Comment,
AN OVERVIEW OF AUTHENTICATION METHODS FOR SOCIAL MEDIA EVIDENCE

I. Introduction

Rule 1.1 of the ABA Rules of Professional Responsibility requires lawyers to obtain necessary knowledge and experience to be competent attorneys.[1] It would logically follow that with the increased use of social media, these "changes" would encompass the use of social media evidence. According to the Pew Research Center, in 2019 "tech use has become the norm" with nine out of ten adults in the United States saying they go online, 81% stating they own a smartphone, and 71% reporting they use social media.[2] This overwhelming use of social media by American adults inevitably leads to social media impacting family law matters. A survey previously conducted in 2010 by the American Academy of Matrimonial Lawyers revealed that 81% of the nation's top divorce attorneys said that they had "seen an increase in social networking evidence."[3] Of these same survey respondents, 66% stated that Facebook was the primary source of this type of evidence, 15% cited MySpace, 5% appeared via Twitter, and 14% was from other social media sites.[4] When considering the statistical use of social media in 2019 alone, inevitably, evidence relevant to family law cases will be found on social media. Social media is undeniably intertwined with family law practice—social media is how families connect and media repositories will hold abundant evidence of communications. Like all evidence,

---

1 MODEL CODE OF PROF'L RESPONSIBILITY r. 1.1 (2020).

2 Katherine Schaeffer, *U.S. Has Changed in Key Ways in the Past Decade, from Tech Use to Demographics*, FACT TANK, PEW RES. CTR. (Dec. 20, 2019), https://www.pewresearch.org/fact-tank/2019/12/20/key-ways-us-changed-in-past-decade/.

3 American Academy of Matrimonial Lawyers, *Big Surge in Social Networking Evidence Says Survey of Nation's Top Divorce Lawyers*, CISION PR NEWSWIRE (Feb. 10, 2010), https://www.prnewswire.com/news-releases/big-surge-in-social-networking-evidence-says-survey-of-nations-top-divorce-lawyers-84025732.html.

4 *Id.*

social media evidence must be authenticated before being offered into evidence, but this type of evidence presents unique challenges in order to be authenticated. Further, digital evidence in general presents similar challenges in authentication, especially with the advancement of technology such as the invention Artificial Intelligence (AI), a topic which will be discussed in detail in the final part of this comment.

This Comment will address authentication challenges in the context of the Federal Rules of Evidence by focusing on different scenarios that provide guidance to the practice of family law. Part II provides a brief, general overview of Rules 901 and 902 of the Federal Rules of Evidence in respect to common methods of authentication for social media evidence. Part III is split into three main parts. Section A focuses on authentication of photos published to social media and how the court treats photographic evidence found through social media platforms such as Facebook and Instagram. Then, Section B discusses authentication of social media posts and pages. Finally, Section C specifically discusses social media messages and how they are authenticated and admitted. The analysis in Part III provides case examples with factual details about how the social media evidence was authenticated in different federal courts. Part IV addresses the Stored Communications Act[5] and other issues around accessing social media that is private and not available for all users on public pages or posts. Finally, Part V raises concern around the development of technology and how that can affect the authentication of social media and digital evidence as a whole.

II. Authentication of Social Media Evidence

While many issues can arise in the process of admitting evidence, the Honorable Paul W. Grimm described authentication of digital evidence at trial as the "greatest challenge."[6] After social media evidence is deemed relevant under Rule 401 of the Federal Rules of Evidence and not prejudicial under Rule 403, then "certain [other] foundational requirements must be met in

---

5 18 U.S.C. §§ 2701-2712.

6 Paul W. Grimm, et al., *Authentication of Social Media Evidence*, 36 Am. J. Trial Advoc. 433, 439 (2013).

order to authenticate social media content."[7] Rule 901 of the Federal Rules of Evidence states that to authenticate evidence, "the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is."[8] Rule 901 does not require that the proponent must "conclusively demonstrate the genuineness of the article" but instead he or she must make a "showing sufficient to support a finding that the matter in question is what its proponent claims."[9] This requisite for authentication has also been recognized by the Uniform Rules of Evidence.[10]

Several methods of authentication are available for social media evidence through Rule 901 of the Federal Rules of Evidence.[11] A common method of authentication for social media evidence is through the use of testimony.[12] Under Rule 901, an attorney may utilize a witness to provide testimony or an opinion in support of the authentication of social media evidence.[13] Rule 901 states that evidence can be authenticated with the use of a witness "with knowledge" stating that an "item is what it is claimed to be."[14] Another method of authentication that can involve testimony is with the support of an expert witness.[15] Rule 901 also allows non-testimonial support for social media evidence when it has "distinctive characteristics taken together with all the circumstances."[16] Furthermore, social media evidence can also be self-authenticating, meaning it does not need additional evidence for authentication because it "bear[s] sufficient indicia of reliability to be 'self-authenticating.'"[17]

---

7 GREGORY J. BATTERSBY & CHARLES W. GRIMES, PAT. DISPUTES LITIG FORMS & ANALYSIS § 5.12[D][1] (2d ed. 2020).

8 FED. R. EVID. 901.

9 George L. Blum, Annotation, *Authentication of Social Media Records and Communications*, 40 A.L.R. 7th Art. 1 § 2 (2019).

10 *Id*.

11 FED. R. EVID. 901.

12 *Id*. at 901b)(1).

13 *Id*. at 901.

14 *Id*. at 901(b)(1).

15 *Id*. at 901(b)(2).

16 *Id*. at 901(b)(4).

17 *See* FED. R. EVID. 902.

III. Social Media Publications

Social media evidence is digital evidence; therefore, social media evidence is different from traditional evidence in that it is not physically written on paper or tangible in a traditional sense. Because digital evidence is unique in this way, one might assume that it would be treated differently for purposes of the Federal Rule of Evidence 901. In some ways, this could be true in that there may not be handwriting to analyze on a social media post where everything is typed in a uniform font. This differs from a traditional "post," such as a public writing on a bulletin board, which would require authorship by hand.[18] However, the distinction for authentication between social media evidence and traditional physical evidence proves to be virtually non-existent in some federal circuits.[19] Specifically, when it comes to photographs, the distinction between a physical and digital image has proved virtually meaningless as well.[20]

A. *Digital Images*

"Digital imaging processing" is the processing of digital images on a computer.[21] A digital image itself is "composed of a finite number of elements, each of which has a particular location and value."[22] Particularly, a digital image is made up of "picture elements, image elements, pels, and pixels."[23] Therefore, a digital image departs from the general concept of a physical photo by its digital conception. Digital images are available on most social media websites, including Facebook, Instagram, Snapchat, and many other popular platforms. Social media platforms like these enable a user to download or "screenshot" digital images and save a copy of them to his or her separate device.

The U.S. Court of Appeals for the Sixth Circuit stated in reference to social media photos that "we see no reason to depart from the ordinary rule that photographs, including social-media photographs, are authenticated by 'evidence sufficient to support

---

18 *See id*. at 901(2).

19 *See* United States v. Thomas, 701 Fed. Appx. 414, 419 (6th Cir. 2017).

20 *Id*.

21 RAFAEL GONZALEZ & RICHARD E. WOODS, DIGITAL IMAGE PROCESSING 1 (2d ed. 1992).

22 *Id*. at 2.

23 *Id*.

a finding that the [photograph] is what the proponent claims it is.'"[24] This Sixth Circuit approach towards digital images is also followed by the Second, Third, and Fifth Circuits.[25] However, there are still appellate cases in federal courts across the United States regarding the specific steps in authentication of digital images depending on how the photos were accessed and how they were authenticated.[26]

1. *Facebook and Instagram*

In a 2019 Pew Research Center survey, 69% of adults responded that they use Facebook, ranking it in second for the most used social media service behind YouTube.[27] Additionally, it took first place as the primary source of social media evidence in the previously mentioned survey by the American Academy of Matrimonial Lawyers.[28] Therefore, it is more likely than not that a family law attorney has interacted with social media evidence derived from Facebook. The website Facebook itself allows users to create profiles and "posts," both of which can be made "public" or "private."[29] Facebook users can elect to make their posts "public," meaning anyone can access the content created by the individual on Facebook, or "private," meaning only select users can access the content.[30]

The same 2019 Pew Research survey showed that Instagram was in third place among nine popular social media websites used by U.S. adults.[31] Instagram, like Facebook, also allows its users to upload photos. Unlike Facebook, Instagram is a social media

---

24 *Thomas*, 701 Fed. Appx. at 419.

25 *See also* United States v. Vayner, 769 F.3d 125, 131–33 (2d Cir. 2014); United States v. Browne, 834 F.3d 403 (3d Cir. 2016); United States v. Barnes, 803 F.3d 209, 217 (5th Cir. 2015).

26 *See Thomas*, 701 Fed. Appx. at 418 (requiring a police officer to authenticate photographic evidence).

27 Schaeffer, *supra* note 2.

28 American Academy of Matrimonial Lawyers, *supra* note 3.

29 *See generally Manage Your Privacy*, FACEBOOK HELP CENTER, https://www.facebook.com/about/basics/manage-your-privacy (last visited July 24, 2020); *See generally Privacy and Safety in Messenger*, FACEBOOK HELP CENTER, https://www.facebook.com/help/messenger-app/1064701417063145/?helpref=HC_fnav&bc[0]=messenger%20App%20Help (last visited July 24, 2020).

30 *Manage Your Privacy*, *supra* note 29.

31 Schaeffer, *supra* note 2.

platform dedicated to the upload of photos and/or videos while Facebook allows other forms of publication. Facebook allows for long "statuses," formation of "groups," "business pages," and many other publication formats.[32] However, like Instagram, Facebook gives its users the options to include photos on a post or to create virtual "albums" where the user can publish photos. Therefore, both social media platforms contain photo publications which present themselves as digital evidence and often require the use of authentication in court.

2. *Government Agent Testimony for Facebook and Instagram Photos*

As previously mentioned, the use of testimony is a common method for authentication of social media evidence. In the First Circuit, the standard for authentication is "straightforward" and only requires showing that "there is enough support in the record to warrant a reasonable person in determining that the evidence is what it purports to be."[33] In *United States v. Vasquez-Soto*, defendant Vasquez-Soto was convicted of making false statements and theft in relation to the disability payments that he received.[34] On appeal, Vasquez-Soto argued that he should be acquitted because the evidence used was insufficient to sustain his convictions.[35] The evidence used to convict him was mostly of photos from Facebook discovered by an investigating agent who was working the fraud investigation involving Vasquez-Soto. The investigator, Jose Morales, found photos of Vasquez-Soto on his ex-wife's Facebook page and downloaded them from her page onto his computer. The photos depicted Vasquez-Soto in Colombia riding motorcycles, entering a paddleboat, among other activities that appeared to show him participating in activities that were used to demonstrate fraudulent use of disability.[36]At the trial, the government used investigator Jose Morales to authenticate the photos he downloaded from Facebook of Vasquez-Soto.[37]

---

32 *See* Facebook.com; Instagram.com

33 United States v. Vazquez-Soto, 939 F.3d 365, 373 (1st Cir. 2019).

34 *Id*. at 368.

35 *Id*.

36 *Id*. at 370.

37 *Id.* at 374.

First, the court addressed the authentication of social media data generally because Vasquez-Soto argued that the government failed to provide the requisite testimony from Vasquez-Soto's ex-wife to authenticate the Facebook page from which the photo was derived.[38] The First Circuit rejected this argument, stating that the ownership of the Facebook account was not at issue in this case; therefore, the defendant's ex-wife's testimony was not necessary to authenticate the Facebook photos.[39] The court instead affirmed the district court decision and accepted the testimony of the investigator Jose Morales to authenticate the photos. To support its decision the court quoted the First Circuit decision in the earlier case *United v. Holmquist*, "A photograph's contents, buttressed by indirect or circumstantial evidence, can form a sufficient basis for authentication even without the testimony of the photographer or some other person who was present at the time it was taken."[40] Therefore, *Vasquez-Soto* demonstrates that in the First Circuit, if a photo is downloaded from Facebook and used as evidence, the person who downloaded it is able to testify to its authenticity by simply recognizing the subject of the photo.[41] This type of authentication approach demonstrated in *Vasquez-Soto* allows attorneys to authenticate photos with the use of anyone who (1) can access public Facebook photos and (2) has personal knowledge of the party in the photo.[42] *Vasquez-Soto* also demonstrates that this court treats the authentication of a digital photo downloaded onto a personal computer in the same way it treats physical photos filed away in a cabinet.[43]

Similarly to the First Circuit *Vasquez-Soto* approach, the Sixth Circuit has stated that "it is not at all clear why our rules of evidence would treat electronic photos that police stumble across on Facebook one way and physical photos that police stumble across lying on a sidewalk a different way."[44] The court in the Sixth Circuit case *United States v. Thomas* appeared to utilize this

---

38 *Id.* at 370.

39 *Id*. at 373.

40 *Id*. (quoting United v. Holmquist, 36 F.3d 154, 169 (1st Cir. 1994)).

41 *Id*.

42 *See generally id*.

43 *Id*.

44 United States v. Farrad, 895 F.3d 859, 879-80 (6th Cir. 2018).

approach when an officer found and authenticated a photograph of the defendant through a Facebook search.[45] In *Thomas*, the defendant challenged, on appeal, the authentication of the photographic evidence derived from Facebook and Instagram used to identify him at trial.[46] The officer who discovered this photo and authenticated it at trial, Officer David Holt, testified that he got onto his personal Facebook and searched "Jabron Thomas" in efforts to find a public profile.[47] Officer Holt found a profile which had photographs associated with it and saved five pictures from the public Facebook profile and offered them into evidence along with his testimony about how he found the photos.[48] Further, Officer Holt admitted at trial that "he did not know who created the Facebook page or whether the Facebook page itself was authentic."[49]

In the same trial, FBI Special Agent George Rienerth offered publicly accessed Instagram photos into evidence after he found an Instagram page that had the full name of the defendant.[50] Like Officer Holt, he also admitted that "he did not know who created the Instagram page, who uploaded the photographs, or whether the Instagram page was authentic."[51] Despite the shared lack of confidence in the authenticity of both social media pages, both officers' testimonies were sufficient to authenticate the photographs found on those social media pages.[52] Interestingly, the court here acknowledged a few scenarios where an individual could be implicated in a crime from falsified social media identities via uploaded photos:

> Our court has not yet confronted the question whether social-media-profile photographs are admissible to identify the person who is purported to be the owner of the profile. In many contexts, the question could conceivably be quite interesting: what if, for example, the owner of a social-media profile (let's call him Alex) used a picture of someone else (say, Bob) as his profile picture? If Bob robbed a bank, Alex would not want to be implicated as the robber simply because he had

---

45 *See generally Thomas*, 701 Fed. Appx. at 418.
46 *Id*.
47 *Id*.
48 *Id*.
49 *Id*. at 419.
50 *Id*.
51 *Id*.
52 *See generally id*.

> Bob's picture on his social-media profile. Or, what if Bob fabricated a social-media profile under Alex's name, but with Bob's picture—and then Bob robbed a bank? Or, less convolutedly, what if there were allegations that the online photographs had been digitally manipulated or hacked in some way?[53]

Nonetheless, the court denied defendant Thomas' argument, stating that "None of these questions—or any like them—is presently before us," and therefore applied the "ordinary rule" for photographs.[54] The court pointed out that the pictures showed Thomas with "distinctive tattoos on his hands and arms," appeared to show him wearing a hat which displayed the name of his employer at the time, and presented other unique characteristics that related to defendant Thomas.[55]

Further, the court made an important distinction in *Thomas* by specifying that the case did not involve authentication of the Facebook or Instagram pages, but instead concerned the authentication of photos of defendant Jabron Thomas and that the jury "was free to consider the photographs as identifying Thomas or not."[56] Therefore, although the officers were not certain as to the authenticity of the Facebook and Instagram pages as a whole, in terms of ownership or forgery, the fact that photos themselves were accessed and provided by the officers were the only foundational requirements relevant to the authentication.[57] Again, like the First Circuit, the Sixth Circuit adopted the same concept for authentication that the photo itself is where the focus should be without regard to its composition: digitally composed or physically printed.[58] Both Officer Holt and FBI Special Agent Rienerth accessed the photos on Instagram and Facebook on public pages and it appeared that the owner of those pages was irrelevant for authentication analysis because the defendant Thomas was still identifiable by the photos alone.[59]

---

53 *Id*.

54 *Id*.

55 *Id*.

56 *Id.* at 419-20.

57 *Id.*

58 *See generally id*; *Vasquez-Soto*, 939 F.3d 365.

59 *Thomas*, 701 Fed. Appx. at 419-20.

3. *Expert Witness to Authenticate Facebook and Instagram Photos*

One accepted method of authenticating Facebook posts is with the support of an expert witness.[60] *United States v. Parker*, in the Eighth Circuit, involved Facebook and Instagram posts showing the defendant in the company of particular gang members.[61] The defendant in *Parker* was convicted of conspiring to possess firearms in relation to gang activity.[62] The court affirmed the authentication of Facebook and Instagram photos which showed the defendant in the presence of members of a gang, based on the support of an expert witness on gang intelligence.[63] The expert in gang intelligence testified that the photos of the defendant met seven out of nine indicators that identify gang members.[64] The court allowed this testimony from the gang expert to authenticate the photo and denied the defendant's claim that the authentication was improper.[65]

The court did not explain in detail why the authentication was proper, except that it mentioned how the expert reasoned that the photo demonstrated gang involvement and that two other witnesses "provided context to the gang war and animosity between the [two gangs]."[66] Therefore, the expert's support with the use of a gang indicator measure was enough to admit into evidence two photos found on Facebook and Instagram without regard to how they were accessed or other identifiers regarding the pages from which they came.[67] This foundation for social media evidence seems to depart from typical testimony in that it focuses more on the content of the photo rather than the photo itself. Moreover, it seems to skip authentication of the photo and instead goes straight to creating a connection between the content of the photo and gang activity. As mentioned, images have been authenticated through testimony, both by individuals with and without expertise. While the testimonial method proves ef-

---

60 United States v. Parker, 871 F.3d 590, 596 (8th Cir. 2017).
61 *Id*.
62 *Id*.
63 *Id*.
64 *Id*.
65 *See id*. at 590.
66 *Id*. at 596.
67 *See generally id*.

fective for digital images, other methods prove effective as well. These will be examined in the following section.

C. *Social Media Pages and Posts*

Many social media websites, such as Facebook, allow users to create their own "pages" and publish their own "posts."[68] For example, a Facebook user has the ability to create his or her own "page" which is a unique collection of information, typically holding biographical information, photos, and posts.[69] Additionally, Facebook allows users to create business pages and groups that host other information such as business hours, locations, and other specifics relating to the business or group.[70] Social media posts and pages differ from traditional written evidence in that the websites typically allow the user to publish in a uniform font, meaning the writing is uniform and not unique handwriting.[71] Further, to publish a post or page under the identity of another's account, all one would need is access to the user's devices where they are logged onto the social media site. Therefore, it is arguably easy to post or make a page that appears to be authored by the social media user when it is in fact posted by someone else. This concern is addressed by the courts in the following section.

1. *Plaintiff Testifies for Facebook Post "Screenshots"*

The Fourth Circuit has followed suit in the "prima facie showing" for authentication, meaning the "burden is not high," and that circuit follows the above First and Third Circuit methods.[72] Within the Fourth Circuit, in the Western District Court of North Carolina, the court ruled that the plaintiff, in her own case, properly authenticated "screenshots"[73] taken from Facebook

---

68 *See generally* FACEBOOK, www.facebook.com; TWITTER, www.twitter.com; *Instagram*, www.instagram.com.

69 *See generally Create and Manage a Page*, FACEBOOK, https://www.facebook.com/help/135275340210354/?helpref=HC_fnav (last visited Jul. 24, 2020).

70 *Id*.

71 *See generally* FACEBOOK, www.facebook.com; TWITTER, www.twitter.com.

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

73 A "screenshot" is an image that shows the contents of a computer display. *Screenshot*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/screenshot (last visited July 16, 2020).

posts published by her co-workers.[74] In *Eschert v. City of Charlotte*, the plaintiff Eschert sued her employer, the Charlotte Fire Department (CFD), stating eight causes of action related to her termination.[75] CFD defended its termination of Eschert claiming that she was fired because she made an inappropriate post on Facebook that violated its social media policy.[76] The plaintiff proffered evidence in the form of Facebook "screenshots" that her husband took on his phone which showed a number of Eschert's co-workers Facebook posts.[77] These Facebook posts demonstrated that the plaintiff's similarly situated co-workers published "equally inappropriate" Facebook posts but were not terminated from their positions.[78] The court agreed that the manner in which they were authenticated, by the plaintiff's husband's testimony, was sufficient. Specifically, the plaintiff's husband testified that he had personally taken the screenshots of the Facebook posts from his phone, the screenshots "notated the date and time that he took them," and that they were still "publicly available" on Facebook.[79] Further, the plaintiff's husband also testified that he provided the screenshots to the defendant at the first termination hearing.[80] The court concluded that the combination of the husband's testimony and the fact that a co-worker also testified as to the authenticity of one of the screenshots, because it was *his* Facebook post, was sufficient foundation to admit the evidence and that the jury could decide the weight of the evidence from there.[81]

Interestingly, the defendant argued that the screenshots constituted inadmissible hearsay. The court, however, rejected this argument, stating that the purpose of admitting these posts was not for the truth of the matter asserted, but instead, to show that there were similarly situated individuals' similar "public statements" to the one that caused the plaintiff's termination.[82] This is

---

74 *See generally* Eschert v. City of Charlotte, No. 3:16-cv-295-FDW-DCK, 2017 WL 3633275 (W.D.N.C. Aug. 23, 2017).

75 *Id*. at 1*.

76 *Id.*

77 *Id*. at 6*.

78 *Id*.

79 *Id*.

80 *Id*.

81 *Id*.

82 *Id*. at 7*.

important to note because it demonstrates that although this was a Facebook post, it was still treated as a statement by another person and was confirmed by another person's testimony. To avoid issues of hearsay, the court instructed the jury to only consider the statements for their limited purpose and actually redacted the individuals' names from the admitted screenshots so that their identities were not shown.[83]

2. *Self-Authenticating Business Records Exception and Facebook Pages*

The Fourth Circuit held in *United States v. Hassan* that Facebook and YouTube videos can be considered self-authenticating business records under Rule 902.[84] *Hassan* involved three criminal defendants: Mohammad Omar Aly Hassan, Ziyad Yaghi, and Hyser Sherifi.[85] All three men were indicted on charges centered around terrorism conspiracies.[86] Part of the evidence used against the defendants consisted of Facebook pages and YouTube videos.[87] The federal appellate court affirmed the trial court's authentication through Rule 902(11), the business records exception to hearsay under Rule 803(6), for those Facebook pages and YouTube videos.[88] However, the court of appeals specified that the trial court reached its conclusion because the government appropriately proved with the use of Rule 901 that the Facebook pages were linked to the defendants Hassan and Yaghi.[89]

Like *Eschert*, defendant Hassan's and Yaghi's Facebook pages were recorded via screenshots which displayed Hassan's and Yaghi's user profiles and postings.[90] The screenshots of the Facebook pages included photos and links to the YouTube videos which were later admitted.[91] The Facebook screenshots displayed the personal biographical information of Hassan and

---

83 *Id*. at 7*.
84 *Id*. at 132-33.
85 *Id*. at 110.
86 *Id.* at 110-11.
87 *Id*. at 132-33.
88 *Id*. at 133.
89 *Id*. at 132-33.
90 *Id*. at 133.
91 *Id*.

Yaghi which supported the fact that the pages belonged to the defendants.[92] Further, the government provided certifications of records custodians for both the Facebook pages and YouTube videos to the court.[93] These certifications were used to show that the pages and videos "were maintained as business records in the course of regularly conducted business activities."[94] Therefore, the Fourth Circuit held that social media evidence can be authenticated with Rule 902(11) when there is proper connection between the identity of a person and his social media posts and the pages relate to his regularly conducted business activities.

D. *Facebook Messenger*

Facebook Messenger in 2019 had approximately 1,300,000,000 users a month, making it the second most utilized messaging app behind Whatsapp.[95] Given its high use, Facebook Messenger has made its appearance in a number of federal court cases, some of which are analyzed in this section. Unlike social media posts or pages, Facebook messages are only between the original sender and a designated recipient.[96] Thus, accessing Facebook messages between private individuals sometimes requires data retrieval from Facebook itself.[97] Another complication of introducing retrieved Facebook messages into evidence, which may not surface as an impediment in a public post or for an image posted to Facebook, is the barrier of the evidence being classified as hearsay.[98]

---

92 *Id*.

93 *Id*.

94 *Id*.

95 J. Clement, *Most Popular Global Mobile Messaging Apps 2020*, STATISTA (July 24, 2020), https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/.

96 *Protecting Your Privacy*, MESSENGER, https://www.messenger.com/privacy (last visited Jul 24, 2020).

97 *Browne*, 834 F.3d at 403 (the government obtained messages from Facebook.com).

98 *See also Hassan*, 742 F.3d 104 (allowing a hearsay exception through Federal Rule of Evidence 902(11)).

1. *Self-Authenticating Business Records Exception and Facebook Messenger*

Contrary to the decision in the Fourth Circuit case *Hassan*, the Third Circuit has held that Facebook chat logs alone do not qualify for self-authentication under Federal Rule of Evidence 902(11).[99] The Third Circuit in *United States v. Browne* addressed authentication standards where the defendant was convicted of crimes relating to child pornography and sexual crimes with minors.[100] The *Browne* court specifically distinguished its decision from the Fourth Circuit case *Hassan*'s choice to authenticate Facebook pages with the Rule 902(11) exception for self-authentication.[101] The government in *Browne* argued that Facebook message logs, provided by Facebook and authenticated with Facebook's records custodian, fell under the "records of regularly conducted activity" business records exception to hearsay.[102] The court concluded that Facebook chat logs are not records of a regularly conducted activity under Rule 803(6) and therefore did not qualify under Rule 902(11).[103]

The *Browne* court is specific about its determination that Facebook chat logs should not qualify under Rule 902(11), reasoning that the relevance of the Facebook records in this case "hinge[d] on that fact of authorship."[104] Specifically, the court pointed out that the government was "required to introduce enough evidence such that the jury could reasonably find, by a preponderance of the evidence, that Browne and the victims authored the Facebook messages at issue."[105] However, the government in *Browne* only provided the records custodian from Facebook who simply attested to the fact that the communications took place as alleged between the named Facebook pages.[106] The court explained that if it accepted this explanation as enough for self-authentication of the Facebook chat logs, that would "amount to holding that social media evidence need not

---

99 *Browne*, 834 F.3d at 413 n.8.
100 *See id*.
101 *Id*.
102 *Id*. at 409.
103 *Id*.
104 *Id*. at 410.
105 *Id*.
106 *Id*.

be subjected to a 'relevance' assessment prior to admission."[107] Additionally, the court pointed out that the Second Circuit and the First Circuit both have adopted the same interpretation for evidence, digital and non-digital.[108] Furthermore, the Third Circuit stated that self-authentication for the Facebook message log in *Browne* failed for another reason: it was predicated on an incorrect interpretation of the business records exception.[109] The court explained that the business records exception is "designed to capture records that are likely accurate and reliable in content, as demonstrated by the trustworthiness of the underlying sources of information and the process by which and purposes for which that information is recorded."[110] Facebook itself did not verify the substantive contents of the communications between the victims and the defendant; it instead could only verify certain aspects of the communications, such as the time the communications took place, between which Facebook accounts the communications took place, and the dates that the communications occurred.[111]

The Third Circuit in *Browne* challenged a perception regarding technology and authentication. That perception is that technology is inherently more reliable because it is automated and occurs without human error. While that may be true in some contexts, it should not be relied on by attorneys in the process of authenticating social media evidence. The government desired to confirm that the Facebook account that sent the incriminating messages to the victims belonged to and was owned by the defendant in *Browne*.[112] However, the government naively relied on Facebook's records custodian to verify the authenticity of the true identities behind the Facebook account's owners under Rule 902(11) and 803(6), when the records custodian could only be used to verify things like timestamps on the Facebook chats or other similar technical information.[113] It appears, then, that the government and the district court in *Browne* overlooked the po-

---

107 *Id*.

108 *Id*.; *See also* United States v. Voyner, 769 F.3d 125, 132 (2d Cir. 2014).

109 *Browne*, 834 F.3d at 410.

110 *Id*.

111 *Id*. at 410-11.

112 *Id*.

113 *Id*. at 411.

tential inaccuracy that can occur on technical platforms, such as Facebook. In fact, the Third Circuit confirmed that if it were to accept the original method of authentication, that would mean that "all electronic information whose storage or transmission could be verified by a third-party service provider would be exempt from hearsay rules,"[114] which is a proposition that it could not accept. The *Browne* court later affirmed authentication of the Facebook chat logs under a different rule with the use of extrinsic evidence; however, the opinion still offers important analysis and provides a diametrically opposed approach from the Fourth Circuit's *Hassan* self-authentication method under Rule 902(11).[115]

2. *Identifying Features Linking the Owner to the Messages*

Another way to authenticate Facebook messages is with the use of identifying factors of the alleged owner and author of the messages as foundation.[116] In the Tenth Circuit case *United States v. Brinson*, the defendant was convicted of engaging in sex trafficking of children and other related charges, in part with the use of Facebook messages.[117] The defendant in *Brinson* argued that the Facebook messages were inadmissible hearsay.[118] The court disagreed and confirmed the trial court's decision in accepting the Facebook messages, stating that a Facebook message was offered "against a party and is that party's own statement," which is an exception to hearsay.[119] At trial, the government linked the defendant to the Facebook account that sent the Facebook messages by showing that the pseudonym "Twinchee Vanto" belonged to the defendant.[120] Specifically, the government established a connection between the defendant and the pseudonym through an email account, self-identification, and his phone number.[121] While this falls outside of the typical authentication analysis that has been discussed in this comment with regard to social media evidence, it presents a scenario that a family

---

114 *Id*.
115 *See id*. at 415 (3d Cir. 2016).
116 *See* United States v. Brison, 772 F.3d 1314 (10th Cir. 2014).
117 *See id*.
118 *Id*. at 1317.
119 *Id*. at 1320 (citing FED. R. EVID. 801(d)(2)(A)).
120 *Id*. at 1320-21.
121 *Id*.

law attorney may run into in practice. This is especially true because someone committing a sex crime with a minor over the internet would not be inclined to use his or her real name.

3. *When an Acquaintance of the Defendant Testifies to the Authenticity of Facebook Messages*

Returning to the concept of authentication supported by testimony, another method utilized by the Fifth Circuit in *United States v. Barnes* is testimonial support from an acquaintance of the defendant in the case.[122] In *Barnes*, the defendant was charged with intent to distribute a number of illegal drugs and conspiracy to possess a firearm in furtherance of a drug trafficking crime.[123] As part of the evidence brought against the defendant, the government provided Facebook messages and introduced them under Federal Rule of Evidence 901.[124] As support for admitting the Facebook messages, the court accepted testimony from an acquaintance who testified to seeing the defendant use Facebook.[125] The witness also testified that she recognized the defendant's Facebook account and that the messages "matched [the defendant's] manner of communicating."[126] However, the witness was "not certain that [the defendant] had authored the messages."[127]

The court, though, pointed out that admission of evidence does not require conclusive proof of authenticity.[128] It also stated that regardless of potential error in admitting the Facebook message, the admission would have been "harmless" because the messages were (1) about drug transactions and were therefore relevant to all charges and (2) "the content of the messages was largely duplicative" of what numerous witnesses testified to directly.[129] Thus the challenge of authentication did not warrant reversal and was without merit.[130] The *Barnes* court

---

122 *See* United States v. Barnes, 803 F.3d 209 (5th Cir. 2015).
123 *Id*.
124 *Id*. at 217.
125 *See id*.
126 *Id*. at 217.
127 *Id*.
128 *Id*.
129 *Id*. at 218.
130 *Id*.

did not provide specific information about how the Facebook messages were accessed, but it did confirm that bringing in an acquaintance with limited knowledge is sufficient for authentication in the Fifth Circuit.[131] The standard for authentication in the *Barnes* decision is seemingly low, putting it at risk for abuse. However, the court seems to consider the additional "duplicative" testimonies significant in its decision not to reverse the decision on authentication.[132]

IV. Private Social Media Evidence

Active social media users are familiar with the concept of making their published information "private" or "public."[133] Whether a piece of social media evidence is publicly or privately accessed will affect the process of authenticating the evidence. For example, Facebook allows users to customize their settings to keep anyone but their Facebook "friends" from seeing their published information.[134] Evident by the previous section, information that is public on social media websites, such as a public post on Facebook, is generally regarded as open for use by the court.[135] On the other hand, social media websites often have privacy settings where users intentionally allow only certain individuals or even a single individual to view their content. If a family law attorney wants to access private social media evidence for a case, the approach to authentication departs greatly from public information that can be downloaded and printed for the court.

A. *The Stored Communications Act and Social Media*

The Stored Communications Act can create barriers for attorneys attempting to access important social media evidence for their clients.[136] Specifically, the Stored Communications Act, in conjunction with Facebook policies, prohibits Facebook from providing contents of a social media account to a non-governmental entity, even if the party requesting the information has a

---

131 *See id*.
132 *Id*. at 218.
133 Stored Communications Act, 18 U.S.C. §§ 2701-2712.
134 *See* FACEBOOK, www.facebook.com.
135 Fawcett v. Altieri, 960 N.Y.S.2d 592 (Sup. 2013).
136 Stored Communications Act, 18 U.S.C. §§ 2701-2712.

valid subpoena or court order.[137] This is important and relevant to family law practitioners because if there is pertinent information in an opposing party's Facebook account, there are significant challenges in accessing that private data as a non-governmental entity. For example, a dissolution proceeding can involve an individual who is aware of pertinent information held on the Facebook account of his or her spouse. The Facebook account may have messages or posts affirming the existence of an additional bank account or other assets relevant to the dissolution. In *Bower v. Bower* in the federal district court of Massachusetts, a father with full custody of his children subpoenaed the email provider for his spouse in relation to the custody of their children.[138] However, even with a civil subpoena, the Stored Communication Act prohibited the father from gaining his spouse's email data. The court stated, "pursuant to § 2703, governmental entities may require the disclosure of the contents of customers' electronic communications or subscriber information in the context of ongoing criminal investigations, but no similar authority is granted to civil litigants."[139] This scenario in a dissolution could create devastating results for a party seeking alimony or an equitable division of assets.

Fortunately for family law practitioners and other civil litigators, there are a number of exceptions available under the Stored Communications Act. Most importantly, the electronic communication may be disclosed if there is "the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service."[140] Therefore, if the spouse seeking dissolution was the intended recipient of the message or is able to gain consent from the individual or addressee who received the message, then the evidence may be accessed via the spouse or relevant individual. This may still prove difficult, though, since the recipient of the electronic communication may not want to aid the other party of the dissolution. Another relevant exception is a disclo-

---

137 John G. Browning, *Digging for the Digital Dirt: Discovery and Use of Evidence from Social Media Sites*, 14 SMU SCI. & TECH. L. REV. 465 (2011)(citing 18 U.S.C.A. § 2702).

138 Bower v. Bower, 808 F. Supp. 2d 348, 349 (D. Mass. 2011).

139 *Id*. at 350.

140 18 U.S.C. § 2702(b)(3).

sure required by an emergency.[141] The U.S. District Court for the District of Massachusetts specifically stated that investigation of a kidnapping was an intended emergency exception under the Stored Communications Act.[142] Due to the nature of custody cases in family law, this may present itself as a useful exception should there be an issue of kidnapping within a custody battle following dissolution.

V. Ethical Concerns: Authentication

The low standard for authenticity has been critiqued throughout this Comment. The Advisory Committee Note to Federal Rule of Evidence 901 specifically addresses the criticisms of "the common law approach to authentication of documents" and observes that it presents "only a slight obstacle to the introduction of forgeries."[143] Surprisingly, it appears that the Advisory Committee does not consider forgery to be a significant obstacle, but rather, only a "slight one."[144] The idea of forgery in the process of authentication is addressed once more under the Advisory Committee Note for Federal Rule of Evidence 902 when it states "forgery is a crime and detection is fairly easy and certain."[145] Again, the Advisory Committee expresses little concern for forgery in the process of authentication.

Colin Miller and Charles White argue that this assumption by the Advisory Committee stems from a "multitude of cases in which handwriting experts testify that 'forgeries [a]re easy to detect' and that these experts utilize "computer-based handwriting analysis systems" which are "capable of detecting 100% of random and simple forgeries."[146] While this technical system may provide reassurance regarding the prevention of forgery in handwriting, most social media platforms utilize uniform fonts for publication on posts and messages. Thus, it is more difficult to

---

141 *Id*. at § 2702(c)(4).

142 *In re* Application of U.S. for a Nunc Pro Tunc Order for Disclosure of Telecommunications Records, 352 F. Supp. 2d 45 (D. Mass. 2005).

143 FED. R. EVID. 901 advisory committee note.

144 *Id.*

145 FED. R. EVID. 902 advisory committee note.

146 Colin Miller & Charles White, *The Social Medium: Why the Authentication Bar Should Be Raised for Social Media Evidence*, 87 TEMP. L. REV. ONLINE 1 (2014).

stay comfortable in the assumption that forgery risk is low and "easy" to detect and ascertain. For example, any individual with a computer connected to the internet is able to make a Facebook page after answering a series of biographical questions.[147] Curiously, the Advisory Committee does not seem to consider or address this problem. Based on the caselaw discussed in this Comment, authentication typically requires an individual who simply knows and can identify the defendant, like in *Thomas*, or who can cross-authenticate photos based on expertise such as "gang intelligence," like in *Parker*, in order to bring in posts and photographs on social media.[148] Arguably then, in some cases it would be plausible for forged social media evidence to be authenticated fairly easily. Therefore, it is interesting to see the relaxed interpretation of Rules 901 and 902 across the board, even with the potential risks within social media. It may be that with the advancement of technology, this will change. The following section addresses Artificial Intelligence and its possible influence on digital forgery.

A. *Ethical Concerns: Artificial Intelligence and Forgery*

Family law attorneys should be prepared to consider the implications of technological advancement on their practices. In fact, the American Bar Association Rules of Professional Conduct Rule 1.1 states that an attorney must be competent, which "requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."[149] Further, comment 8 under Rule 1.1 specifically states that "to maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology."[150] The degree of technological competence will change as technology develops

---

147 *How Do I Create a Facebook Account?*, FACEBOOK, https://www.facebook.com/help/188157731232424?helpref=topq (last visited July 24, 2020).

148 *See also Thomas*, 701 Fed. Appx. 414; *Parker*, 871 F.3d 590.

149 MODEL CODE OF PROF'L RESPONSIBILITY r. 1.1 (2020).

150 *Id*. at Cmt. 8; *See also* Robert W. Nelson, *Ethical Obligations of Family Law Attorneys in Dealing with Social Media and Discovery*, 31 J. AM. ACAD. MATRIM. LAW. 415 (2019).

and begins to perform more advanced functions.[151] One of those advanced functions that is becoming more prevalent in society is the use of artificial intelligence (AI).[152] *Forbes* magazine's Neil Sahota published an article questioning whether AI will make lawyers obsolete, in which he commented, "AI could be used to conduct time-consuming research, reducing the burdens on courts and legal services and accelerating the judicial process."[153] However, AI also brings with it ethical concerns that Sahota outlines such as unconscious bias which can create biased AI.[154]

1. *Artificial Intelligence: "Deepfakes"*

"Deepfakes" are a creation of artificial intelligence.[155] Specifically, deepfakes are "false yet highly realistic" media that can appear in the form of a photo or video.[156] Deepfakes are a portmanteau of the word "deep learning" and "fake" and are characterized by the use of deep-learning algorithm, automated creation, and the "potential to deceive."[157] With the use of artificial intelligence and a home computer, a deepfake can be created in a matter of hours after training an algorithm with a large data set, including images of the person whom the deepfake is meant to depict.[158] The most common forms of deepfake include the "face swap," in which "one person's face is digitally replaced with another."[159] For example, in the movie *Nymphomaniac*, the filmmakers utilized similar digital technology to transpose the faces of the actors, who did not perform pornographic scenes,

---

151 Tad Simons, *For a Lawyer, What Does "Technology Competence" Really Mean?*, THOMSON REUTERS LEGAL EXECUTIVE INST., (Apr. 20, 2018) https://www.legalexecutiveinstitute.com/lawyers-technological-competence/.

152 Neil Sahota, *Will A.I. Put Lawyers Out of Business?*, FORBES (Feb. 9, 2019), https://www.forbes.com/sites/cognitiveworld/2019/02/09/will-a-i-put-lawyers-out-of-business/#378f5748310.

153 *Id*.

154 *Id*.

155 Jason Chipman, Matthew Ferraro & Stephen Preston, *First Federal Legislation on Deepfakes Signed into Law*, JD SUPRA (Dec. 24, 2019), https://www.jdsupra.com/legalnews/first-federal-legislation-on-deepfakes-42346/.

156 *Id*.

157 Danielle Van Lier, *The People vs. Deepfakes*, 43 L.A. LAW. 16, 17 (May 2020).

158 *Id*. at 18.

159 *Id*.

onto the faces of people performing the pornographic scenes.[160] While this was beneficial for the actors in the movie who did not want to perform sexual acts on camera, the difference is that all actors in the movie gave their consent for the face swap.[161] On the other hand, victims of deepfake face swap technology typically do not consent to the use of their faces for those purposes.[162] The rise of this type of technology has created a need for legislation related to pornography and other forms of face swap.[163]

In 2019, Texas and California both created legislation prohibiting the creation of deepfakes that depict other individuals without their consent.[164] Further, President Trump signed the first federal law on December 20, 2019 involving deepfakes, named the National Defense Authorization Act for Fiscal Year 2020 (NDAA).[165] Section 5709 of the NDAA imposes a reporting requirement and notification provision on the Director of National Intelligence (DNI).[166] The DNI is required to submit to the Congressional Intelligence Committees an unclassified report on the potential national security impacts of deepfakes, which it refers to as "machine-manipulated media and machine-generated text."[167] Section 5709 also requires the DNI to report when it determines there is credible intelligence that a foreign entity is utilizing deepfakes against the political process within the United States.[168] Finally section 5724 addresses a deepfakes "competition," which outlines rewards given for development of technologies "to automatically detect machine-manipulated media."[169] Evidenced by the NDAA's concern with deepfakes and their effect on National Security, deepfakes are starting to be monitored and controlled by the law and the federal government. There-

---

160 *Id*.

161 *Id*.

162 *Id*.

163 Chipman et al., *supra* note 153.

164 *Id*.

165 National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92, § 5709, 133 Stat. 1198 (2019).

166 *Id*.

167 *Id*.

168 Chipman et al., *supra* note 153.

169 National Defense Authorization Act of 2020, Pub. L. No. 116-92, § 5724, 133 Stat. 1198 (2019).

fore, it is safe to assume that the U.S. government along with California and Texas feel threatened by deepfakes. Further, this growing concern will likely prove itself relevant in the practice of family law too, specifically with face swaps.

2. *The Legal Fight Against Child Pornography Depicted by Deepfakes*

For family law attorneys dealing with children and families directly, deepfakes present a disturbing danger because of face swaps.[170] In 2019, the Governor of Maryland signed a bill that expanded prohibition of child pornography to include computer-generated images.[171] The unfortunate reality of deepfakes is that they will be used for good and bad. When it comes to regulation of the bad, the caselaw is not yet sufficient. Furthermore, the Supreme Court declined to federally outlaw virtual child pornography in 2002.[172] In *Ashcroft v. Free Speech Coalition*, Anthony Kennedy argued in favor of allowing flexibility in freedom of speech under the First Amendment to the point that it protects virtual child pornography creations.[173]

While the protections of fundamental rights, such as freedom of speech, should be protected, there are dangers in allowing absolutism in the technological age. For example, the idea that any person could create and distribute child pornography with the depiction of a minor's actual face is concerning to say the least. Additionally, it is important for the federal government to weigh the interest of absolute free speech against the interest of protecting children's individuality and privacy from obscene creations. Fortunately, it appears that the federal government and some state governments have come to the same conclusion about the danger of deepfakes and have begun to create legislation against them.[174] It is important for attorneys of all kinds to keep up with these changes as they come so that they

---

170 *See In re* S.K., 215 A.3d 300, 315 n.22 (Md. Ct. App. 2019)(discussing House Bill 1027 in Maryland which specifically expanded the prohibition of child pornography to include computer-generated images).

171 *Id*.

172 *See* Ashcroft v. Free Speech Coalition, 122 S.Ct. 1389 (2002).

173 *Id*. at 1393.

174 Chipman et al. *supra* note 153.

can formulate an opinion and understanding of technology, such as deepfakes, and advocate to eliminate dangers that they create.

VI. Conclusion

Authentication is a key step in bringing important social media evidence into a lawsuit. The caselaw discussed in this comment supports the notion that authentication is fairly easy to achieve under the Federal Rules of Evidence. This low standard is beneficial to family law attorneys because it can help families and children submit evidence to find justice in their cases. On the other hand, this standard can be harmful for a family law attorney trying to help juvenile defendants if negatively impacting evidence is too easily authenticated, when it is not in fact authentic. Overall, an important takeaway for the future of authentication and social media is that technology is evolving and challenges in authentication may grow as technology, like AI-powered face swaps, become more available and manipulated by people. Further, with the rise of social media use in 2020 because of COVID-19,[175] it logically follows that there will be more social media publications showing up in lawsuits. Therefore, an attorney practicing family law would be wise to turn her attention towards the challenges and changes to come with authentication of social media and other forms of digital evidence.

Yasmin Herdoiza

---

175 Ryan Holmes, *Is COVID-19 Social Media's Levelling Up Moment?*, FORBES (Apr. 24, 2020), https://www.forbes.com/sites/ryanholmes/2020/04/24/is-covid-19-social-medias-levelling-up-moment/#49c350636c60 (last visited July 24, 2020).