University of Baltimore Law Forum

Volume 42
Number 2 *Spring 2012*

Article 3

2012

What Happens on Myspace Stays on Myspace: Authentication and Griffin v. State

Mark C. Kopec

ARTICLE

WHAT HAPPENS ON MYSPACE STAYS ON MYSPACE: AUTHENTICATION AND *GRIFFIN V. STATE*

By: Mark C. Kopec

This Article discusses authentication of social media evidence and focuses on the recent Court of Appeals of Maryland decision in *Griffin v. State*.[1] *Griffin* was a split-decision in a case of first impression in Maryland.[2] The majority held that certain social media requires a greater degree of authentication than non-electronic evidence because of "the potential for abuse and manipulation of a social networking site by someone other than its purported creator and/or user."[3] The court described three "authentication opportunities" and stated that possible avenues "will, in all probability, continue to develop as the efforts to evidentially utilize information from the [social media] sites increases."[4] These authentication opportunities are explored below, and *Griffin*'s application to other factual scenarios is discussed.

I. MYSPACE

Griffin involved an account on Myspace, a social networking website.[5] In order to create a free account on myspace.com,[6] a user must fill in information for first and last name, provide an email address, choose a password, enter a birth date, and indicate gender.[7] The user is then given an opportunity to upload a photo.[8] The site automatically sets your location based on the location of the computer used to create the account, but the information can be changed.[9] Additionally, a country and state

---

[1] Griffin v. State, 419 Md. 343, 19 A.3d 415 (2011).

[2] *See id.* at 351, 19 A.3d at 420.

[3] *Id.* at 357, 19 A.3d at 424.

[4] *Id.* at 363, 19 A.3d at 427 (citing Katherine Minotti, Comment, *The Advent of Digital Diaries: Implications of Social Networking Web Sites for the Legal Profession*, 60 S.C. L. REV. 1057 (2009)).

[5] MYSPACE, http://www.myspace.com/Help/AboutUs?pm_cmp=ed_footer (last visited Feb. 19, 2012); *see also* United States v. Drew, 259 F.R.D. 449, 453 (C.D. Cal. 2009) (citing testimony of a Myspace executive describing Myspace as "a social networking" website).

[6] *See* MYSPACE, https://www.myspace.com/signup (last visited Feb. 19, 2012) (click on the "Sign up free" hyperlink located on the right side of the webpage).

[7] *Id.*

[8] *See Drew*, 259 F.R.D. at 453-55 (detailing procedures to become a member through testimony of a Myspace executive).

[9] *See* MYSPACE, http://www.myspace.com/my/settings/profile/basicinfo (last visited Mar. 2, 2012).

must be selected from drop down menus, but anything can be listed as the town, real or fictional.[10]

In fact, all of a user's identifying information can be fictional. The fields for first and last name must be filled in, but the information entered does not have to be accurate. Nicknames can be used. The fields will accept anything, including gibberish. Anyone who possesses the requested information about another person can create an account purporting to be that person.[11]

Once an account is created, the user gets a page on the website.[12] The user can then post different types of content on the page, including statements, photos, and links to other websites.[13] A user can become "friends" with other users.[14] Those "friends" also can post items on the user's page.[15] Myspace has privacy settings that allow users to limit access to their personal pages only to their "friends," while excluding the general public.[16] Users who are "friends" with one another can also send private messages between themselves, which works just like email.[17]

Myspace was founded in 2003.[18] Prior to the advent of social media, the court in *St. Clair v. Johnny's Oyster & Shrimp, Inc.* provided an often-cited early commentary on the "inherently untrustworthy" nature of information on the Internet in the context of electronic evidence.[19] In *St. Clair*, the plaintiff attempted to introduce a printout from the United States Coast Guard online vessel database to prove the defendant's ownership of a boat.[20] The court rejected that evidence, stating:

> Plaintiff's electronic "evidence" is totally insufficient to withstand Defendant's Motion to Dismiss. While some look to the Internet as an innovative vehicle for communication, the Court continues to warily and wearily view it largely as one large

---

[10] *See id.*

[11] *Griffin*, 419 Md. at 352-53, 19 A.3d at 421 (citing Nathan Petrashek, Comment, *The Fourth Amendment and the Brave New World of Online Social Networking*, 93 MARQ. L. REV. 1495, 1499-1500 (2009-2010) (evaluating whether social networking users maintain a reasonable expectation of privacy in their online activity such that the police would require a warrant to search that activity)).

[12] *See* MYSPACE, http://www.myspace.com/pages/privacysettings?pm_cmp=ed_footer (last visited Feb. 20, 2012).

[13] *Id.*

[14] *Id.*

[15] *Id.*

[16] *Id.*

[17] MYSPACE, http://www.myspace.com/guide/im (last visited Mar. 2, 2012).

[18] John S. Wilson, Comment, *Myspace, Your Space, or Our Space? New Frontiers in Electronic Evidence*, 86 OR. L. REV. 1201, 1222 (2007) (citing MYSPACE – WIKIPEDIA, http://en.wikipedia.org/wiki/MySpace (last visited Apr. 11, 2008)).

[19] St. Clair v. Johnny's Oyster & Shrimp, Inc., 76 F. Supp. 2d 773, 774 (S.D. Tex. 1999).

[20] *Id.*

> catalyst for rumor, innuendo, and misinformation. So as to not mince words, the Court reiterates that this so-called Web provides no way of verifying the authenticity of the alleged contentions that Plaintiff wishes to rely upon in his Response to Defendant's Motion. There is no way Plaintiff can overcome the presumption that the information he discovered on the Internet is inherently untrustworthy. Anyone can put anything on the Internet. No web-site is monitored for accuracy and *nothing* contained therein is under oath or even subject to independent verification absent underlying documentation. Moreover, the Court holds no illusions that hackers can adulterate the content on *any* web-site from *any* location at *any* time. For these reasons, any evidence procured off the Internet is adequate for almost nothing, even under the most liberal interpretation of the hearsay exception rules found in FED.R.CIV.P. 807.[21]

While our society's acceptance of, and reliance on, the Internet has increased greatly since the 1999 *St. Clair* decision, similar concerns continue with social media. One tragic example involving creation of a fictional profile on MySpace occurred in *U.S. v. Drew*.[22] There, the defendant was the mother of a 13-year-old girl.[23] The defendant created a page on MySpace for a fictional 16-year-old boy, named him "Josh Evans," and a posted a photograph of a boy without that boy's knowledge.[24] The defendant used the fictional profile to contact one of her daughter's female classmates and flirted with her over a number of days.[25] Then, the defendant had "Josh" inform the classmate that he was moving away, and told the classmate that "the world would be a better place without her in it."[26] That same day, the classmate killed herself.[27]

An anonymous identity can also conceal financial interests that are behind information placed on the Internet. For example, the Chief Executive Officer of Whole Foods Market created an identity called "Rahodeb" and posted over 1,100 times to an online financial bulletin board over a 7-year period, often championing his company's stock and occasionally blasting his company's rival, Wild Oats Market.[28]

---

[21] *Id.* at 774-75 (emphasis in original).

[22] *Drew*, 259 F.R.D. at 452.

[23] *Id.* at 452.

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] *Id.* The defendant's conviction under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, was overturned based on a violation of the void-for-vagueness doctrine. *Id.* at 463-64.

[28] Andrew Martin, *Whole Foods Executive Used Alias*, N.Y. TIMES, Jul. 12, 2007, *available at* http://www.nytimes.com/2007/07/12/business/12foods.html?scp=1&sq=whole%20foods%20executive%20used%20alias&st=cse.

As the use of email expanded, it became increasingly sought by parties in litigation, in part because of the casual and candid manner in which people use email. The same thing is happening with social media. Social media sites like Myspace and Facebook have hundreds of millions of users.[29] A party's page may contain a statement or picture that is inconsistent with a position taken by the party in litigation, or consistent with an opponent's position. It can happen in every type of civil or criminal case. The issues discussed in this article are arising in litigation with ever-increasing frequency.

II. *GRIFFIN V. STATE*

In April 2011, the Court of Appeals of Maryland decided *Griffin v. State,*[30] in which the defendant, Griffin, was on trial for a shooting death.[31] During the trial, the prosecution sought to introduce pages printed from what it contended was Griffin's girlfriend's Myspace page.[32] The purpose was to provide corroboration of the testimony of a prosecution witness that, prior to trial, the witness was threatened by the defendant's girlfriend, Jessica Barber.[33]

Barber's Myspace profile was under the name "Sistasouljah."[34] The printed pages from the profile described her as a 23-year-old female from Port Deposit with a birthday of 10/2/1983, and contained a photograph of a male and female.[35] The printed pages also contained the following statement: "FREE BOOZY!!!! JUST REMEMBER SNITCHES GET STITCHES!! U KNOW WHO YOU ARE!!"[36]

Ms. Barber was called as a witness at trial by the prosecution, but was not questioned about the Myspace printed pages.[37] Instead, the prosecution attempted to authenticate the printed pages through the testimony of an investigating police officer.[38] After the defense objected,

---

[29] *See* FACEBOOK, http://newsroom.fb.com/content/default.aspx?NewsAreaId=22 (last visited Feb. 28, 2012) (noting that, on average, at the end of December 2011, Facebook had 845 million monthly active users and 483 million daily active users); *see also* Melissa Bell, *Facebook and MySpace joint announcement: MySpace welcomes Facebook users*, WASH. POST BLOG (Nov. 18, 2010, 12:18 PM), http://voices.washingtonpost.com/blog-post/2010/11/facebook_and_myspace_joint_ann.html (explaining that in 2007, MySpace was the reigning social network startup with 180 million registered users, but that number shrunk to 100 million in February 2010).

[30] *Griffin*, 419 Md. at 343, 19 A.3d at 415.

[31] *Id.* at 348, 19 A.3d at 418.

[32] *Id.*

[33] *Id.* at 348-49, 19 A.3d at 418-19.

[34] *Id.* at 348, 19 A.3d at 418.

[35] *Id.*

[36] *Griffin*, 419 Md. at 348, 19 A.3d at 418.

[37] *Id.*

[38] *Id.*

the officer testified outside the presence of the jury that he believed the Myspace page belonged to Ms. Barber because of the photograph of her and the defendant on the front, the reference to the defendant, and her birth date on the page.[39]

The following exchange took place between the trial judge and the prosecutor:

> Court: On its face, there is no way that you can conclude that on its face this establishes anything in regard to [the witness]. What it's being offered for, as I understand it, is corroboration, consistency that she's making a statement in a public forum, "snitches get stitches." And I guess the argument is going to be made that that's consistent with what [the witness] said, that she threatened him.
>
> [Prosecutor]: That's correct.
>
> Court: It's weak. I mean, there's no question it's weak, but that's what it is offered for.[40]

The trial judge permitted the testimony and the defense entered into a stipulation, in lieu of the testimony, while maintaining an objection.[41] A jury ultimately convicted Griffin of second-degree murder and other related charges.[42] The Court of Special Appeals of Maryland held that the trial judge did not abuse his discretion in admitting the Myspace pages into evidence.[43]

The Court of Appeals discussed what is required to create a Myspace page, and generally how the site works. The court noted concerns that someone can create a fictitious account under someone else's name, or can gain access to another's account by obtaining the user's login information.[44] The court also discussed the *Drew* decision and observed, "[t]hus, the relative ease in which anyone can create fictional personas or gain unauthorized access to another user's profile, with deleterious consequences, is the *Drew* lesson."[45] The court stated, "[t]he potential for fabricating or tampering with electronically stored information on a social

---

[39] *Id.* at 349, 19 A.3d at 418-19.

[40] *Id.* at 349-50, 19 A.3d at 419.

[41] *Id.* at 350, 19 A.3d at 419.

[42] *Griffin*, 419 Md. at 343, 19 A.3d at 415.

[43] *Id.* at 346, 19 A.3d at 417; Griffin v. State, 192 Md. App. 518, 546, 995 A.2d 791, 808 (2010) *rev'd*, 419 Md. 343, 19 A.3d 415 (2011).

[44] *Griffin*, 419 Md. at 351-54, 19 A.3d at 420-22.

[45] *Id.* at 354, 19 A.3d at 421-22.

networking site, thus poses significant challenges from the standpoint of authentication of printouts of the site, as in the present case."[46]

Authentication is governed by Maryland Rule 5-901.[47] Subsection (a) provides:

> **General provision.** The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.[48]

Methods of authentication are illustrated in Rule 5-901(b).[49] The *Griffin* court stated that the applicable subsections were (b)(1) and (b)(4), which provide:

> (b) **Illustrations**. By way of illustration only, and not by way of limitation, the following are examples of authentication or identification conforming with the requirements of this Rule:
>
> (1) Testimony of witness with knowledge. Testimony of a witness with knowledge that the offered evidence is what it is claimed to be.
>
> (4) Circumstantial evidence. Circumstantial evidence, such as appearance, contents, substance, internal patterns, location, or other distinctive characteristics, that the offered evidence is what it is claimed to be.[50]

The Court of Appeals looked to the widely cited discussion of authentication of electronically stored evidence by Magistrate Judge Paul W. Grimm in *Lorraine v. Markel Am. Ins. Co.*,[51] in which he noted that authenticating electronically stored information presents a myriad of concerns because "technology changes so rapidly."[52] Judge Grimm also noted that the "complexity" or "novelty" of electronically stored information, with its potential for manipulation, requires greater scrutiny of the "foundational requirements" than paper records to bolster reliability.[53]

---

46 *Id.*

47 MD. R. 5-901. The federal counterpart is FED. R. EVID. 901.

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

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

50 *Griffin*, 419 Md. at 355, 19 A.3d at 422.

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

52 *Id.* at 544.

53 *Id.* at 543-44 (quoting WEINSTEIN & BERGER, WEINSTEIN'S FEDERAL EVIDENCE § 900.06[3] (2d. ed. 1997)).

In its reversal, the Court of Appeals held that the Court of Special Appeals had "failed to acknowledge the possibility or likelihood that another user could have created the profile in issue or authored the 'snitches get stitches' posting."[54] The Court of Appeals explained its ruling:

> We agree with Griffin that the trial judge abused his discretion in admitting the MySpace evidence pursuant to Rule 5-901(b)(4), because the picture of Ms. Barber, coupled with her birthdate and location, were not sufficient "distinctive characteristics" on a MySpace profile to authenticate its printout, given the prospect that someone other than Ms. Barber could have not only created the site, but also posted the "snitches get stitches" comment. The potential for abuse and manipulation of a social networking site by someone other than its purported creator and/or user leads to our conclusion that a printout of an image from such a site requires a greater degree of authentication than merely identifying the date of birth of the creator and her visage in a photograph on the site in order to reflect that Ms. Barber was its creator and the author of the "snitches get stitches" language.[55]

A. Rule 5-104(b)

The court declined to address authentication under Maryland Rule 5-104(b), stating:

> Federally, some of the uncertainty involving evidence printed from social networking sites has been addressed by embracing the notion of "conditional relevancy," pursuant to Federal Rule 104(b), which provides "[w]hen the relevancy of evidence depends upon the fulfillment of a condition of fact, the court shall admit it upon, or subject to, the introduction of evidence sufficient to support a finding of the fulfillment of the condition." In this way, the trier of fact could weigh the reliability of the MySpace evidence against the possibility that an imposter generated the material in question. *See Lorraine v. Markel American Insurance*, 241 F.R.D. 534, 539-40 (2007). Maryland Rule 5-104(b) establishes a nearly identical protocol; we,

---

[54] *Griffin*, 419 Md. at 357, 19 A.3d at 423 (quoting *Griffin*, 192 Md. App. At 543, 995 A.2d at 806).

[55] *Id.* at 357-58, 19 A.3d at 423-24. The court recognized that other courts have suggested that greater scrutiny is appropriate for authentication of electronically stored information on social networking sites because of the heightened possibility for manipulation by other than the true user or poster. *Id.* at 358, 19 A.3d at 424 (discussing Commonwealth v. Williams, 926 N.E. 2d 1162 (Mass. 2010); People v. Lenihan, 911 N.Y.S.2d 588 (N.Y. Sup. Ct. 2010); United States v. Jackson, 208 F.3d 633 (7th Cir. 2000)).

> however, have not been asked been asked in this case to address the efficacy of the Rule 5-104(b) protocol.[56]

Professor McLain wrote in her treatise on Maryland Evidence that "Md. Rule 5-901(a), consistent with prior Maryland case law, establishes that the standard of proof is the same as is found in Md. Rule 5-104(b) for facts on which the relevance of an item is conditioned."[57] It therefore appears that the *Griffin* analysis under Rule 5-901(a) may also apply under 5-104(b).

III. *GRIFFIN* DISSENT

Judge Harrell wrote a dissenting opinion, joined by Judge Murphy, who is the author of another Maryland evidence treatise, *Maryland Evidence Handbook*.[58] The dissent noted that Maryland Rule 5-901 derives from Federal Rule of Evidence 901, and that federal cases construing the federal rule are "almost direct authority impacting construction ... of an [analogous Maryland Rule]."[59] The dissent relied on federal cases in which courts held that "a document is properly authenticated if a *reasonable juror could find in favor of its authenticity*."[60] The dissent noted that, although the Court of Appeals had not previously enunciated such a standard, it is consistent with Maryland Rule 5-901's requirement of "evidence sufficient to support a finding that the matter in question is what its proponent claims."[61] The dissent stated:

> Applying that standard to the present case, a reasonable juror could conclude, based on the presence of the MySpace profile of (1) a person appearing to [the investigating officer] to be Ms. Barber posing with the defendant, her boyfriend; (2) a birthdate matching Ms. Barber's; (3) a description of the purported creator of the MySpace profile as being a twenty-three year old from Port Deposit; and (4) references to freeing "Boozy" (a nickname for the defendant), that the redacted printed pages of the MySpace profile contained information posted by Ms. Barber.[62]

The dissent acknowledged the concern that someone other than Ms. Barber could have accessed or created the account, and have posted the

---

[56] *Griffin*, 419 Md. at 365 n.15, 19 A.3d at 428 n.15.

[57] *Id.* at 367 n.2, 19 A.3d at 429 n.2 (Harrell, J., dissenting) (quoting LYNN MCLAIN, MARYLAND EVIDENCE § 901:1 (2001)).

[58] JOSEPH F. MURPHY, JR., MARYLAND EVIDENCE HANDBOOK (4th ed. 1999).

[59] *Griffin*, 419 Md. at 365-66, 19 A.3d at 428-29 (Harrell, J., dissenting).

[60] *Id.* at 366, 19 A.3d at 429 (Harrell, J., dissenting) (emphasis in original) (internal citations omitted).

[61] *Id.* (emphasis in original).

[62] *Id.* at 367, 19 A.3d at 429 (Harrell, J., dissenting).

threatening message, but stated that the record suggested no motive to do so.[63] The dissent felt that such concerns went not to the admissibility of the Myspace page printouts under Rule 5-901, but rather to the weight to be given by the trier of fact.[64] The dissent added:

> It has been said that the "purpose of authentication is to...filter untrustworthy evidence." Like many filters that are unable to remove completely all impurities, Rule 5-901 does not act to disallow any and all evidence that may have impurities (i.e., in this case evidence that could have come, conceivably, from a source other than the purported source). As long as a reasonable juror could conclude that the proffered evidence is what its proponent purports it to be, the evidence should be admitted. The potentialities that are of concern to the Majority Opinion are fit subjects for cross-examination or rebuttal testimony and go properly to the weight the fact-finder may give the print-outs.[65]

IV. MAJORITY V. DISSENT

One court has suggested that electronic evidence has the "same uncertainties" concerning authenticity as traditional documents, which can have forged signatures or be on a stolen letterhead, but it declined to create unique rules for electronic evidence.[66] There is a strong argument, however, that the opportunity and ease with which electronic evidence can be fabricated has led to substantially more widespread abuse in electronic media than with traditional documents. This includes digital photographs, which can be altered much more easily than traditional photographs developed from film.

These differing views are what divided the majority and dissent in *Griffin.* The majority has placed a greater burden on the authentication of printouts from social media sites than on traditional documents. In doing so, the court ensures that juries will not receive unreliable evidence that fails to meet this heightened standard.

Under the dissent's approach, the jury would receive the evidence upon a minimal showing from which it could be concluded that the evidence is authentic. An opponent of fabricated evidence would essentially have the burden shifted to him to prove the fabrication. Depending on the facts of an individual case, the opponent of the

---

[63] *Id.* at 367, 19 A.3d at 429-30 (Harrell, J. dissenting).

[64] *Id.* at 367, 19 A.3d at 430 (Harrell, J., dissenting) (citing Hays v. State, 40 Md. 633, 648 (1874)).

[65] *Griffin*, 419 Md. at 368, 19 A.3d at 430 (Harrell, J., dissenting) (internal citations omitted).

[66] *See In re* F.P., 878 A.2d 91, 95-96 (Pa. Super. Ct. 2005).

evidence may not have access to the same sources and evidence as the proponent in order to make such a showing. Meanwhile, all of this plays out in front of the jury in a potentially distracting sideshow. While this may be the usual process under Rule 5-104(b) when the jury has to decide admissibility, the area of social media evidence is likely to involve more instances of fabricated evidence. The majority's requirement of a greater degree of authentication for this type of evidence should reduce the number of such sideshows.

The tradeoff is that, under the majority's analysis, otherwise relevant and admissible social media evidence will be excluded if the heightened burden of authentication is not met. The methods of authentication discussed by the *Griffin* majority are discussed below. Some of the methods can be costly and time consuming, and there will be situations where parties do not have the resources to pursue them.

V. *GRIFFIN* METHODS OF AUTHENTICATION

The *Griffin* court stated that:

> [W]e should not be heard to suggest that printouts from social networking sites should never be admitted. Possible avenues to explore to properly authenticate a profile or posting printed from a social networking site, will, in all probability, continue to develop as the efforts to evidentially utilize information from the sites increases.[67]

The court added that a number of opportunities come to mind.[68] These are discussed below in reverse order as they appear in the majority's analysis.

A. Information from Social Networking Site

The *Griffin* court stated that one method "may be to obtain information directly from the social networking site that links the establishment of the profile to the person who allegedly created it and also links the posting sought to be introduced to the person who initiated it."[69] The court stated, "[t]his method was apparently successfully employed to authenticate a Myspace site in *People v. Clevenstine*."[70] In *Clevenstine*, the court described the testimony from Myspace: "[A] legal compliance officer for MySpace explained that the messages on the computer disk had been exchanged by users of accounts created by

---

[67] *Griffin*, 419 Md. at 363, 19 A.3d at 427.

[68] *Id.*

[69] *Id.* at 364, 19 A.3d at 428.

[70] *Id.* (citing People v. Clevenstine, 891 N.Y.S.2d 511 (N.Y. App. Div. 2009)).

defendant and the victims ..."[71] The basis for this statement is not provided in the *Clevenstine* opinion. It is possible that Myspace was able to demonstrate that the defendant's account was accessed by a computer using the Internet with the Internet Protocol ("IP") address that was assigned to the defendant, but that is not known. The *Clevenstine* court also relied on other evidence, as further discussed below.

There are hurdles, however, in obtaining information directly from the social networking site. Myspace and Facebook are the largest sites, and they are both located in California. Both sites can decline to voluntarily provide information, and have done so. Without voluntary cooperation, an out of state litigant must arrange for a California subpoena to be issued and properly served. In addition, any attempt to quash the subpoena may be heard by the California court that issued the subpoena.

Moreover, there may be a motion to quash the subpoena under the Stored Communications Act ("SCA").[72] In 2010, the U.S. District Court for the Central District of California held in a case of first impression that the SCA applies to social networking sites.[73] "The SCA prevents 'providers' of communication services from divulging private communications."[74] The court noted that the SCA was passed in 1986, before the advent of the World Wide Web.[75] The court observed that the "[SCA] is not built around clear principles that are intended to easily accommodate future changes in technology."[76] The court went through a lengthy analysis before quashing the subpoenas, finding that private messages and page postings that could only be viewed by "friends" were protected from discovery under the SCA.[77]

The SCA also contains a complex scheme allowing for disclosure of certain information in response to a subpoena issued by a governmental entity in connection with a criminal investigation or case.[78] The SCA's scheme does not apply in civil cases, and was not at issue in *Crispin*. It is not clear whether the scheme was invoked to obtain the Myspace representative's testimony in *Clevenstine*.

The *Crispin* decision will be an important precedent for issues involving application of the SCA to social networking sites, particularly when the dispute is heard in a California court that has jurisdiction over Myspace and Facebook. Presently, this method of pursuing

---

71 *Clevenstine*, 891 N.Y.S.2d at 514.
72 Stored Communications Act (SCA),18 U.S.C. § 2701 (2008).
73 Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 971-72 (C.D. Cal. 2010).
74 *Id.*
75 *Id.* at 971 n.15.
76 *Id.*
77 *Id.* at 991.
78 *Id.* at 974-75 (discussing 18 U.S.C. § 2703 (2009)).

authentication is likely to be the least attractive one, especially in civil litigation.

B. Computer Search

The second method "may be to search the computer of the person who allegedly created the profile and posting and examine the computer's internet history and hard drive to determine whether that computer was used to originate the social networking profile and posting in question."[79] The *Griffin* court noted that computer forensic firms could conduct such a search.[80] One complicating factor for this option is the variety of ways in which someone can create and use a social networking profile, like Myspace. It can be created or used on a computer or a smart phone. In addition, it can be created or used on devices owned by someone else, including a computer at the public library. Moreover, the creation of the profile might be done on one device, while the use occurs on another.

The *Griffin* court specified that the search would be to determine if the person's computer was used to create the profile and posting. In a case decided after *Griffin*, one court noted that someone other than the creator could use the profile because people "frequently remain logged in to their accounts while leaving their computers and cell phones unattended."[81] Given the emphasis by the *Griffin* court on the computer, and not the user, it appears that such an argument against authentication would fail in Maryland.

The *Griffin* court discussed the *Clevenstine* case in connection with the method of obtaining information directly from the social networking site. *Clevenstine* is discussed in this section of this Article because one of the facts not discussed in *Griffin* is that the defendant's wife in *Clevenstine* testified that she saw the Myspace instant messages at issue in the defendant's Myspace account while logged on to the computer they shared.[82]

In *Clevenstine*, the defendant was convicted of rape and other sexual crimes involving two teenage girls.[83] The defendant's wife found the saved instant message communications between the defendant and the younger victim, revealing sexually explicit discussions and indicating that the two had engaged in sexual intercourse.[84] The defendant contended

---

79 *Griffin*, 419 Md. at 363, 19 A.3d at 427.
80 *Id.* at 363-64, 19 A.3d at 427-28.
81 State v. Eleck, 23 A.3d 818, 822 (Conn. App. Ct. 2011).
82 *Clevenstine*, 891 N.Y.S.2d at 513.
83 *Id.* at 511.
84 *Id.* at 513.

that the instant messages were improperly admitted into evidence because they had not been properly authenticated.[85] The court held:

> Here, both victims testified that they had engaged in instant messaging about sexual activities with defendant through the social networking site MySpace, an investigator from the computer crime unit of the State Police related that he had retrieved such conversations from the hard drive of the computer used by the victims, a legal compliance officer for MySpace explained that the messages on the computer disk had been exchanged by users of accounts created by defendant and the victims, and defendant's wife recalled the sexually explicit conversations she viewed in defendant's MySpace account while on their computer. Such testimony provided ample authentication for admission of this evidence. Although, as defendant suggested at trial, it was possible that someone else accessed his MySpace account and sent messages under his username, County Court properly concluded that, under the facts of this case, the likelihood of such a scenario presented a factual issue for the jury.[86]

The wife's discovery of the messages on the computer she shared with the defendant is what one court called a "confirming circumstance."[87] That term is further explored below.

Once it appears that social media evidence is relevant to a case, practitioners will want to evaluate the option of searching the computer and smart phone devices that belong to the purported creator of the social media evidence at issue. In addition to the issues discussed above, it must be kept in mind that people can replace these devices on a frequent basis, whether it is due to wear and tear, to upgrade, to get the newest technology, or otherwise. Practitioners should keep in mind replacement issues when deciding when to conduct such a search, as the delay could be very costly.

C. Testimony by Creator

The *Griffin* court stated that the "first, and perhaps most obvious method would be to ask the purported creator if she indeed created the profile and also if she added the posting in question ..."[88] This corresponds under Rule 5-901(b)(1) to testimony of a witness with

---

[85] *Id.* at 514.
[86] *Id.* (internal citations omitted).
[87] Commonwealth v. Purdy, 945 N.E.2d 372, 380 (Mass. 2011).
[88] *Griffin*, 419 Md. at 363, 19 A.3d at 427.

knowledge that offered evidence is what it is claimed to be.[89] The court stated that "a witness with knowledge, such as Ms. Barber, could be asked whether the MySpace profile was hers and whether its contents were authored by her; she, however, was not subject to such inquiry when she was called by the State."[90]

In addition to being the most obvious method, asking the purported creator also is the method that can provide the most reliable evidence of authentication. The question is whether the purported creator created the evidence at issue. The best evidence is an admission by the creator under subsection (b)(1). By contrast, evaluation of circumstantial evidence under subsection (b)(4) can merely provide a picture from which it is hoped that authentication can be determined. While each case of circumstantial evidence will have to be evaluated on a case-by-case basis, cases involving an admission by the creator should result in easy authentication. Practitioners will therefore want to consider all of the discovery tools available in pursuing an admission by the creator of social media evidence. Methods will differ based on whether the purported creator is a party or non-party, and whether the proceeding is a civil or criminal one. Careful planning may be required to match available discovery tools with each of the steps in the process: discovering the existence of social media evidence; determining whether it is relevant; obtaining the actual social media evidence; and developing the evidence of authentication.

VI. APPLICATION OF *GRIFFIN* TO OTHER SOCIAL MEDIA SCENARIOS

The *Griffin* case involved a posting on a Myspace profile. However, the decision will be looked to for guidance in cases involving other social media scenarios under the Rule 5-901(b)(4) circumstantial evidence standard, such as private messages between two users. The *Griffin* court's discussion of two particular cases may be useful: One involved private Myspace messages that work like email; the other involved instant messages on an unspecified system.

The *Griffin* court discussed *Commonwealth v. Williams*[91] as an instance in which a court "suggested greater scrutiny [of social media] because of the heightened possibility for manipulation by other than the true user or poster."[92] In *Williams*, the Supreme Judicial Court of Massachusetts held that Myspace computer messages were not properly authenticated.[93] A prosecution witness testified that she was with the

---

89 *Id.*

90 *Id.* at 355 n.11, 19 A.3d at 422 n.11.

91 Commonwealth v. Williams, 926 N.E.2d 1162 (Mass. 2010).

92 *Griffin*, 419 Md. at 358, 19 A.3d at 424.

93 *Williams*, 926 N.E.2d at 1172.

defendant on the night of the murder, heard him speak on the phone with the victim, saw him display a gun before leaving, and then saw him return with a lot of money.[94] At trial, the witness testified that she received messages on MySpace from the defendant's brother urging her not to testify against the defendant, or to claim a lack of memory about the events.[95] The witness printed out the messages.[96] The printout showed a picture of the defendant's brother on the MySpace page, and that the username was "Doit4it," but the messages did not identify the sender by his or her given name.[97]

The witness responded to three of the messages received from the defendant's brother, and said that the defendant's brother sent messages back to her.[98] She did not respond to a fourth message.[99] The *Griffin* court did not discuss these facts, and the *Williams* opinion did not provide the details of the messages or responses.[100] The *Williams* court held that there was insufficient evidence to authenticate the Myspace messages:

> The contents of the messages demonstrate that the sender was familiar with [the witness] and the pending criminal cases against the defendant and desired to keep her from testifying.
>
> There was insufficient evidence to authenticate the messages and they should not have been admitted. Although it appears that the sender of the messages was using [defendant's brother's] MySpace Web "page," there is no testimony (from [the witness] or another) regarding how secure such a Web page is, who can access a MySpace Web page, whether codes are needed for such access, etc.... Here, while the foundational testimony established that the messages were sent by someone with access to [defendant's brother's] MySpace Web page, it did not identify the person who actually sent the communication. Nor was there expert testimony that no one other than Williams could communicate from that Web page. Testimony regarding the contents of the messages should not have been admitted.[101]

---

94 *Id.*
95 *Id.*
96 *Id.*
97 *Id.*
98 *Id.*
99 *Williams*, 926 N.E.2d at 1172.
100 *See Griffin*, 419 Md. at 358-60, 19 A.3d at 424-25; *see also Williams*, 926 N.E.2d at 1171-73 (discussing the authentication of the Myspace messages, but not the details of the messages).
101 *Williams*, 926 N.E.2d at 1172-73.

The other notable case is *In re F.P.*[102] The *Griffin* court distinguished the case because it involved instant messages between two persons, rather than postings on social media that could be viewed by anyone.[103] *In re F.P.* analyzed instant messages sent using an unidentified system.[104] The proceeding was an appeal from adjudication on aggravated assault by a delinquent.[105] The defendant argued that the trial court inappropriately admitted transcripts of instant messages between him and the victim, which occurred prior to the assault, and that the instant messages were not properly authenticated.[106]

The instant messages were between a user with the screen name "Icp4Life30" and "WHITEBOY Z 404."[107] The victim testified that his screen name was "WHITE BOY Z," that he printed the instant messages off of his computer, and that he believed that the other participant in the conversation was the defendant.[108] Defendant believed that the victim had stolen a DVD from him, and allegedly sent the victim messages saying he wanted to fight.[109] The court described the instant messages as follows:

> It appears that there are transcripts of several instant message "conversations" between [victim] and [defendant] on at least two different dates. In the first conversation, apparently taking place July 30, 2003 and initiated by [defendant], [victim] asks "who is this," and [defendant] replies, using his first name as it appears in the record. Throughout the transcripts, [defendant] threatens [victim] with physical violence and accuses [victim] of stealing from him. [Victim] states, "i got no reason to fight u and u got no reason to fight me[";] [defendant] answers, "ya i do. u stole off me." Later, [defendant] taunts [victim] and tells him to come over to his house; when [victim] states, "well i won't [sic] be there cuz [sic] i not fightin u[";] [defendant] replies, "well i am fightin u so when i see u ur [sic] dead."[110]

After receiving these instant messages, the victim notified his school counselor and social worker.[111] Defendant and the victim met with the school officials separately regarding the messages and the alleged theft.[112]

---

102 *In re* F.P., 878 A.2d 91 (Pa. Super. Ct. 2005).
103 *Griffin*, 419 Md. at 361, 19 A.3d at 426.
104 *Id.*
105 *In re F.P.*, 878 A.2d at 92.
106 *Id.*
107 *Id.* at 94.
108 *Id.*
109 *Id.*
110 *Id.* (internal citations omitted).
111 *In re F.P.*, 878 A.2d at 94.
112 *Id.*

One fact not discussed in *Griffin* is that the defendant did not deny sending the instant messages.[113] Subsequent to the school meeting, and just before the assault, another instant message conversation occurred.[114] Defendant allegedly stated "u gotta tell tha [sic] school shit n stuff like a lil [sic] bitch."[115] He also threatened, "want my brother to beat ur ass on tha [sic] steel center bus" and "want [sic] till i see u outta school ima [sic] beat ur aSS [sic]."[116]

The court found that there existed sufficient evidence that the defendant sent the instant messages.[117] The defendant referred to himself by his first name, and he repeatedly accused the victim of stealing from him, which mirrored testimony that the defendant was angry about a stolen DVD. The defendant also referenced the fact that the victim had approached school authorities about the instant messages, and repeatedly threatened the victim. The court stated, "[a]ll of this evidence, taken together, was clearly sufficient to authenticate the instant message transcripts as having originated from [defendant]."[118] The court also stated:

> Essentially, [defendant] would have us create a whole new body of law just to deal with e-mails or instant messages. The argument is that e-mails or text messages are inherently unreliable because of their relative anonymity and the fact that while an electronic message can be traced to a particular computer, it can rarely be connected to a specific author with any certainty. Unless the purported author is actually witnessed sending the e-mail, there is always the possibility it is not from whom it claims. As [defendant] correctly points out, anybody with the right password can gain access to another's e-mail account and send a message ostensibly from that person. However, the same uncertainties exist with traditional written documents. A signature can be forged; a letter can be typed on another's typewriter; distinct letterhead stationary can be copied or stolen. We believe that e-mail messages and similar forms of electronic communication can be properly authenticated within the existing framework of Pa.R.E. 901 and Pennsylvania case law. ... We see no justification for construing unique rules for admissibility of

---

[113] *See generally Griffin v. State*, 419 Md. 343 (2011). The *In re F.P.* court discussed the fact that the defendant did not deny sending the instant messages, but the Court of Appeals of Maryland did not discuss this fact in its analysis. *In re F.P.*, 878 A.2d at 94.

[114] *In re F.P.*, 878 A.2d at 94-95.

[115] *Id.* at 95.

[116] *Id.*

[117] *Id.*

[118] *Id.*

> electronic communications such as instant messages; they are to be evaluated on a case-by-case basis as any other document to determine whether or not there has been an adequate foundational showing of their relevance and authenticity.[119]

The *Griffin* court distinguished the case, stating:

> *In the Interest of F.P.* is unpersuasive in the context of a social networking site, because the authentication of instant messages by the recipient who identifies his own "distinctive characteristics" and his having received the messages, is distinguishable from the authentication of a profile and posting printed from MySpace, by one who is neither a creator nor user of the specific profile ...[120] We further note that authentication concerns attendant to e-mails, instant messaging correspondence, and text messages differ significantly from those involving a MySpace profile and posting printout, because such correspondences is sent directly from one party to an intended recipient or recipients, rather than published for all to see.[121]

It is not clear how the *Griffin* court would have addressed the authentication of messages sent by social media. There are similarities between *In re F.P.* and *Williams*, yet the *Griffin* court discussed them differently. Both cases involved messages that were sent from one user to another that appeared to be private, although *In re F.P.* did not specify the system used for the instant messages. The content of the messages in *Williams* is unknown. In *In re F.P.*, the court provided significant details that persuaded it to find sufficient evidence of authentication, including defendant's failure to deny sending the instant messages during communications with school officials.[122]

Authentication of privates messages sent with social media under Rule 5-901(b)(4)'s circumstantial evidence standard will focus on the overall picture to determine whether there exists sufficient evidence to conclude that the messages are authentic. In addition to testimony of the recipient of the messages, the content of the messages will be important to the extent that they contain information and details likely only known by the alleged sender. The overall picture will vary from case to case, and courts will likely have to grapple with this issue on a case-by-case basis. Also likely to be important are "confirming circumstances," which are further discussed below.

---

119 *Id.* at 95-96.
120 *Griffin*, 419 Md. at 361, 19 A.3d at 426.
121 *Griffin*, 419 Md. at 361 n.13, 19 A.3d at 426 n.13.
122 *In re F.P.*, 878 A.2d at 94.

VII. CONFIRMING CIRCUMSTANCES

When the *Griffin* court discussed testimony of a witness with knowledge under Rule 5-901(b)(1), it noted that, in the case at hand, Ms. Barber could have been asked whether the MySpace profile was hers, and whether its contents were authored by her, but she was not asked those questions.[123] The *Griffin* court then cited *U.S. v. Barlow*[124] and *U.S. v. Gagliardi*.[125] Both cases, however, did not involve a profile post; they involved private messages.[126] In both cases, adult defendants were convicted of crimes relating to attempts to have sex with minors.[127] Both involved authentication of messages sent between the defendants and informants working for law enforcement posing as minors.[128]

In *Barlow*, the messages were exchanged on the Yahoo! Messenger instant messaging service, and by email.[129] At the defendant's instigation, the conversations were explicit, and the defendant emailed multiple pornographic pictures of himself.[130]

The court noted that the defendant did not contend that the message log was altered.[131] The court then stated:

> At trial, [informant] testified that the transcripts fairly and fully reproduced the chats between her (posing as [a minor]) and [defendant]. [Informant], as the other participant in the year-long "relationship," had direct knowledge of the chats. Her testimony could sufficiently authenticate the chat log presented at trial, and it was not plainly erroneous to admit the transcript on this basis.[132]

In *Gagliardi*, the instant messages were sent through an Internet chat room called "I Love Older Men."[133] The defendant expressed his desire to have sex, and emailed a picture of himself to the purported underage girl.[134] He also sent similar messages to an FBI agent who was posing as another minor.[135] The court held that authentication was proper because the informant and FBI agents both testified that "the exhibits were in fact

---

123 *Griffin*, 419 Md. at 355-56, 19 A.3d at 422-23.
124 United States v. Barlow, 568 F.3d 215 (5th Cir. 2009).
125 United States v. Gagliardi, 506 F.3d 140 (2d Cir. 2007).
126 *Barlow*, 568 F.3d at 217-18; *Gagliardi*, 506 F.3d at 143-44.
127 *Barlow*, 568 F.3d at 218; *Gagliardi*, 506 F.3d at 143-44.
128 *Barlow*, 568 F.3d at 217; *Gagliardi*, 506 F.3d at 143.
129 *Barlow*, 568 F.3d at 218.
130 *Id.* at 218.
131 *Id.* at 220.
132 *Id.*
133 *Gagliardi*, 506 F.3d at 143.
134 *Id.*
135 *Id.*

accurate records" of the conversations with defendant.[136] The court found that the informant and FBI agents were witnesses with knowledge under Rule 5-901(b)(1).[137]

There is a good argument that the analysis in *Barlow* and *Gagliardi* would not be appropriate under *Griffin*. There were no details in the opinions about any distinctive characteristics in the messages. It can be argued under the *Williams* decision, also cited in *Griffin*, that testimony by the recipient of the messages alone in these cases is insufficient to establish the identity of the actual sender of the messages. There were other important facts, however, that the *Barlow* and *Gagliardi* courts did not make part of their authentication analysis. They are what the Supreme Judicial Court of Massachusetts has called "confirming circumstances."[138] When these confirming circumstances are added into the analysis, it appears that even a heightened degree of authentication required by *Griffin* would be met.

In *Barlow*, the instant message communications at issue scheduled a meeting for a particular time and place, and the defendant showed up as planned.[139] That is certainly strong corroborative evidence that the defendant was the one participating in the communications. Moreover, when the defendant was arrested at the meeting place, his laptop was in his car, and it had "remnants of the chats" with the informant.[140] It is these two facts, or "confirming circumstances," that provide the strongest evidence of authentication, yet they were not part of the court's analysis.

Similarly, in *Gagliardi*, the defendant was arrested at a meeting time and place that had been arranged in the messages at issue.[141] The defendant also admitted to police that "he was at the location to meet two thirteen-year-old girls with whom he had previously had sexually explicit online conversations."[142] Those "confirming circumstances" were not part of the court's authentication analysis.

The Supreme Judicial Court of Massachusetts discussed "confirming circumstances" in *Commonwealth v. Purdy*,[143] which was decided 13 days before *Griffin*. In *Purdy*, the defendant was convicted of crimes relating to running a house of prostitution.[144] On appeal, he claimed that

---

136 *Id.* at 151.

137 *Id.*

138 *See Purdy*, 945 N.E.2d at 380 (Mass. 2011) (explaining that "confirming circumstances" are those "that would allow a reasonable jury to conclude that [the] evidence is what its proponent claims it to be.").

139 *Barlow*, 568 F.3d at 218.

140 *Id.*

141 *Gagliardi*, 506 F.3d at 143.

142 *Id.* at 143-44.

143 *Purdy*, 945 N.E.2d 372.

144 *Id.* at 376.

ten email exchanges admitted into evidence had not been properly authenticated.[145] The emails were taken from a computer located on the premises at issue.[146] The defendant admitted that the computer was his and that he used it.[147] He also provided from memory the passwords necessary to access the computer.[148] The emails were sent from an email address that had defendant's first and last names in it, and defendant admitted he used the account.[149] The court described some of the emails as follows:

> Among the e-mail exchanges admitted in evidence was one that was initiated from the defendant's e-mail address and signed with the defendant's name and the address of the salon, and had the "header," "personal assistant with benefits?." The author wrote that he was "seeking a personal secretary with an open mind, who . . . knows where to keep her nose and where not." In response to a reply from a recipient, the author described himself as a "working artist, as well [as an] entrepreneur, small business guy, hairstylist, art and antiques dealer, [and] massage therapist," and added "and I operate a service." In a later e-mail in this exchange, also from the defendant's e-mail address, the author asserted that potential earnings could range from $200 to $2,000 per week.
>
> A separate e-mail was entitled "massage" and was sent from the defendant's e-mail address and signed with the defendant's first name. The author describes a "blond girl" who is "fairly new and so a little nervous," and states: "If you are gentle and kind to her I'm sure you're going to have a very good time." He adds, "She has beautiful breasts and she will allow light touching. It is ok, but no other touching." The recipient of the e-mail responded that he wanted an "unhurried session" with a "gal who will treat me right[,] be slow [,] gentle and very friendly within her limits." An e-mail from the defendant's e-mail address and signed with defendant's first initial replied, "I will make sure you are treated well."[150]

The defendant denied authoring the emails, and moved *in limine* to preclude their admission into evidence.[151] He stated that the computer

---

145 *Id.*
146 *Id.* at 377-78.
147 *Id.* at 377.
148 *Id.*
149 *Purdy*, 945 N.E.2d at 378.
150 *Id.*
151 *Id.* at 379.

was always on, and that the masseuses knew his passwords and used the computer frequently.[152] He testified that they used his email account to play pranks on him and to answer emails in his name.[153] The court observed that the prosecution "did not furnish direct evidence that the defendant had authored any of the ten e-mails admitted in evidence; there was no testimony that anyone observed him typing any of the e-mails or that anyone had discussed any of the e-mails with him."[154]

The court stated, "[w]hile e-mails and other forms of electronic communication present their own opportunities for false claims of authorship, the basic principles of authentication are the same."[155] The court added that a "judge making a determination concerning the authenticity of a communication sought to be introduced in evidence may look to 'confirming circumstances' that would allow a reasonable jury to conclude that this evidence is what its proponent claims it to be."[156] The court concluded:

> Here there were adequate "confirming circumstances" to meet this threshold: in addition to the e-mails having originated from an account bearing the defendant's name and acknowledged to be used by the defendant, the e-mails were found on the hard drive of the computer that the defendant acknowledged he owned, and to which he supplied all necessary passwords. While this was sufficient to authenticate the e-mails in the absence of persuasive evidence of fraud, tampering, or "hacking," there was additional evidence of the defendant's authorship of most of the emails. At least one e-mail contained an attached photograph of the defendant, and in another, the author described the unusual set of services provided by the salon when he characterized himself, among other things, as a "hairstylist, art and antiques dealer, [and] massage therapist." The defendant's uncorroborated testimony that others used his computer regularly and that he did not author the e-mails was relevant to the weight, not the admissibility, of these messages.[157]

The court distinguished its opinion in *Williams*, noting that the sender of the messages in that case did not identify himself with the name of the defendant's brother, or any other name.[158] The messages in *Williams*

---

152 *Id.* at 378.
153 *Id.*
154 *Id.* at 379-80.
155 *Purdy*, 945 N.E.2d at 381.
156 *Id.* at 380.
157 *Id.* at 381-82.
158 *Id.* at 382 n.7.

could have been sent from any computer, while the messages in *Purdy* were sent from the defendant's password protected computer.[159]

Although the *Purdy* court did not apply a heightened degree of authentication for the emails, its use of "confirming circumstances" should be applicable in Maryland cases. The *Griffin* court did not use that term, but did discuss searching a computer as a method of authentication, which could yield evidence that constitutes "confirming circumstances."[160] Moreover, there will be other evidence that will be significant "confirming circumstances," even if it is not part of the "distinctive characteristics" of the social media evidence itself under 5-901(b) (4). Good examples are the defendants in *Barlow* and *Gagliardi* showing up at meetings that were planned in the messages they allegedly sent.

VIII. CONCLUSION

Under *Griffin*, a greater degree of authentication is required of certain social media evidence. Practitioners will find that the best evidence of authentication of social media evidence is an admission by the creator. Cases without such an admission will have to be analyzed on a case-by-case basis, particularly the cases in which the proponent relies on circumstantial evidence under Rule 5-901(b)(4). Confirming circumstances will be important in cases where the evidence itself does not contain sufficient "distinctive characteristics" under 5-901(b)(4) to establish authentication.

The *Griffin* court noted that methods to authenticate social media evidence might continue to develop. Developments could include changes in technology or laws, such as revision to the SCA to bring it in accord with updated technology. Advances in technology, however, have at times raised more questions than they have answered. Such is the current state of affairs with authentication of social media. Open questions remain as the courts implement *Griffin*'s guidance to other factual scenarios.

---

[159] *Id.*

[160] *See Griffin*, 419 Md. at 363-64, 19 A.3d at 427-28 (discussing possible avenues available to properly authenticate printouts from social networking websites).