Similar to its federal analog, the business record exception under Illinois Rule of Evidence 803(6) provides that records kept in the course of a regularly conducted business activity are admissible with a certificate of authenticity from the record custodian.[123] In *Maya*, the certificate attested to the fact that the messages were recorded by the automated systems of Facebook in the regular course of business and as a matter of practice, and thus complied with requirements for self-authentication under Rule 902(11).[124] Although the defendant in *Maya* did not directly challenge the authenticity of the messages by denying authorship, its precedential value is unmistaken: Illinois courts are willing to consider Facebook records as self-authenticating.

Putting aside *Nunn* and *Maya*, when you consider *Kent* and the other cases surveyed above, they all agree on one thing: proving authorship is the key to authenticating a social media post.[125] Whether Illinois decides to adopt the more permissive Texas approach followed by federal courts,[126] or resolves to apply a heightened standard of proof for social media authenticity, metadata can be useful in proving authorship.[127]

---

118. *Id.* at *9.

119. *Id.* at *8.

120. *Nunn*, 2016 WL 2866361 at *9.

121. People v. Maya, 88 N.E.3d 10, 30 (Ill. App. Ct. 2017).

122. *Id.* at 30–31.

123. Ill. R. Evid. Rule 803(6).

124. *Maya*, 88 N.E.3d at 30–31.

125. Robbins, *supra* note 7, at 30.

126. Panel Discussion, *Symposium on the Challenges of Electronic Evidence*, 83 FORDHAM L. REV. 1163, 1178 (2014) (agreeing that the federal cases apply the Texas approach because it is more consistent with the low threshold established by Rule 901(a)).

127. John Patzakis, *Overcoming Potential Legal Challenges to the Authentication of Social Media Evidence*, FORENSIC FOCUS (Apr. 2. 2012) [hereinafter FORENSIC FOCUS], https://articles.

D. How to Prove the Authenticity of Social Media Evidence

As the cases discussed above suggest, metadata can provide sufficient circumstantial evidence of authenticity.[128] But demonstrating how metadata can be used for authentication necessitates discussion of the pertinent evidentiary rules. Social media, and ESI generally, can be authenticated under the traditional rules of authentication.[129] Recently, however, new federal rules have been enacted to include machine-generated data and copies of ESI as self-authenticating.[130] This section first discusses how to use metadata to authenticate social media under the traditional federal rules, especially Rule 901(b)(4), as distinctive characteristics. Second, this section describes how the new federal rules might be applied to metadata before discussing how Illinois approaches computer-generated data. Finally, it observes the importance of conditional relevance under Rule 104(b).

1. Metadata as Distinctive Characteristics under Rule 901(b)(4)

Rule 901(b)(4) provides that authentication can be accomplished via its distinctive characteristics including, but not limited to, "the appearance, contents, substance, [or] internal patterns . . . of the item, taken together with all the circumstances."[131] In addition to basic biographical information and photographs included on the face of a social media page, the associated metadata are also distinct characteristics that can be used to establish authenticity.[132] Metadata harvested from a Facebook post can provide information such as the timestamp and unique identification numbers of the post, the author, and the account associated with it.[133] Uploaded photographs, tweets,

---

forensicfocus.com/2012/04/02/overcoming-potential-legal-challenges-to-the-authentication-of-social-media-evidence/.

128. Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 548 (D. Md. 2007) ("[M]etadata certainly is a useful tool for authenticating electronic records by use of distinctive characteristics."); Griffin v. State, 19 A.3d 415, 428 (Md. 2011) (suggesting that basic subscriber information can be used to link the author to the profile); People v. Kent, 81 N.E.3d 578, 598–99 (Ill. App. Ct. 2017) (suggesting, in dicta, that Facebook records would have been sufficient for authentication).

129. *See generally* Panel Discussion, *supra* note 126, at 1180 (discussing whether the Federal Rules of Evidence should be revised to address digital evidence).

130. *See* Fed. R. Evid. 902(13); Fed. R. Evid. 902(14).

131. Fed. R. Evid. 901(b)(4); Ill. R. Evid. 901(b)(4). Subsection 4 of Rule 901(b) is identical under Illinois and Federal law.

132. FORENSIC FOCUS, *supra* note 127.

133. John Patzakis, *Key Facebook Metadata Fields Lawyers and eDiscovery Professionals Need to be Aware of*, X1 DISCOVERY: EDISCOVERY LAW & TECH BLOG (Oct. 11, 2011), https://blog.x1discovery.com/2011/10/11/key-facebook-metadata-fields-lawyers-and-ediscovery-professionals-need-to-be-aware-of/.

and Snapchat geofilters may even include location information.[134] Additionally, the metadata collected and stored by social network providers like Facebook includes the IP address or mobile device identifier from which a post originated.[135] Taken together, this information provides circumstantial evidence of authenticity.[136]

Of course, metadata is not the only method of authenticating social media evidence.[137] Other distinct characteristics of the content such as the vernacular used or inside information known only to the purported author can also be used as circumstantial evidence of authorship.[138] Authentication can also be achieved via Rule 901(b)(1)[139] by testimony of the purported author, testimony of a witness that saw the purported author publish the post, or testimony from a witness that often communicated with the author via the account connected with the post.[140] Expert testimony could be used to describe the security features of a particular social networking site, or if available, the results of a search of the account holder's computer hard drive.[141]

Additionally, if somehow authorship is not at issue, authentication can be accomplished under Rule 901(b)(9), which allows evidence describing a system or process producing reliable results.[142] The "Wayback Machine," a service developed by an organization called the Internet Archive, provides litigants with screenshots of web content as it appeared on a particular date and time.[143] Traditionally, courts have required a witness from the Internet Archive to testify as

134. *See* Hoffman, *supra* note 34; John Patzakis, *Key Twitter Metadata Fields Lawyers and eDiscovery Professionals Need to be Aware of*, X1 DISCOVERY: EDISCOVERY LAW & TECH BLOG (Oct. 6, 2011), https://blog.x1discovery.com/2011/10/06/key-twitter-metadata-fields-lawyers-and-ediscovery-professionals-need-to-be-aware-of/; Patrick Ciapciak, *Selfies in Court: Snapchat As Admissible Evidence*, 2017 B.C. INTELL. PROP. & TECH. F., Feb. 7, 2017, at 1, 3–4, https://bciptf.org/2017/02/selfies-in-court-snapchat-as-admissible-evidence/. "[G]eofilters let mobile users add a location illustration—specific to where they are by city, neighborhood, or even store—to photos that they may then share with friends or followers via Snapchat." Lauryn Chamberlain, *GeoMarketing 101: What Are Geofilters?*, GEOMARKETING (Mar. 2, 2016, 2:28 PM), https://geomarketing.com/geomarketing-101-what-are-geofilters.

135. *See supra* note 38 and accompanying text.

136. *See infra* text accompanying notes 247–267.

137. *See* Grimm 2017, *supra* note 12, at 32 (containing a more exhaustive list); *see also* Grimm 2013, *supra* note 8, at 469.

138. *See* Grimm 2017, *supra* note 12, at 32; *see also* Grimm 2013, *supra* note 8, at 469.

139. Fed. R. Evid. 901(b)(1); Ill. R. Evid. 901(b)(1).

140. Grimm 2017, *supra* note 12, at 32.

141. Grimm 2017, *supra* note 12, at 32.

142. Fed. R. Evid. 901(b)(9); Ill. R. Evid. 901(b)(9); Grimm 2013, *supra* note 8, at 470.

143. *See About the Internet Archive,* INTERNET ARCHIVE WAYBACK MACHINE, https://archive.org/web/ (last visited Mar. 16, 2018); Specht v. Google Inc., 758 F. Supp. 2d 570, 580 (N.D. Ill. 2010), *aff'd*, 747 F.3d 929 (7th Cir. 2014).

to the accuracy of the process used to retrieve the screenshot.[144] But some courts have gone so far as to take judicial notice of the reliability of the Wayback Machine.[145] The utility of the Wayback Machine is particularly relevant due to the fleeting nature of social media content.[146] In particular, one of the defining features of Snapchat, a mobile application that shares photographs and videos, is the automatic deletion of "snaps."[147] However, at least one digital forensic company is capable of retrieving snaps that have already been deleted.[148] But authenticity may still be an issue if the accuracy of the retrieved copy cannot be verified.[149] Snapchat users may also take screenshots to save snaps, and these images are easily edited and reproduced.[150]

Copies of ESI such as retrieved snaps have also been subject to authenticity challenges. Here too, metadata, in the form of hash values, provides a distinguishing characteristic that can be used to establish the accuracy of a copy.[151] Running a hash algorithm against the contents of a file will generate a unique numerical value, known as a hash value.[152] Hash values are so distinctive that it is mathematically certain that no two files will have the same hash signature unless their content is identical.[153] Just as a Bates stamp functions as a method of providing each paper document with a unique identification number, hash values are inserted into a file to function as an electronic Bates stamp.[154] Even the slightest change to the content—something as insignificant as removing a space—will alter the hash signature.[155] Verifying authenticity using hash values has usually required expert testimony.[156] However, as of December 1, 2017, certified copies of ESI are self-authenticating under the new federal rules.[157]

---

144. Grimm 2017, *supra* note 12, at 27 n.80 (2017); *see, e.g., Specht*, 758 F. Supp. 2d at 580.

145. Grimm 2017, *supra* note 12, at 37 n.131; Panel Discussion, *supra* note 126, at 1189.

146. Forensic Focus, *supra* note 127.

147. "Snaps" are photographs or videos captured and shared via the application. Ciapciak, *supra* note 134, at 1.

148. *Id.* at 6.

149. *Id.*

150. *Id.*

151. Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 546 (D. Md. 2007).

152. Hannon, *supra* note 47, at 318.

153. *Id.* The odds that two distinct data sets will have the same hash signature is less than one in a billion. Zachary Rosenberg, *Returning to Plato's Cave: Metadata's Shadows in the Courtroom*, 48 Ariz. St. L.J. 439, 452 (2016).

154. *Lorraine*, 241 F.R.D. at 546–547.

155. Rosenberg, *supra* note 153, at 452. Depending on the type, a change in the metadata will also affect the hash value. Rosenberg, *supra* note 153, at 452.

156. Panel Discussion, *supra* note 126, at 1197.

157. Fed. R. Evid. 902(14).

2. The New Federal Rules

The 2017 amendment to the Federal Rules of Evidence included two new subdivisions to the list of evidence that is self-authenticating under Rule 902.[158] Rule 902 now provides:

> The following items of evidence are self-authenticating; they require no extrinsic evidence of authenticity in order to be admitted:
>
> . . .
>
> (13) *Certified Records Generated by an Electronic Process or System.* A record generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent must also meet the notice requirements of Rule 902(11).
> (14) *Certified Data Copied from an Electronic Device, Storage Medium, or File.* Data copied from an electronic device, storage medium, or file, if authenticated by a process of digital identification, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent also must meet the notice requirements of Rule 902(11).[159]

These new rules were established to streamline the authentication of certain kinds of digital evidence that would likely be authenticated by witness testimony under 901(b)(1) anyway.[160] The Advisory Committee on Evidence (Advisory Committee) recognized that the authenticity of machine-generated information and copies of electronic files are rarely the subjects of a legitimate dispute, and the Advisory Committee sought to avoid the expense and inconvenience associated with calling an authentication witness.[161] Instead of testifying live, a custodian could attest to the accuracy of the record by signing a certificate; this process is known as certification. By allowing authentication via certification, the parties are forced to confront questions of authenticity before trial rather than scrambling to line up a witness that becomes unnecessary once the opposing party stipulates to authenticity at trial.[162] The certification process shifts the burden of going forward (not the burden of proof) on authenticity questions to the opponent of

158. Fed. R. Evid. 902(13); Fed. R. Evid. 902(14).

159. Fed R. Evid. 902.

160. Advisory Committee on Evidence Rules, Reporter's Memorandum on Possible Amendments to Rule 902 for Authenticating Machine-Generated Data and Electronic Information Through Hash Value to Advisory Committee on Evidence Rules, at 210–16 (Oct. 24, 2014) [hereinafter Reporter's Memorandum], http://www.uscourts.gov/sites/default/files/fr_import/EV2014-10.pdf.

161. *Id.*

162. Fed. R. Evid. 902 advisory committee's note to the 2017 amendment.

the evidence, who is given fair notice and opportunity to challenge the certificate and the underlying record.[163]

It is important to note that these new rules do not change the standards for authenticating ESI, only the manner by which a proponent may establish their authenticity.[164] The certificate is only a substitute for live testimony and must contain information sufficient for authentication as if that information was provided by a witness at trial.[165] Furthermore, the certificate is only a means of satisfying the requirements of authentication, and the opponent is free to challenge its admissibility on other grounds—it does not automatically meet the requirements of the Rule 803(6) hearsay exception.[166] To illustrate, Rule 902(13) would provide for the authentication of a webpage collected by the Wayback Machine via a certificate attesting to the accuracy of the process used to retrieve it.[167] It would not prove that the defendant was the author of the statement contained therein.[168] Therefore, while these new rules certainly streamline the process of authenticating certain digital evidence, they do not ultimately resolve one of the central issues concerning social media evidence—proving authorship.

3. Authentication as a Business Record & Illinois Rules for Computer-Generated Data

The Illinois Rules of Evidence provide that records kept in the course of a regularly conducted business activity may be considered self-authenticating when they comply with the requirements of Rules 803(6) and 902(11).[169] However, Illinois imposes additional common-law requirements for computer-generated records beyond the requirements of the business record exception:[170]

> [A] proper foundation additionally requires a showing that standard equipment was used; the particular computer generates accurate records when used appropriately; the computer was used appropriately; and the sources of information, the method of recording uti-

163. Reporter's Memorandum, *supra* note 160, at 211.

164. Grimm 2017, *supra* note 12, at 40.

165. Fed. R. Evid. 902 advisory committee's note to the 2017 amendment.

166. *Id.*

167. Reporter's Memorandum, *supra* note 160, at 210–11.

168. Fed. R. Evid. 902 advisory committee's note to the 2017 amendment.

169. Ill. R. Evid. Rule 803(6); Ill. R. Evid. Rule 902(11); *See also* People v. Maya, 88 N.E.3d 10, 30–31 (Ill. App. Ct. 2017).

170. People v. Nixon, 36 N.E.3d 349, 369 (Ill. App. Ct. 2015).

> lized, and the time of preparation indicate that the record is trustworthy and should be admitted into evidence.[171]

Satisfying these requirements can be accomplished by a witness with knowledge.[172] Whether or not such testimony must occur live is undetermined.[173] In criminal cases, the witnesses have testified live, but in a civil case the court found that an affidavit submitted with the summary judgment motion satisfied the requirements.[174]

4. The Importance of Conditional Relevance under Rule 104(b)

While *Maya* provides the means to authenticate metadata as a business record under Rule 902(11), whether such a record is enough to support a prima facie case of authorship is still an open question.[175] There is a debate over whether authorship must be determined prior to admission or whether questions of authorship are properly determined by the fact-finder.[176] Unfortunately, it is unclear where Illinois law falls on the issue.[177] Further discussion on the relationship between Rule 104 and the rules on authentication is necessary.[178]

Rule 104(a) provides that "[p]reliminary questions concerning . . . the admissibility of evidence shall be determined by the court" and thus imposes on a judge the gatekeeping function of determining what evidence should be presented to the jury.[179] Authenticity is one relevant consideration.[180] But determining the authenticity of social media evidence might depend on a question of fact, specifically, who authored the post in question.[181] Such questions of fact are appropriately submitted to the jury, otherwise "the functioning of the jury as a trier of fact would be greatly restricted and in some cases virtually

171. *Id.* (quoting People v. Universal Pub. Transp., Inc., 974 N.E.2d 251, 262 (Ill. App. Ct. 2012)).

172. *See* People v. Lopez, No. 1-15-0167, 2016 WL 3202022 at *3 (Ill. App. Ct. 2016); *see also Nixon*, 36 N.E.3d at 369; People v. Morrow, 628 N.E.2d 550, 555 (Ill. App. Ct. 1993).

173. *See infra* Part IV.C and its discussion of whether business and computer-generated records may be admitted with a certificate of authenticity without violating a criminal defendant's Sixth Amendment right to confrontation.

174. *Compare Lopez*, 2016 WL 3202022 at *3 *and Morrow*, 628 N.E.2d at 555, *with* US Bank, Nat'l Ass'n v. Avdic, 10 N.E.3d 339, 349–50 (Ill. App. Ct. 2014).

175. The defendant in *Maya* challenged the Facebook records as inadmissible hearsay rather than denying authorship of the messages in question. People v. Maya, 88 N.E.3d 10, 30–31 (Ill. App. Ct. 2017).

176. Robbins, *supra* note 7, at 20.

177. *See infra* text accompanying notes 186–88.

178. Grimm 2017, *supra* note 12, at 5. It should be noted that Judge Grimm discusses the Federal Rules of Evidence, rather than the Illinois Rules of Evidence. *Compare* Fed. R. Evid. 104 *with* Ill. R. Evid. 104.

179. Fed. R. Evid. 104(a); Ill. R. Evid. 104(a); Panel Discussion, *supra* note 126, at 1175.

180. Panel Discussion, *supra* note 126, at 1175.

181. Grimm 2017, *supra* note 12, at 6.

destroyed."[182] Because the jury, as fact-finder, must first determine whether the evidence is authentic before it becomes relevant, the evidence is said to be "conditionally relevant." Rule 104(b) provides for situations where the relevance of evidence depends on the fulfillment of a condition, or in other words, it depends on the establishment of a fact.[183]

Under Illinois law "the court shall admit it upon, or subject to, the introduction of evidence sufficient to support a finding of the fulfillment of the condition."[184] Although the language is mandatory, as compared to Federal Rule 104(b),[185] the Illinois Rule leaves room for discretion as to whether the evidence shall be admitted *upon* production of proof, or whether the proposed evidence is admitted *subject to* the condition that proof will be presented to the jury at trial.[186] The difference is significant considering that when a judge admits evidence subject to condition, there is a possibility that sufficient proof of authenticity will never be presented at trial, and then, as the saying goes, the bell cannot be unrung.[187] When Illinois Rule 104 is applied to *People v. Kent*, it is unclear whether the error occurred when the trial court preliminarily determined that the Facebook post would be admitted subject to the condition that Facebook records would be presented to the jury.[188] Or the error may have occurred at trial, where the defense's objection to an inadequate foundation should have been sustained because the State failed to produce the promised Facebook records.[189] It is unclear from the appellate court's decision when exactly the error occurred.[190] Regardless, the result is the same.

So why does it matter? Suppose that the State had produced records showing that the post originated from the defendant's girlfriend's IP address.[191] The defense objects on the basis that anyone with access to her computer could have authored the post because the

182. Fed. R. Evid. 104(b) advisory committee's note to the 1972 amendment. *Contra* Robbins, *supra* note 7, at 20 ("Leaving the fact-finder, often a jury, to consider potentially untrustworthy evidence is precisely what the court's role as gatekeeper is designed to prevent.").

183. Ill. R. Evid. 104(b). For instance, the relevance of the Facebook post in *Kent*, turned on whether the prosecution could show that it was attributable to the defendant. People v. Kent, 81 N.E.3d 578, 591 (Ill. App. Ct. 2017).

184. Ill. R. Evid. 104(b).

185. Federal Rule of Evidence 104(b) provides that "the court *may* admit the proposed evidence on the condition that the proof be introduced later." Fed. R. Evid. 104(b) (emphasis added).

186. Ill. R. Evid. 104(b).

187. *See, e.g.*, *Kent*, 81 N.E.3d at 591.

188. *Id.* at 595.

189. *Id.*

190. *Id.*

191. *See Id.*

defendant never logs out of his account.[192] In this scenario, the trial judge could have admitted the Facebook post without error under Rule 104(a).[193] Contrary to the heightened standard required under the Maryland approach,[194] Rule 104 does not require the proponent to prove a negative—that no one but the defendant could have authored the Facebook post.[195] Instead, the burden is the same low threshold imposed by Rule 901(a), requiring only "evidence sufficient to support a finding that the matter in question is what its proponent claims."[196] As a distinctive characteristic, metadata offers strong circumstantial evidence satisfying the requirements of Rule 901(b)(4),[197] and the defense's alternate theory of authorship could be argued against the reliability of the evidence.[198]

But consider another hypothetical, where the defendant introduces contradictory evidence to refute authorship of the post in question.[199] This scenario implicates Rule 104(b), where the relevance of the Facebook post is dependent on whether the defense's version of the facts is enough to dissuade the jury that the defendant authored the post.[200] Opponents argue that conditionally admitting social media evidence under Rule 104(b) will punt all reliability concerns with social media to the fact-finder, thereby effectively shirking the judge's gatekeeper role.[201] However, before allowing the jury to consider the potentially admissible evidence, the judge must still make a threshold determination that a reasonable jury could find the evidence authentic.[202] Furthermore, this criticism confuses the distinction between admissibility and determining what weight to assign to the evidence.[203] With the proper instruction, the jury would be weighing the competing evidence of authorship to determine admissibility, rather than the weight of the evidence itself.[204] Notes from the Advisory Committee

192. *See* Grimm 2017, *supra* note 12, at 7 (discussing a similar hypothetical).

193. *See Kent*, 81 N.E.3d at 595 (indicating that evidence linking the post to the girlfriend's IP address would have provided circumstantial evidence of authenticity); *see also* Grimm 2017, *supra* note 12, at 8 (discussing a similar hypothetical).

194. *See supra* text accompanying notes 66–67.

195. *See* Grimm 2017, *supra* note 12, at 8. Judge Grimm and company argue that social media evidence would never be authenticated "if 'it might have been hacked' or 'it might have been photoshopped' were enough to preclude authentication." Grimm 2017, *supra* note 12, at 8.

196. Ill. R. Evid. 901(a).

197. *See supra* text accompanying notes 132–36.

198. *See* Grimm 2017, *supra* note 12, at 8.

199. *See* Grimm 2017, *supra* note 12, at 9.

200. *See* Grimm 2017, *supra* note 12, at 9.

201. Robbins, *supra* note 7, at 20.

202. Panel Discussion, *supra* note 126, at 1176.

203. Panel Discussion, *supra* note 126, at 1178.

204. Panel Discussion, *supra* note 126, at 1176; *see also* Grimm 2017, *supra* note 12, at 9–10.

also suggest that a judge may withdraw evidence from the jury's consideration if the proponent ultimately fails to meet the 901(a) threshold.[205]

Thus, social media evidence is admissible under the Federal Rules of Evidence without requiring the proponent to prove a negative, and competing evidence does not prevent it from reaching the jury.[206] Yet, the ambiguity created by the language of Illinois Rule of Evidence 104(b), and left unresolved by *Kent*, leaves Illinois practitioners with something to be desired: a best practice for admitting social media evidence.[207]

III. Analysis

As the preceding discussion on the rules of authentication demonstrates, there are several ways to authenticate social media evidence.[208] So what makes using metadata the best practice? Each of the landmark cases—*Lorraine*, *Griffin*, *Tienda*, and *Kent*—advocate for the use of metadata as a means of authentication.[209] Therefore, regardless of the standard applied, using metadata is a viable and successful method. Furthermore, metadata effectively counters the standard objections to social media evidence. The first part of the analysis focuses on the ways in which metadata can be used to prove the evidence presented is an accurate representation of the social media content and to prove who authored the content in question. The argument proceeds to examine Illinois jurisprudence specifically, distilling the guidance Illinois appellate courts have provided.

However, by advocating the use of metadata as a best practice for authentication, this Comment is not suggesting it as the rule. In some circumstances, social media communications might be more readily authenticated by a witness with knowledge, perhaps by the author herself.[210] But that is not always the case, especially when the purported author is a criminal defendant and will likely invoke her Fifth Amendment right against self-incrimination.[211] This Comment aims to address circumstances where other methods of authentication are ei-

205. Fed. R. Evid. 104(b) advisory committee's note to the 1972 amendment.

206. Grimm 2017, *supra* note 12, at 10–11.

207. *See supra* text accompanying notes 186–89.

208. *See* discussion *supra* Part II.D.

209. Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 548 (D. Md. 2007); Griffin v. State, 19 A.3d 415, 428 (Md. 2011); Tienda v. State, 358 S.W.3d 633, 647 (Tex. Crim. App. 2012); People v. Kent, 81 N.E.3d 578, 598 (Ill. App. Ct. 2017).

210. *See, e.g.*, People v. Nunn, No. 3–14–0137, 2016 WL 2866361 at *18 (Ill. App. Ct. May 16, 2016).

211. John G. Browning, *Introducing Social Media Evidence,* 74 Advocate 110, 111 (2016).

ther unavailable or ineffective. Under such circumstances, metadata can provide the means to foreclose otherwise indefensible claims that the social media profile is fake, hacked, or that the specific communication was posted by someone other than the page's owner.

A. Metadata Effectively Addresses Common Authenticity Challenges

Social media evidence is inherently vulnerable to authenticity challenges due to the dynamic and anonymous nature of internet-based communications.[212] Unlike letters or other hardcopy documents, ESI is ephemeral and vulnerable to inadvertent alteration.[213] Social media content is considered especially suspect because of the ease with which an account can be fraudulently created, hacked, or accessed by a third-party.[214] As a result, the two central questions in authenticating social media evidence are: (1) whether the proffered exhibit accurately represents what appeared on the internet at a given time; and (2) whether the communication can be properly attributed to the alleged declarant.[215] Metadata effectively addresses both of these concerns.[216]

1. Proving Accuracy

A social media page may appear quite different from one day to the next depending on the owner's desire to update or delete its contents.[217] The ephemeral nature of social media urges litigants to capture a screenshot[218] in order to generate a static record of its contents at a certain date and time.[219] But because a screenshot is merely an image representing the social media page,[220] the proponent has the added challenge of demonstrating that the screenshot accurately de-

212. Democko, *supra* note 4, at 381–82.

213. Kling et al., *supra* note 39, at 40.

214. Keefe, *supra* note 6, at 1047; *see also* Elizabeth A. Flanagan, #*guilty?* Sublet v. State *and the Authentication of Social Media Evidence in Criminal Proceedings*, 61 VILL. L. REV. 287, 301 (2016) ("Social media evidence presents two separate concerns regarding authentication: first, anyone can make a profile under a fictitious name, and second, a person can access another's profile simply by attaining the profile's username and password.").

215. Democko, *supra* note 4, at 381–82; Steven Goode, *The Admissibility of Electronic Evidence*, 29 REV. LITIG. 1, 16–17 (2009); Merritt, *supra* note 4, at 52.

216. Rosenberg, *supra* note 153, at 456.

217. Browning, *supra* note 211, at 116.

218. A screenshot is analogous to a photograph in that it depicts what was displayed on a particular electronic device at a given point in time. Merritt, *supra* note 4, at 52.

219. *Effective Claims Practices: Overcoming Hurdles to the Use of Social Media*, HEYL, ROYSTER, VOELKER & ALLEN (May 22, 2013) [hereinafter *Effective Claims Practices*], www.heylroyster.com/_data/files/Seminar%202013/B%20-%20SKH%20-%20V6%20-%20Final.pdf.

220. Merritt, *supra* note 4, at 52.

picts the page at the time it was captured.[221] This requires "factual specificity about the process by which the electronically stored information is created, acquired, maintained, and preserved without alteration or change, or the process by which it is produced if the result of a system or process that does so."[222] Factual specificity about the steps taken to collect and preserve the screenshot can be achieved through an affidavit or a witness attestation, but metadata offers a more reliable method of authentication.[223] Metadata provides contextual information as to the origins of a document, such as the date and time of its creation.[224] Rather than rely on a witness whose recollection or credibility may be called into doubt, metadata can definitively establish the date and time a screenshot was captured.[225]

This is not to say that metadata is immune to manipulation.[226] Even absent bad faith, metadata is highly susceptible to inadvertent alteration.[227] For instance, the last-accessed or last-modified timestamps might be automatically updated each time a file is opened for viewing.[228] But with the use of special software, digital forensic experts can access and preserve a file without affecting the metadata and are often able to detect when metadata has been fabricated.[229] Metadata is also quite easily stripped or "scrubbed" from a document.[230] Simply converting the document to a PDF version will typically remove metadata from the file.[231] Likewise, printed hard copies do not include metadata useful for authentication.[232] For this reason, printouts of social media pages are likely insufficient to authenticate the content pictured therein.[233]

---

221. Finkel, *supra* note 89, at 278; Rosenberg, *supra* note 153, at 457.

222. Rosenberg, *supra* note 153, at 458 (quoting Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 545 (D. Md. 2007)).

223. Rosenberg, *supra* note 153, at 456; *see also* Bibart, *supra* note 29, at 793 (discussing metadata's value in overcoming false testimony).

224. Rosenberg, *supra* note 153, at 457.

225. Rosenberg, *supra* note 153, at 457. Metadata is especially preferable to witness testimony when the individual who captured the screenshot was the attorney rather than a disinterested third-party. *See Effective Claims Practices*, *supra* note 219 ("Attorneys cannot call themselves to the stand to testify about how they gathered this information.").

226. Rosenberg, *supra* note 153, at 451.

227. Rosenberg, *supra* note 153, at 451.

228. *See* Rosenberg, *supra* note 153, at 451.

229. Rosenberg, *supra* note 153, at 451; Bibart, *supra* note 29, at 794.

230. *See* Rosenberg, *supra* note 153, at 452. "Scrubbing" a document, or redacting the invisible data, is typically done to protect privileged information. *See* Rosenberg, *supra* note 153, at 452.

231. *See* Rosenberg, *supra* note 153, at 452.

232. Finkel, *supra* note 89, at 278.

233. Finkel, *supra* note 89, at 278.

However, because metadata is highly volatile by nature, it inherently provides a record of if and when an electronic document has been modified.[234] Knowing whether a file has been modified can be important to prove or disprove tampering.[235] Screenshots are particularly vulnerable to such attacks due to the many ways in which technology enables users to alter digital images.[236] Some courts have ruled that absent specific proof, allegations of tampering only go to the weight of the evidence rather than its authenticity.[237] Even so, challenges to the integrity of the chain of custody are defensible using a specific type of metadata known as a hash value.[238] Hash values are akin to fingerprints in that they uniquely identify a computer file.[239] Because hash values are mathematically generated, a file's hash signature will be the same each time the algorithm is applied.[240] Therefore, hash values can be used to verify the accuracy of a copy when compared to the original file.[241]

The Advisory Committee specifically contemplated the mathematical reliability of hash values when it crafted the new Federal Rules of Evidence.[242] Observing that forensic examiners must work with a copy to preserve and avoid contaminating the original,[243] Rule 902(14) provides that these copies can be admitted as self-authenticating via certification of identical hash values.[244] By recognizing hash values as the

234. Hannon, *supra* note 47, at 318–19. System metadata consists of timestamps of when the file was "modified, accessed, and created," otherwise known as "MAC" data. Hannon, *supra* note 47, at 318–19. Because this type of metadata records the changes made to a file, it can be useful in proving attribution and accuracy. Hannon, *supra* note 47, at 318–19.

235. Hannon, *supra* note 47, at 317.

236. Goode, *supra* note 215, at 19–20.

237. Hansen & Pratt, *supra* note 43, at 13 (collecting federal case law); Hannon, *supra* note 47, at 318 (relying on Missouri and Ohio appellate decisions).

238. Hannon, *supra* note 47, at 318.

239. Rosenberg, *supra* note 153, at 452. Similarly, hash values have been compared to DNA. Hannon, *supra* note 47, at 318.

240. Rosenberg, *supra* note 153, at 452.

241. Rosenberg, *supra* note 153, at 452. The utility of hash values is somewhat limited when applied to data stored on mobile devices. Hannon, *supra* note 47, at 320. Because such devices are constantly powered on and continuously update, even back-to-back downloads will acquire slightly different content and thus, distinct hash values. Hannon, *supra* note 47, at 320 (quoting Nat'l Inst. of Standards & Tech., U.S. Dep't of Commerce, NIST Special Pub. 800-101, Guidelines on Mobile Device Forensics, at 26 (May 2014), http://dx.doi.org/10.6028/NIST.SP.800-101r1). But while hash values cannot be used to verify the entire data set, hash values generally remain consistent for individual files. Hannon, *supra* note 47, at 320.

242. Fed. R. Evid. 902 advisory committee's note to the 2017 amendment; Reporter's Memorandum, *supra* note 160, at 213.

243. Reporter's Memorandum, *supra* note 160, at 213.

244. Fed. R. Evid. 902 advisory committee's note to the 2017 amendment.

industry standard in authenticating copies,[245] the new rules should assist in proliferating the use of metadata in authentication generally.

2. *Proving Attribution*

Not only can metadata offer conclusive proof that the proffered exhibit is an accurate representation, but it can also be convincing circumstantial evidence of authorship.[246] The identity of the alleged declarant is the most frequently contested authentication issue when introducing social media evidence.[247] Not surprisingly, proving attribution can be a significant hurdle given the proliferation of fake profiles and the ease with which legitimate profiles can be accessed by third parties.[248] As a result, proponents of social media evidence must overcome challenges based on two general theories: first, that the account is fraudulent; or second, that someone besides the alleged author had access to the account.[249] While other methods of authentication might be used in rebuttal, metadata can be especially convincing in undermining the credibility of such claims.[250]

First, the contextual information gleaned from metadata can go a long way to eliminate the possibility that it is a fake account.[251] While basic biographical information and photographs containing the likeness of the purported author are insufficient to disprove fabrication,[252] information contained in metadata can provide the link between the profile and its alleged owner.[253] Although social networking sites do not verify owner identity, a subpoena would at least reveal the email address used to register the account.[254] And even when proxy servers, virtual private networks (VPNs), or onion routing is used to conceal the IP address from which a specific post originated,[255] some social

245. *Id.*; Reporter's Memorandum, *supra* note 160, at 213.

246. *See* Hansen & Pratt, *supra* note 43, at 3.

247. Democko, *supra* note 4, at 382.

248. Flanagan, *supra* note 214, at 301–02.

249. Flanagan, *supra* note 214, at 302; Democko, *supra* note 4, at 382.

250. Hansen & Pratt, *supra* note 43, at 3.

251. Michael D. Dean, *Authenticating Social Media in Evidentiary Proceedings*, 28 CRIM. JUST., Winter 2014, at 49, 50.

252. Grimm 2017, *supra* note 12, at 31.

253. Dean, *supra* note 251, at 64.

254. Dean, supra note 251, at 50, 64; Robbins, *supra* note 7, at 33.

255. Proxy servers act as an intermediary, forwarding a communication from the generating computer to the recipient such that the return IP address listed is that of the proxy server rather than the author. JAMES GRIMMELMANN, INTERNET LAW: CASES AND PROBLEMS 255 (8th ed. 2018). In a virtual private network (VPN) the traffic is encrypted on its way to the proxy. *Id.* Onion routing is most secure in that it "separately encrypt[s] each layer of communication: each proxy except the last knows only that it is somewhere in the middle of a chain, and has no idea of the contents of a message." *Id.* But despite their ability to conceal the message's originating IP

media providers also record the device identifiers of devices used to access the account.[256] By showing that the email address attached to the account is the same utilized by the alleged owner, the proponent of the evidence successfully forecloses a claim that the account is fake.[257] More conclusively, by demonstrating that the alleged account holder owns the devices used to access the account, it becomes exceedingly unlikely that this same person does not also own the profile in question.[258]

Second, metadata can provide circumstantial evidence that the alleged declarant had control over the account during the time in question.[259] The prevalence of hacking[260] means that it is not enough to demonstrate that the alleged declarant owns the account in question.[261] Furthermore, many users remained logged in on their devices, which means anyone could access the account simply by using an account holder's unguarded phone or computer.[262] But by using metadata to flag the associated devices and routine IP addresses, remote access by a malicious hacker would be easy to detect.[263] Theories based on surreptitious access via the account holder's own devices are not as easily defensible; still metadata can provide sufficient contextual information to test the veracity of such a claim.[264]

For example, knowing the timestamp and GPS location at which a social media post originated allows the proponent to establish control by implication—thus limiting the number of potential authors to those present at that specific time and place.[265] Armed with this information, the lawyer might use it to undermine the alleged declarant's alibi, obtain an admission at a deposition, or negotiate a stipulation ahead of trial. If nothing else, the number of witnesses needed to dispel fears

---

address, proxy servers and onion routing do not "guarantee anonymity" as IP addresses are not the only means of identification online. *Id.*

256. *Data Policy*, *supra* note 19.

257. Robbins, *supra* note 7, at 34.

258. *See* Dean, *supra* note 251, at 64.

259. Dean, *supra* note 251, at 64.

260. Robbins, *supra* note 7, at 11 ("[P]ervasive posting of personal information on social-networking sites has facilitated identity theft because hackers can obtain this information and use it for their own gain.").

261. Flanagan, *supra* note 214, at 301–03.

262. Flanagan, *supra* note 214, at 301–03.

263. Megan Uncel, *"Facebook Is Now Friends with the Court": Current Federal Rules and Social Media Evidence*, 52 JURIMETRICS 43, 62 (2011). Even without consulting the metadata, it is unlikely that the account holder would fail to notice their account had been hacked. *Id.*

264. Dean, *supra* note 251, at 64; Hansen & Pratt, *supra* note 43, at 3.

265. Dean, *supra* note 251, at 64.

of fabrication is significantly reduced.[266] In short, when authorship hinges on establishing who had control over the account in question, location metadata may prove indispensable.[267]

Therefore, metadata can provide valuable circumstantial evidence in establishing who authored a social media communication. Likewise, metadata's utility in verifying that the evidence accurately represents the online content on a particular date cannot be questioned. Having demonstrated how metadata supports these prerequisites to authentication, this Comment turns to address this method's application under Illinois law.

B. Best Practices for Authenticating Social Media Evidence in Illinois

A survey of the few Illinois cases addressing the admission of social media evidence demonstrates a general inclination to admit social media evidence.[268] Overall, the more lenient Texas standard has been gaining widespread acceptance.[269] The *Kent* court cites *Tienda* with approval, seeming to suggest that Illinois jurisprudence will follow a less rigorous approach.[270] However, the court's reasoning demonstrates its hesitance to trust social media evidence.[271] It interprets *Tienda* as requiring "something more" than a name and photograph to authenticate social media evidence, but expressly declines to elabo-

---

266. Dean, *supra* note 251, at 64 (offering Campbell v. State, 382 S.W.3d 545, 552 (Tex. Crim. App. 2012) as an illustration).

267. Whether location information can be obtained is a separate and more complicated question. *See infra* Part IV.A.

268. *See* People v. Maya, 88 N.E.3d 10, 31 (Ill. App. Ct. 2017) (affirming that Facebook messages were properly admitted as a business record via a certificate of authenticity provided by a Facebook records custodian); People v. Nunn, No. 3–14–0137, 2016 WL 2866361 at *8 (Ill. App. Ct. May 16, 2016) (finding reversible error where the trial court excluded a printout of Facebook messages despite finding that it could be authenticated); *In re* Marriage of Miller, 40 N.E.3d 206, 219–20 (Ill. App. Ct. 2015) (finding that directing the witness to the time and origins of Facebook status posts laid an adequate foundation for impeachment evidence); People v. Macias, 36 N.E.3d 373, 399 (Ill. App. Ct. 2015) (deferring to trial court's discretion in admitting pictures from a MySpace profile based on testimony from a witness with knowledge); People v. Flores, 21 N.E.3d 1227, 1243 (Ill. App. Ct. 2014) (deferring to trial court's discretion in admitting pictures from a MySpace profile based on testimony from a witness with knowledge); Stapp v. Jansen, 988 N.E.2d 234, 238 (Ill. App. Ct. 2013) (admitting printouts of messages received via online dating applications). *But cf.* People v. Kent, 81 N.E.3d 578, 587–98 (Ill. App. Ct. 2017) (affirming that defendant's likeness and alias were not sufficient to authenticate a Facebook post).

269. *See* section titled "Texas's Standard Gets the Most Likes" in Flanagan, *supra* note 214, at 295.

270. *Kent*, 81 N.E.3d at 598.

271. *Id.* at 597–98.

rate on what more would be sufficient.[272] The resulting uncertainty leaves Illinois practitioners guessing at what is required to introduce social media evidence.[273]

Recent Illinois appellate decisions, such as *Kent* and *Maya*, do provide some implicit guidance. In dicta, the *Kent* court hints that metadata would have provided sufficient circumstantial evidence to admit a Facebook post—at least enough to submit it to the jury to decide authorship.[274] The court observed that Facebook records revealing that the post originated from an IP address belonging to the defendant's girlfriend would have provided an adequate foundation to argue that the defendant authored the post.[275] While this observation holds no precedential value as dicta, it endorses metadata as a reliable method of authentication.

The reliability of Facebook records was subsequently acknowledged in *Maya*.[276] Although the defense challenged their admission as hearsay rather than on authentication grounds, the appellate court held that the trial court did not abuse its discretion in admitting Facebook records accompanied by a certificate of authenticity in compliance with Rule 902(11).[277] Rule 902(11) provides that business records kept in the course of regularly conducted activity are self-authenticating.[278] The certificate provided by Facebook indicated that the records were "made and kept by the automated systems of Facebook."[279]

As discussed previously, Illinois requires additional foundation requirements for computer-generated business records.[280] The proponent must make a secondary showing as to the standardization and accuracy of the process to indicate that the record is trustworthy and should be admitted into evidence.[281] The fact that Illinois has requirements beyond those provided in Rules 803(6) and 902(11) might suggest that computer-generated records are subject to increased scrutiny. The court in *Kent* reaffirmed these additional requirements in a separate part of its opinion when it considered the admissibility of phone records.[282]

---

272. *Id.* at 598–99.
273. Kling et al., *supra* note 39, at 41.
274. *Kent*, 81 N.E.3d at 595.
275. *Id.*
276. People v. Maya, 88 N.E.3d 10, 31 (Ill. App. Ct. 2017).
277. *Id.*
278. Ill. R. Evid. Rule 902(11).
279. *Maya*, 88 N.E.3d at 31.
280. *See* discussion *supra* Part II.D.3.
281. People v. Nixon, 36 N.E.3d 349, 369 (Ill. App. Ct. 2015).
282. People v. Kent, 81 N.E.3d 578, 600 (Ill. App. Ct. 2017) (citing *Nixon*, 36 N.E.3d at 369).

Curiously though, it is not readily apparent that the *Maya* court required the secondary showing to admit the Facebook records.[283] The discrepancy between *Kent* and *Maya* is somewhat troubling, but it may have no practical significance if Facebook's certifications are drafted to meet the additional requirements under Illinois law. There is precedent allowing a proponent to show standardization and accuracy of the records by affidavit.[284] The *Maya* court's willingness to admit Facebook records as self-authenticating is significant, as it would avoid the expense of providing an authentication witness.[285]

Finally, one other feature of Illinois jurisprudence in this area bears mentioning: Recognizing the value of social media evidence, Illinois appellate courts have found that errors in admitting, or failing to admit, social media evidence are not harmless but dispositive.[286] While social media is undoubtedly pertinent in civil litigation, it plays a significant role in criminal prosecutions where social media communications might be admissions or otherwise bear on intent, state of mind, or motive.[287] Perhaps the prosecution's burden of proof in criminal trials helps to explain the more rigorous standard applied in *Kent*, where the prosecution offered the evidence, versus the court's willingness to admit social media evidence in *Nunn*, where the defense offered the evidence.[288]

Knowing the stakes and considering the absence of a clear standard, attorneys "should err on the safe side and prepare to meet strict authentication requirements."[289] But regardless of whether Illinois sides with Maryland or Texas, both approaches and Illinois precedent contemplate metadata as a viable means of authentication. Authenticating using metadata is the best method to address concerns over the accuracy of social media evidence as a representation of dynamic on-

283. *See Maya*, 88 N.E.3d at 31.

284. *See* US Bank, Nat'l Ass'n v. Avdic, 10 N.E.3d 339, 349–50 (Ill. App. Ct. 2014) (admitting computer-generated records by affidavit attached to the motion for summary judgment). *But cf.* People v. Lopez, No. 1-15-0167, 2016 WL 3202022 at *3 (Ill. App. Ct. 2016) (admitting computer-generated records with the testimony of a witness with knowledge of the computer system); People v. Morrow, 628 N.E.2d 550, 555 (Ill. App. Ct. 1993) (admitting computer-generated records with the testimony of a witness with knowledge of the computer system).

285. Reporter's Memorandum, *supra* note 160, at 211 (seeking to accomplish the same end by enacting the new federal rules of evidence).

286. *See Kent*, 81 N.E.3d at 599 (holding that admitting the Facebook post was reversible error); People v. Nunn, No. 3–14–0137, 2016 WL 2866361 at *9 (Ill. App. Ct. May 16, 2016) (holding that excluding Facebook messages was not harmless error).

287. Grimm 2013, *supra* note 8, at 439.

288. *Compare Kent*, 81 N.E.3d at 599 (holding that admitting the Facebook post was reversible error) *with Nunn*, 2016 WL 2866361 at *9.

289. Kling et al., *supra* note 39, at 41.

line content and provides convincing circumstantial evidence to identify who authored the content.

IV. IMPACT

While the focus of this Comment is on the use of metadata to authenticate social media evidence, the argument presupposes that the metadata is discoverable. In order to advocate for the use of metadata as the primary means of authentication, this Comment must outline the risks and benefits associated with collecting metadata. This part aims to demonstrate that collecting metadata for use in authentication is not only viable but cost-effective. The first section explains the privacy considerations associated with obtaining metadata, including the Supreme Court's recent decision in *Carpenter v. United States*[290] and the controversy over the Stored Communications Act (SCA).[291] The second section engages in a cost-benefit analysis, highlighting a lawyer's duties under the discovery rules and professional standards. The analysis continues by observing metadata's utility in avoiding other evidentiary challenges. Finally, the third section addresses how self-authenticating electronic records fare under the Confrontation Clause.

A. Data Privacy Considerations

The revealing nature of metadata has been a subject of controversy ever since Edward Snowden blew the whistle on the National Security Agency's metadata surveillance program.[292] The amount of personal data collected by social media companies is of special concern ever since the Cambridge Analytica scandal revealed how easily a third party harvested data on Facebook subscribers during the 2016 presidential campaign.[293] Whether social media communications and the metadata collected by social media companies should be afforded protection under the Fourth Amendment's right to privacy continues to be the subject of lively debate.[294]

---

290. 138 S. Ct. 2206, 2211 (2018).

291. 18 U.S.C. § 2701 et seq. (2012). The SCA provides that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1) (2012).

292. *See* Heller, *supra* note 30.

293. Matthew Rosenberg, Nicholas Confessore, & Carole Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. TIMES (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

294. *See* Mallory Allen & Aaron Orheim, Comment, *Get Outta My Face(book): The Discoverability of Social Networking Data and the Passwords Needed to Access Them*, 8 WASH. J. L.

Confined to the challenges associated with authenticating social media evidence, this Comment takes no position with regard to whether a subscriber has a reasonable expectation of privacy in her metadata. But in contemplating whether using metadata is truly the best method of authentication, some attention must be given to whether all litigants—the Government and private parties of all means—can avail themselves of its advantages. Therefore, this section considers the recent developments in data privacy law, how social media companies respond to discovery requests, and whether the current rules disadvantage criminal defendants.

Undoubtedly, the most efficient way to obtain the content of a social media page would be to request it from the user.[295] But while formal discovery requests are the best practice in civil litigation, criminal defendants are not required to disclose their social media communications to the prosecution under the Illinois Supreme Court Rules.[296] Furthermore, under the "act of production doctrine" a criminal defendant is not required to comply with a grand-jury subpoena to produce his social media pages because such an act of production would compromise his Fifth Amendment privilege against self-incrimination.[297] Instead, both *Kent* and *Maya* specifically contemplate obtaining records directly from Facebook.[298] But whether this strategy is feasible in all circumstances is not immediately clear[299] and deserves discussion.

TECH. & ARTS 137 (2012); Monu Bedi, *Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply,* 54 B.C. L. REV. 1, 3 (2013); Andrew Gray, Comment, *"Cloud" Atlas-A Map to Amending Metadata Privacy Law in the Modern Era,* 52 GONZ. L. REV. 147, 161 (2017); Lisa A. Schmidt, Note, *Social Networking and the Fourth Amendment: Location Tracking on Facebook, Twitter, and Foursquare,* 22 CORNELL J. L. & PUB. POL'Y 515 (2013).

295. Finkel, *supra* note 89, at 278.

296. Ill. Sup. Ct. R. 413.

297. *See* United States v. Hubbell, 530 U.S. 27, 36–37 (2000) ("[W]e have also made it clear that the act of producing documents in response to a subpoena may have a compelled testimonial aspect."); *see also* Orin Kerr, *Does Carpenter Revolutionize the Law of Subpoenas?* REASON.COM: VOLOKH CONSPIRACY (June 26, 2018, 5:36 PM), https://reason.com/volokh/2018/06/26/does-carpenter-revolutionize-the-law-of ("The recipient can claim that complying with the subpoena implies certain statements – that the records exist, that the recipient has them, and that the recipient thinks that they are authentic – and that he can't be forced to testify against himself.").

298. People v. Kent, 81 N.E.3d 578, 595 (Ill. App. Ct. 2017); People v. Maya, 88 N.E.3d 10, 18 (Ill. App. Ct. 2017).

299. Whether or not Facebook with respond to a request or court order to produce records depends on what records are being sought and by whom. *Compare Information for Law Enforcement Authorities,* FACEBOOK, [hereinafter *Information for Law Enforcement Authorities*, FACEBOOK], https://www.facebook.com/safety/groups/law/guidelines/ (last visited Mar. 15, 2018) *and Law Enforcement & Third-Party Matters,* FACEBOOK HELP CTR., [hereinafter *Law Enforcement & Third-Party Matters*, FACEBOOK HELP CTR.], https://www.facebook.com/help/473784375984502 (last visited Mar. 15, 2018).

1. The Third-Party Doctrine After Carpenter v. United States

First, the Supreme Court's recent decision in *Carpenter v. United States* marked a significant shift in how the third-party doctrine is applied to ESI.[300] The third-party doctrine is premised on the idea that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[301] Prior to *Carpenter*, the third-party doctrine operated as a bright-line rule that eliminated any Fourth Amendment privacy rights in records stored by a third-party custodian.[302] As a result, the Government could obtain records pertaining to a criminal defendant without a warrant by simply serving a subpoena on the third-party custodian.[303]

Recently, however, the Supreme Court renounced the mechanical application of the third-party doctrine and declined to extend its application to cell site location information (CSLI).[304] In *Carpenter*, the Court recognized "the deeply revealing nature of CSLI" and found "the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection."[305] As a result, the Government can no longer obtain a subscriber's location information from his wireless provider with a subpoena but must ob-

---

300. *See* Orin Kerr, *First Thoughts on Carpenter v. United States*, REASON.COM: VOLOKH CONSPIRACY (June 22, 2018, 12:20 PM), https://reason.com/volokh/2018/06/22/first-thoughts-on-carpenter-v-united-sta. Even before *Carpenter*, jurists and scholars had begun to challenge the third-party doctrine's applicability in the digital age. *See, e.g.*, United States v. Jones, 565 U.S. 400, 417–18 (2012) (Sotomayor, J. *concurring*); Bedi, *supra* note 294, at 3.

Moreover, the continued operation of the third-party doctrine under U.S. law runs contrary to the many protections afforded by the General Data Protection Regulation (GDPR) of the European Union, so much so that the European Commission has adopted an EU-US Privacy Shield to protect the data privacy rights of EU citizens. European Commission Press Release IP/16/2461, European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows (July 12, 2016), http://europa.eu/rapid/press-release_IP-16-2461_en.htm.

301. Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018) (quoting Smith v. Maryland, 442 U.S. 735, 743–44 (1979)).

302. *First Thoughts on Carpenter v. United States*, *supra* note 301*; see also Carpenter*, 138 S. Ct. at 2255 (Alito, J., dissenting) ("[U]ntil today—defendants categorically had no 'reasonable expectation of privacy' and no property interest in records belonging to third parties."). *Contra* United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010) (holding that a subscriber had a reasonable expectation of privacy in the contents of remotely stored emails).

303. *See*, for example, the Stored Communications Act, 18 U.S.C. § 2703(d) (2012), allowing the government to access ESI stored by third-parties through compulsory process. Note that the standard for obtaining a subpoena is purposefully less stringent than the probable cause required to obtain a warrant. *See* Justice Alito's discussion of *Oklahoma Press Publishing Co. v. Walling*, 327 U.S. 186 (1946), in his dissent to *Carpenter*, 138 S. Ct. at 2254–58 (Alito, J. dissenting).

304. *Carpenter*, 138 S. Ct. at 2210 ("In mechanically applying the third-party doctrine to this case the Government fails to appreciate that there are no comparable limitations on the revealing nature of CSLI."). Cell site location information refers to the timestamped records created each time a cell phone connects to a nearby cell tower site. *See id.* at 2208.

305. *Id.* at 2223.

tain a warrant instead.[306] More broadly, this means that the third-party doctrine no longer operates as a categorical rule.[307]

Still, Chief Justice Roberts made clear that the *Carpenter* decision was a narrow one, which did not "address other business records that might incidentally reveal location information" such as a Facebook subscriber's IP address.[308] Moreover, the Court deliberately left some questions unanswered: "[W]e need not decide whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be."[309] Therefore, there may be room to distinguish *Carpenter* in instances where the historical location records span fewer than seven days.[310]

Another question is whether data beyond location information might fall within *Carpenter's* purview.[311] Likewise, it is unclear whether *Carpenter* applies consistently to all forms of location data—e.g., geotags[312] embedded in social media posts and photographs. Because CSLI is automatically collected without any affirmative action by the subscriber, the Court observed that one of the rationales underlying the third-party doctrine—voluntary disclosure—is no longer implicated.[313] Consequently, the third-party doctrine does not extend to CSLI.[314] Perhaps because geotagging is typically an automatic function, such data may be an exception from the third-party doctrine. On the other hand, posting or sharing a picture on social media *is* an affirmative action that shares location information with not just the social media provider, but with the public at large. At this point, however, *Carpenter* is limited to CSLI and does not proscribe the application of the third-party doctrine to all types of metadata.

2. The Stored Communications Act

Carpenter not only upset the traditional operation of the third-party doctrine but also effectively abrogated the SCA with respect to

306. *Id.* at 2221.

307. *See First Thoughts on Carpenter v. United States*, *supra* note 300.

308. 138 S. Ct. at 2220.

309. *Id.* at 2217 n.3.

310. *See First Thoughts on Carpenter v. United States*, *supra* note 300. The theory is that longer-term surveillance allows the government to gather enough bits of information to create a mosaic of the suspect's life in total. *First Thoughts on Carpenter v. United States*, *supra* note 301.

311. *First Thoughts on Carpenter v. United States*, *supra* note 301.

312. Geotags refer to the Exchangeable Image File Format (EXIF) data embedded in a digital photograph that describes the time, date, and GPS coordinates of the photo. *See* Redlitz, *supra* note 34.

313. *Carpenter*, 138 S. Ct. at 2210.

314. *Id.*

CSLI.[315] Generally, the SCA permits third-party custodians to disclose subscriber records to law enforcement officials in response to a subpoena.[316] This is significant considering the standard to obtain a subpoena is less stringent than the probable cause required for a warrant.[317] In *Carpenter*, the Court chipped away at the constitutionality of the SCA in ruling that "an order issued under Section 2703(d) of the [SCA] is not a permissible mechanism for accessing historical cell-site records."[318]

While Fourth Amendment challenges to the SCA are concerned with restricting government access to sensitive data without probable cause, the SCA was designed as a means to prevent misuse of ESI by private actors.[319] The SCA prohibits disclosure to private entities.[320] Social media providers have frequently invoked the SCA in refusing to turn over data and have developed their own policies against disclosure.[321]

But the scope of the SCA's protection only extends to content.[322] Content is defined under the statute to include "any information con-

315. *Id.* at 2221.

316. *See* 18 U.S.C. § 2703(d) (2012). A warrant is only required for records in storage for 180 days or less. 18 U.S.C. § 2703(a) (2012). Disclosure of records in storage longer than 180 days may be compelled by warrant, administrative subpoena, or court order under § 2703(d). 18 U.S.C. § 2701(a)–(b) (2012); United States v. Warshak, 631 F.3d 266, 283 (6th Cir. 2010).

317. *Carpenter*, 138 S. Ct. at 2221. Under § 2703(d), the government need only "'offer[ ] specific and articulable facts showing that there are reasonable grounds to believe' that the records sought 'are relevant and material to an ongoing criminal investigation.'" *Id.* at 2212 (quoting 18 U.S.C. § 2703(d)).

318. *Id.* at 2221. The Court's decision in *Carpenter* is not the only instance in which the SCA was ruled unconstitutional however. Similarly, in *United States v. Warshak*, the Sixth Circuit ruled that "to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional." 631 F.3d at 288. It likewise questioned whether "the mere *ability* of a third-party intermediary to access the contents of a communication can[ ] be sufficient to extinguish a reasonable expectation of privacy." *Id.* at 286–87 (emphasis in original). Because the defendant had a reasonable expectation of privacy in the contents of his emails, the court held that the government may not compel the disclosure of the contents of a subscriber's emails absent a warrant. *Id.* at 288. *Warshak* has yet to be extended to email metadata. Gray, *supra* note 295, at 161.

319. *See Carpenter*, 138 S. Ct. at 2261 (Alito, J. dissenting) ("[T]oday, some of the greatest threats to individual privacy may come from powerful private companies that collect and sometimes misuse vast quantities of data about the lives of ordinary Americans.").

320. Emma W. Sholl, *Exhibit Facebook: The Discoverability and Admissibility of Social Media Evidence*, 16 TUL. J. TECH. & INTELL. PROP. 207, 214 (2013).

321. *See Law Enforcement & Third-Party Matters,* FACEBOOK HELP CTR., *supra* note 299; *Guidelines for Law Enforcement*, TWITTER HELP CTR., [hereinafter TWITTER HELP CTR.], https://help.twitter.com/en/rules-and-policies/twitter-law-enforcement-support#8 (last visited Mar. 15, 2018); *Snapchat Law Enforcement Guide*, SNAPCHAT, https://storage.googleapis.com/snap-inc/privacy/lawenforcement.pdf (last updated Apr. 27, 2018).

322. *Privacy: Stored Communications Act*, ELECTRONIC FOUND. FRONTIER, https://ilt.eff.org/Privacy__Stored_Communications_Act.html (last updated Apr. 1, 2014, 5:46 PM).

cerning the substance, purport, or meaning of that communication."[323] It does not include metadata.[324] Several courts have ruled that because metadata is not content under the SCA, "basic subscriber information"[325] may be obtained pursuant to a civil subpoena.[326] However, this can present a significant burden considering that Facebook may seek reimbursement for responding to requests, as permitted by law.[327] Furthermore, an out-of-state subpoena must first be domesticated, or reissued by a California superior court, before it can be served on Facebook, a California domiciliary.[328] Thus, although obtaining basic subscriber information is not without its challenges, issuing a subpoena to Facebook is still a feasible strategy to obtain metadata (besides CSLI) with which to authenticate social media evidence—for now.

3. The SCA and the Right to a Fair Trial

While *Carpenter* reviewed the SCA's constitutionality under the Fourth Amendment,[329] other courts have begun to consider the criminal defendant's disadvantage in social discovery.[330] Not only does the SCA shield the contents of electronic communications from being disclosed to civil litigants pursuant to a civil subpoena,[331] but it also pre-

323. 18 U.S.C. § 2510(8) (2012).

324. *Metadata is Not Content Under the Stored Communications Act*, ESI CASE LAW (Mar. 1, 2013), https://www.ilsteam.com/metadata-is-not-content-under-the-stored-communications-act.

325. Basic subscriber information is the term used by social media companies to describe non-content or metadata. *Law Enforcement & Third-Party Matters,* FACEBOOK HELP CTR., *supra* note 299. For instance, Snapchat describes basic subscriber information as including: the email address, phone number, Snapchat account creation date and IP address, and timestamp and IP address of account logins and logouts. *Snapchat Law Enforcement Guide*, *supra* note 321.

326. *See, e.g.*, Lucas v. Jolin, No. 1:15-CV-108, 2016 WL 2853576, at *6 (S.D. Ohio May 16, 2016).

327. 18 U.S.C. § 2706 (2012); *Information for Law Enforcement Authorities,* FACEBOOK, *supra* note 300.

328. *See* Interstate and International Depositions and Discovery Act, CAL. CIV. PROC. CODE § 2029.300 (West 2008); *see also Law Enforcement & Third-Party Matters,* FACEBOOK HELP CTR., *supra* note 300 ("[T]he subpoena must be a valid federal, California or California domesticated subpoena . . . .").

329. United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) ("[T]o the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional.").

330. *See, e.g.*, Facebook v. S.C. (Touchstone), 408 P.3d 406 (Cal. 2018). Social discovery is a term used to describe the process by which investigators and law firms search, collect, and preserve information conveyed on social media platforms. *See* Tera Brostoff, *Social Media Tools Aren't Just for the Police Anymore,* BLOOMBERG NEWS (Nov. 2, 2016) https://www.bna.com/social-media-tools-n57982082168/.

331. ELECTRONIC FOUND. FRONTIER, *supra* note 322.

vents disclosure to criminal defendants.[332] The California Supreme Court is poised to decide whether the "statutory privacy protections afforded a social media user must yield to a criminal defendant's constitutional rights to due process, presentation of a complete defense, and effective assistance of counsel."[333] In *Facebook v. S.C. (Touchstone)*, petitioners claim that the SCA "undermines the ability of the defendants to put on their case,"[334] especially because the social media communications of the victim are often relevant to a claim of self-defense.[335] Under the SCA, defendants, as private parties, cannot compel social media companies to disclose the contents of non-public communications.[336] Thus, while extending *Carpenter* or the SCA might grant privacy rights over metadata, it would also further disadvantage criminal defendants.

B. Metadata's Utility Beyond Authentication: A Cost-Benefit Analysis

Fortunately, subpoenaing Facebook is not the only means of obtaining social media evidence: a party can hire a third-party vendor to conduct "social discovery" or collect the data themselves.[337] Of course, direct collection by a party extends to publicly-shared information only, unless a friend of the social media user is willing to divulge private communications shared with them.[338] It might be

---

332. Andrew Cohen, *How Social Media Giants Side with Prosecutors in Criminal Cases*, MARSHALL PROJECT (Jan. 15, 2018) [hereinafter Andrew Cohen], https://www.themarshallproject.org/2018/01/15/how-social-media-giants-side-with-prosecutors-in-criminal-cases.

333. *California Supreme Court to Review Whether Criminal Defendant Has a Constitutional Right to Obtain Social Media Records*, ESI CASE LAW (Jan. 29, 2018), https://www.ilsteam.com/issue-whether-criminal-defendant-constitutional-right-obtain-social-media-records-electronic-communication-service-federal-stored-communications-act-review (referring to *Facebook*, 408 P.3d at 406).

334. 408 P.3d at 406; Andrew Cohen, *supra* note 332.

335. *See* People v. Nunn, No. 3–14–0137, 2016 WL 2866361 at *8 (Ill. App. Ct. May 16, 2016) (finding Facebook messages relevant to the defendant's self-defense claim); *see also* Frances Robles, *Judge: Zimmerman defense can go after Trayvon records, social media accounts*, MIAMI HERALD (Oct. 19, 2012, 6:00 AM), http://www.miamiherald.com/news/state/florida/trayvon-martin/article1943776.html ("Defense lawyers are free to subpoena Trayvon Martin's school records and social media accounts, a judge ruled Friday, setting the stage for a show-down between a man facing life in prison and new media companies that are unlikely to turn over records without a fight.").

336. *See* 18 U.S.C. § 2702(a)(1) (2012); Andrew Cohen, *supra* note 332.

337. *See* Brostoff, *supra* note 330.

338. Sharon D. Nelson & John W. Simek, *Preserving, Harvesting, and Authenticating Social Media Evidence*, 53 JUDGES J. 26, 27 (2014). Ethics rules have been interpreted to prohibit an attorney from sending friend requests to adverse parties or witnesses, especially under false pretenses. Murphy & Fontecilla, *supra* note 52, at 19. Here, again, "government agents are allowed to go further than defense counsel . . . by creating fake online identities or by securing cooperating witnesses to grant them access to [private] information." Murphy & Fontecilla, *supra* note 52,

preferable to use e-discovery software or services to request the data directly from the social media provider for a couple of reasons. First, social media providers will only preserve account records when requested by law enforcement or government agencies and even then, only for ninety days.[339] On the other hand, e-discovery software employs forensic data collection techniques to ensure that "data is preserved in a defensible manner."[340] Second, social media companies do not provide authentication witnesses,[341] whereas e-discovery consultants are credible experts.[342]

The increased use of ESI in litigation has led to a robust and lucrative e-discovery market.[343] Although e-discovery is notorious for being expensive, it may not be as cost-prohibitive as it seems.[344] The pressure on law firms to keep litigation costs down has prompted creative and flexible pricing options.[345] As a result, social discovery tools are not just available to the Government and repeat players with deep pockets.[346] In fact, there are various open-source programs that can be used to harvest social media data and metadata for free.[347] Even if

---

at 7; *see, e.g.*, United States v. Meregildo, 883 F. Supp. 2d 523, 526 (S.D.N.Y. 2012) ("[T]he Government did not violate the Fourth Amendment when it accessed Colon's Facebook profile through a cooperating witness.").

339. *Law Enforcement & Third-Party Matters,* FACEBOOK HELP CTR., *supra* note 299; TWITTER HELP CTR., *supra* note 321; *Snapchat Law Enforcement Guide*, *supra* note 321.

340. David Ahrens, *eDiscovery Trends & Predictions for 2017*, FRONTEO (Jan. 30, 2017), https://web.archive.org/web/20170304044621/http://www.fronteo.com/usa/ediscovery-trends-predictions-for-2017/ (original URL unavailable).

341. *Information for Law Enforcement Authorities,* FACEBOOK, *supra* note 300; *Snapchat Law Enforcement Guide*, *supra* note 321.

342. Nelson & Simek, *supra* note 338, at 27. "[I]t really doesn't make sense to . . . put anyone from your firm on the stand to authenticate the evidence, particularly because your firm and your client have a vested interest in the outcome of the case. The evidence may seem suspect." Nelson & Simek, *supra* note 338, at 27.

343. Bibart, *supra* note 29, at 793; "The global market for eDiscovery (Software & Services) is projected to reach US$11.6 billion by 2020, driven by growing demand from governments and private enterprises, rise in criminal prosecutions & civil litigations and increased admissibility of digital data in investigational proceedings." *The Global E-Discovery (Software and Services) Market Trends, Drivers & Projections*, GLOBAL INDUSTRY ANALYSTS, INC., http://www.strategyr.com/MarketResearch/eDiscovery_Software_and_Service_Market_Trends.asp (last visited, Mar. 13, 2018).

344. *See* Nelson & Simek, *supra* note 338, at 26 ("[T]he costs are minimal, generally several hundred dollars."). Some e-discovery companies "cheerfully give you . . . a free 30-day trial." Nelson & Simek, *supra* note 338, at 26.

345. Ahrens, *supra* note 340; For examples of low-cost alternatives *see* Tom O'Connor, *Cost-Effective E-discovery for Small Cases*, 30 GP SOLO 1 (2013).

346. Brostoff, *supra* note 330; O'Connor, *supra* note 345.

347. *Social Media Harvesting Tools*, NCSU LIBR., https://www.lib.ncsu.edu/social-media-archives-toolkit/collecting/social-media-harvesting-tools (last visited Mar. 13, 2018); *Protocol for Metadata Harvesting Tools*, OPEN ARCHIVES INITIATIVE, https://www.openarchives.org/pmh/tools/ (last visited Mar. 13, 2018).

there is some sticker shock, "the initial expense is likely to be outweighed by the future benefit."[348] For instance, a single-user license for X1 Social Discovery software costs less than $2,000 a year before taxes.[349] To put that in perspective, a litigant will spend an average of $35,000 in discovery costs in each federal suit and approximately half that amount in each state suit.[350] Furthermore, research shows that the cost of discovery is proportional to what is at stake in the litigation.[351]

E-discovery software tools can save time and money by automatically collecting data from multiple social media accounts and across several social media platforms.[352] Unlike printing to paper or using image capturing software, these tools capture social media content in native format and thus preserve critical metadata.[353] The software can also insert hash values at the time of preservation, which not only serves as a digital Bates stamp but also can be used to verify the integrity of the chain of custody.[354] E-discovery tools utilize location data gathered by social media platforms to "geostream," or perform searches by location—for instance, collecting all of the tweets from a designated area.[355] These "geo-pinpoints can also be viewed on a map"[356] and perhaps later turned into demonstrative evidence. Fi-

348. Andrew B. Delaney & Darren A. Heitner, *Made for Each Other: Social Media and Litigation*, 85 N.Y. ST. B. ASS'N. J. 10, 14 (2013).

349. More precisely, X1 Social Discovery 5.3 costs $2,119.69. *Shopping Cart*, X1 SOC. DISCOVERY, https://www.x1.com/products/x1_social_discovery/ (last visited Oct. 12, 2018) (follow "Buy Now" hyperlink).

350. Robert Hilson, *How Much Does E-Discovery Cost the U.S. Every Year?*, LOGIKCULL (July 20, 2015), http://blog.logikcull.com/estimating-the-total-cost-of-u-s-ediscovery.

351. Brooke D. Coleman, *The Real Cost of Litigation Reform: Justice, Not Discovery Costs, Are at Stake*, AM. CONST. SOC'Y BLOG (Feb. 14, 2014), https://www.acslaw.org/acsblog/the-real-cost-of-litigation-reform-justice-not-discovery-costs-are-at-stake ("[A Federal Judicial Center] study found a 1 percent increase in stakes was associated with a 0.25 percent increase in total discovery costs.").

352. *Social Media and Internet-Based Data Collection*, X1 SOC. DISCOVERY, https://www.x1.com/products/x1_social_discovery/ (last visited Mar. 13, 2018). "Each Collection takes a few minutes to several hours, depending on how much you're grabbing. You can set a schedule for how often collections check for new posts or information." Brett Burney, *X1 Social Discovery tackles social media collection in a logical fashion*, LEGAL TECH NEWS (Sept. 2016), https://www.x1.com/download/X1_Social_Discovery_LTN_Review.pdf (reviewing X1 Social Discovery).

353. *Social Media and Internet-Based Data Collection*, *supra* note 352. Preserving data in native format and with its accompanying metadata is not only important for authentication, but a party may be required to produce ESI and its metadata in native format pursuant to Ill. Sup. Ct. R. 214(b), which is the functional equivalent of Fed. R. Civ. P. 34(b)(2)(E)(i).

354. *See* discussion *supra* Part III.A.1; *Social Media and Internet-Based Data Collection*, *supra* note 352.

355. Brostoff, *supra* note 330; *see also* Burney, *supra* note 352.

356. Burney, *supra* note 352.

nally, both the publicly available and licensed e-discovery software products seem relatively easy to use.[357]

Thus, while it may seem expensive to hire an e-discovery consultant or purchase the software needed to harvest the data in-house, the investment certainly pays off considering how valuable social media evidence can be.[358] Do-it-yourself methods such as taking a screenshot or printing to paper are quickly becoming less and less viable given that they fail to preserve the metadata.[359] The remaining parts of this section will show how failing to preserve the metadata can prove to be an expensive mistake.[360] First, the rules of discovery and a lawyer's professional and ethical duties promote, if not demand, the preservation of metadata. Second, metadata's utility extends beyond discovery and authentication—it can be used to avoid other evidentiary objections.

1. Spoliation and Professionalism

Preserving data in native format and with its accompanying metadata is not only important for authentication, but sometimes necessary in discovery.[361] The rules of discovery dictate that if a discovery request does not specify the form, "a party must produce [ESI] in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms."[362] In other words, the document's native format includes metadata.[363] This is partly because metadata is used by the recipient to search, sort, and cull documents in order to facilitate a more efficient—and consequently less costly—review.[364] Although stripping metadata may sometimes be justified to protect client confidences,[365] lawyers can face sanctions for failing to preserve and pro-

357. *See* Nelson & Simek, *supra* note 338, at 26 ("Lawyers could certainly use any of the products we've cited above."); *see generally* Burney, *supra* note 352.

358. Murphy & Fontecilla, *supra* note 52, at 28; *see also* Grimm 2013, *supra* note 8, at 437–38.

359. *See* Nelson & Simek, *supra* note 338, at 27.

360. Keefe, *supra* note 6, at 1043 (observing that the failure to perform an adequate investigation and preservation of social media evidence "might make the difference between winning a case and receiving sanctions").

361. Rosenberg, *supra* note 153, at 468–69.

362. Ill. Sup. Ct. R. 214(a); *see also* Fed. R. Civ. P. 34(b)(2)(E)(i).

363. Rosenberg, *supra* note 153, at 468–69.

364. The Sedona Conference, *supra* note 40, at 170.

365. *See* Rosenberg, *supra* note 153, at note 452.

duce metadata.[366] Additionally, Illinois recognizes a separate and distinct claim for the tort of negligent spoliation of evidence.[367]

On the other hand, several states have weighed in on whether mining the metadata of documents received from the opposing party is ethically permissible.[368] The concern is with safeguarding client confidence, knowing that metadata reveals potentially devastating information.[369] Although the guidance varies greatly depending on the state, the American Bar Association opined that litigants may review metadata contained in documents sent from adverse parties, but they are still obligated to notify the adverse party when there is reason to believe the transmission was inadvertent.[370] Notably, the American Bar Association's Model Rules of Professional Conduct impose no explicit duty to scrub a document of its metadata, but presumably, the duty to protect confidentiality applies equally to metadata.[371] Illinois has yet to weigh in, but other states that have opined on the subject impose a reasonable care standard.[372]

Furthermore, lawyers "have a duty to understand and appreciate the potential pitfalls" of handling ESI.[373] The Illinois Rules of Profes-

---

366. *See* Ill. Sup. Ct. R. 219 committee comment to 2002 amendment (revised May 29, 2014); *cf.* Fed. R. Civ. P. 37. When the Illinois Supreme Court Rules were updated to address the discovery of ESI, rule 219 addressing discovery sanctions was not changed, only a comment was added stating:

> The Committee believes that the rule is sufficient to cover sanction issues as they relate to electronic discovery. The rulings in *Shimanovsky v. GMC*, 181 Ill.2d 112 (1998) and *Adams v. Bath and Body Works*, 358 Ill. App. 3d 387 (1st Dist. 2005) contain detailed discussion of sanctions for discovery violations for the loss or destruction of relevant evidence and for the separate and distinct claim for the tort of negligent spoliation of evidence.

Ill. Sup. Ct. R. 219 committee comment to 2002 amendment. However, Illinois decisions addressing sanctions for the loss or destruction of responsive evidence have traditionally involved human intervention. "ESI on the other hand, can be lost simply from the routine operation of a computer . . . . Accordingly, the issue of sanctions for the loss of ESI will present new scenarios" for the court to address. Steven M. Puiszis, *Understanding Illinois' New Discovery Rules,* http://c.ymcdn.com/sites/iadtc.site-ym.com/resource/resmgr/Understanding_Illinois%27_New_.pdf (last visited Mar. 16, 2018).

367. *See* Ill. Sup. Ct. R. 219 committee comment to 2002 amendment (revised May 29, 2014).

368. *Metadata Ethics Opinions Around the U.S.*, A.B.A. LEGAL TECH. RES. CTR., https://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/metadatachart.html (last visited Mar. 13, 2018) (collecting ethics opinions on the topic).

369. *Id*.

370. *Id.*; Karel Mazanec & Douglas B. Mishkin, *"Mining for Metadata": Will You Strike Gold or Strike Out?*, VENABLE LLP: LABOR & EMP. LAW TRADE SECRETS & TRANSITIONS (May 4, 2017), https://www.tradesecretsandtransitions.com/2017/05/mining-for-metadata-will-you-strike-gold-or-strike-out/.

371. *Metadata Ethics Opinions Around the U.S.*, *supra* note 368.

372. *Metadata Ethics Opinions Around the U.S.*, *supra* note 368.

373. Jan L. Jacobowitz & Danielle Singer, *The Social Media Frontier: Exploring A New Mandate for Competence in the Practice of Law*, 68 U. MIAMI L. REV. 445, 466 (2014).

sional Conduct mandate that "a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*."[374] The lawyer's duty of competence has thus expanded to require lawyers to become familiar with various social media platforms and e-discovery technology, and to prepare for the challenges associated with both.[375] In *Lorraine*, Judge Grimm observed that "the inability to get evidence admitted because of a failure to authenticate it almost always is a self-inflicted injury which can be avoided by thoughtful advance preparation."[376] Merely by adhering to the professional standards and the rules of discovery, metadata will be preserved and can be used for authentication later.

2. Avoiding Other Evidentiary Objections

Metadata is not only useful in authenticating social media evidence but can also be used to avoid other evidentiary objections. For instance, hash values could be used to avoid an objection based on the original writing rule.[377] Timestamps and location data could prove tweets were present sense impressions.[378] In *Maya*, the certificate of authenticity also served to satisfy the business record hearsay exception.[379] More generally, as machine-generated information, metadata "is not hearsay because it is not 'statements' of a 'person' under Rule 801(a)."[380] Because metadata serves more than one function, litigators can introduce social media evidence more efficiently. The process is all the more expeditious if the metadata records are self-authenticating as business records under 902(11), or under the new federal rules 902(13) and 902(14).[381] Self-authentication alleviates the need to call and compensate an expert witness to lay a foundation.[382]

374. Ill. Sup. Ct. R. Prof'l Conduct r.1.1 cmt. 8 (eff. Jan. 1, 2016) (emphasis added).

375. *See* Keefe, *supra* note 6, at 1043.

376. Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 542 (D. Md. 2007).

377. *See* Rodolfo Ramirez et al., *Location! Location! Location! Data Technologies and the Fourth Amendment*, CRIM. JUST., Winter 2016, at 19, 22 (explaining that duplicates are admissible so long as it accurately reflects the original).

378. *See* Pannozzo, *supra* note 3, at 1706.

379. People v. Maya, 88 N.E.3d 10, 31 (Ill. App. Ct. 2017).

380. John M. Haried, *How Two New Rules for Self-Authentication Will Save You Time and Money*, 100 JUDICATURE, Winter 2016, at 34, 39.

381. Reporter's Memorandum, *supra* note 160, at 210.

382. Reporter's Memorandum, *supra* note 160, at 211.

C. The Right to Confrontation & the Illinois Approach to Computer-Generated Data

As always, the concern with self-authentication is that the opponent loses the ability to cross-examine the authenticating witness.[383] This is of particular concern in the criminal context where defendants are guaranteed the right to cross-examine by the Sixth Amendment's Confrontation Clause.[384] The Confrontation Clause is only applicable to testimonial statements, and it is yet unresolved as to whether certificates from computer forensic analysts qualify as testimonial.[385] In *Melendez-Diaz v. Massachusetts*, the Supreme Court found that statements prepared solely to be submitted at a criminal trial were testimonial.[386] However, the decision carved out a narrow exception for records used to authenticate other documents.[387] This exception could be read to include certificates authenticating Facebook records as business records under 902(11), or machine-generated records under 902(13), because their sole purpose is to authenticate preexisting records.[388] Since *Melendez-Diaz*, lower courts have uniformly found that certifications of authenticity made pursuant to 902(11) do not violate the Confrontation Clause.[389] Furthermore, the Advisory Committee on the Federal Rules of Evidence notes that the new 902(13) and 902(14) fit more squarely within the *Melendez-Diaz* dictum.[390]

Melendez-Diaz has experienced a mixed reception in Illinois courts.[391] Most famously, the Illinois Supreme Court distinguished *Melendez-Diaz* in *People v. Williams*,[392] which was later affirmed by the United States Supreme Court in a plurality opinion.[393] Illinois courts have continued to apply the primary purpose test narrowly,[394] consistently finding *Melendez-Diaz* inapplicable to business records as

383. *See generally* Melendez-Diaz v. Mass., 557 U.S. 305 (2009).

384. U.S. CONST. amend. VI.

385. Reporter's Memorandum, *supra* note 160, at 218.

386. 557 U.S. at 305.

387. *Id.* at 322–23.

388. Reporter's Memorandum, *supra* note 160, at 218.

389. Reporter's Memorandum, *supra* note 160, at 219; *see, e.g.*, United States v. Yeley-Davis, 632 F.3d 673 (10th Cir. 2011).

390. Reporter's Memorandum, *supra* note 160, at 220.

391. According to Westlaw, 18 of 46 Illinois cases citing *Melendez-Diaz* either declined to extend its holding, declined to follow it on state law grounds, or distinguished it (last viewed Oct. 31, 2018).

392. People v. Williams, 939 N.E.2d 268, 282 (2010), *aff'd sub nom.* Williams v. Illinois, 567 U.S. 50 (2012).

393. *Williams v. Illinois*, 567 U.S. at 86.

394. *See* People v. Leach, 980 N.E.2d 570, 593 (Ill. 2012) (finding an autopsy report was a non-testimonial business record); People v. Coleman, 24 N.E.3d 373, 408 (Ill. App. Ct. 2014) (finding IP address logs and subscriber information were non-testimonial business records); People v.

they are not "made for the purpose of proving the guilt of a particular criminal defendant at trial."[395] Specifically, in *People v. Coleman*, the court ruled that Google IP address logs and subscriber information were non-testimonial business records.[396] However, the logs still needed to be authenticated by a Google representative in order to be admitted.[397] Most recently in *Maya*, the court found that Facebook messages could be admitted under the Rule 803(6) business record exception to the hearsay rule.[398] What is more, the court held that the messages were self-authenticating under 902(11) and therefore, did not require an authentication witness.[399] This is convenient considering that most social media companies will not provide an authentication witness.[400] It seems as though Illinois courts have and will continue to treat metadata records as falling within the *Melendez-Diaz* carve out.

But wherever courts land on the constitutional and ethical issues discussed in these preceding sections, there is no doubt that criminal defendants stand to benefit from a streamlined method of authenticating social media evidence.[401] Metadata is equally effective at disproving the defendant is the putative author. Moreover, because errors in admitting social media evidence are often dispositive, using metadata

---

Jacobs, 939 N.E.2d 64, 71 (Ill. App. Ct. 2010) (finding the accuracy logbooks for a breathalyzer non-testimonial).

395. *See, e.g.*, *Leach*, 980 N.E.2d at 590 (quoting *Williams v. Illinois*, 567 U.S. at 84). Even before the Illinois Rules of Evidence were codified in 2011, § 115-5 of the Illinois Code of Criminal Procedure provided for a business record exception to the hearsay rule. 725 Ill. Comp. Stat. 5/115-5(a) (2014). Furthermore, § 115-5(c)(2) provides the exception that "[n]o writing or record made in the regular course of any business shall become admissible as evidence . . . if . . . [s]uch writing or record has been made by anyone during an investigation of an alleged offense or during any investigation relating to pending or anticipated litigation of any kind." People v. Universal Pub. Transp., 974 N.E.2d 251, 261 (Ill. App. Ct. 2012) (quoting § 5/115-5(c)(2)). Thus, section 115-5(c)(2) provides the statutory equivalent of the primary purpose test articulated in *Williams v. Illinois*. *Compare* § 5/115-5(c)(2) *with Williams*, 567 U.S. at 84. In fact, the Illinois Supreme Court ruled that admitting drug lab reports by affidavit not only violated § 115-5(c)(2) of the Illinois Code of Criminal Procedure but denied the defendant his right to confrontation in *People v. McClanahan* in 2000—nine years before *Melendez-Diaz* was decided. *See* People v. McClanahan, 729 N.E.2d 470, 474, 478 (Ill. 2000).

396. 24 N.E.3d at 408.

397. *Id.* at 409.

398. People v. Maya, 88 N.E.3d 10, 31 (Ill. App. Ct. 2017).

399. *Id.*

400. *Information for Law Enforcement Authorities,* FACEBOOK, *supra* note 299; *Snapchat Law Enforcement Guide*, *supra* note 321.

401. *See supra* text accompanying notes 330–36 (describing the criminal defendant's disadvantage in social discovery).

effectively should reduce the number of appeals and increase judicial efficiency.[402]

V. Conclusion

The ubiquitous use of social media in today's society means its use in litigation will only grow.[403] As a result, attorneys must familiarize themselves with the peculiar challenges presented by its use as evidence and prepare to meet them or risk disastrous results.[404] Authentication arguably poses the biggest hurdle to the admission of social media evidence, and errors committed on this issue have largely been found to be dispositive.[405] This Comment advocates for the use of metadata as the best method of authenticating social media evidence and argues that this method should be adopted as the standard practice in Illinois. Not only is the method endorsed by Illinois courts, and by most courts writing on the subject,[406] but using metadata to authenticate is effective in rebutting the most common challenges to authenticity.[407] Metadata offers conclusive evidence of the accuracy of a copy, as well as convincing circumstantial evidence of authorship.[408] Moreover, collecting metadata for use in authentication is feasible, reduces costs, and provides collateral benefits.[409] Finally, although social media may generally be perceived as untrustworthy, metadata is likely more reliable as it is machine-generated data.[410] Thus, metadata advances the basic truth-seeking function authentication was meant to serve.[411]

Linda Greene

---

402. *See* Kling et al., *supra* note 39, at 40 (observing that failure to properly authenticate social media evidence gives rise to arguments of error on appeal). *See, e.g.*, People v. Kent, 81 N.E.3d 578, 591 (Ill. App. Ct. 2017).

403. Margaret DiBianca, *Discovery and Preservation of Social Media Evidence*, A.B.A. Bus. L. Today, Jan. 2014, at 1.

404. *See supra* text accompanying notes 362–64 (describing the potential for sanctions); *see also, supra* text accompanying note 286 (observing that errors related to the authentication of social media evidence often have a dispositive effect on the outcome of the case, which in turn leads to overturned verdicts, potential malpractice liability, or both).

405. *See* Grimm 2013, *supra* note 8 at 437–39.

406. *See, e.g.*, *Kent*, 81 N.E.3d at 598; *see also* Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 548 (D. Md. 2007); Griffin v. State, 19 A.3d 415, 428 (Md. 2011); Tienda v. State, 358 S.W.3d 633, 647 (Tex. Crim. App. 2012).

407. *See* discussion *supra* Part III.A.

408. *See* discussion *supra* Part III.A.

409. *See* discussion *supra* Part IV.

410. *See* Reporter's Memorandum, *supra* note 160, at 210–16 (explaining the rationale for considering machine-generated information to be self-authenticating).

411. *See* Robbins, *supra* note 7, at 5.