AUTHENTICITY AND ADMISSIBILITY OF SOCIAL MEDIA WEBSITE PRINTOUTS

WENDY ANGUS-ANDERSON[†]

ABSTRACT

Social media posts and photographs are increasingly denied admission as evidence in criminal trials. Courts often cite issues with authentication when refusing to admit social media evidence. Cases and academic writings separate recent case law into two approaches: The Maryland Approach and the Texas Approach. The first method is often seen as overly skeptical of social media evidence, setting the bar too high for admissibility. The second approach is viewed as more lenient, declaring that any reasonable evidence should be admitted in order for a jury to weigh its sufficiency. This Brief addresses the supposed differences between the two sets of cases and suggests that courts are not actually employing two distinct approaches. The Maryland Approach courts are not holding social media content to a higher standard than the Texas Approach courts, but are merely responding to a lack of evidence connecting the proffered content to the purported author.

INTRODUCTION

Sarah and Megan, both thirteen years old, had been friends for most of their lives. They went to the same school, were always spending time at the other's house, and even traveled with each other's family for vacations. As sometimes happens when getting older, however, Megan transferred from the public school to a Catholic school and the two girls had a "falling out." Sometime thereafter, Sarah became worried that Megan might be spreading rumors about her old friend to her new social group. Sarah's mother shared her daughter's concerns, and conceived of a scheme to humiliate Megan.

Sarah's mother set up a fictitious MySpace account under the name "Josh Evans." "Josh" was sixteen years old, attractive, and new to the neighborhood. She then used the new account to draw Megan into conversation online. About two weeks later, Sarah's mother had Josh tell Megan that he no longer liked her and that the world would be a better

[†] Duke University School of Law, J.D. expected 2016; B.A. in Anthropology, 2008, Franklin & Marshall College.

place without Megan in it. Distraught, the thirteen-year-old hung herself in her bedroom closet that night.[1]

The circumstances leading to Megan's death demonstrate the relative ease with which anyone can create a fictional persona online, sometimes with horrific consequences. In the world of social media, it is particularly easy for users to create fake accounts, access and manipulate another's account, and then change or delete the material at a later date. The electronic nature of social media evidence presents many new legal challenges, leaving case law regarding this type of evidence murky at best. The requirement of authentication is therefore especially vital for social media evidence to ensure that the offered material is what it appears to be. The proponent should not only offer evidence that the printout accurately reflects the online webpage, but also that it was created by the purported author. Only then can the evidence be properly presented to a jury.

I. THE PREVALENCE OF SOCIAL MEDIA

Social media is defined as "forms of electronic communications . . . through which users create online communities to share information, ideas, personal messages, and other content."[2] Social media sites are "sophisticated tools of communication where the user voluntarily provides information that the user wants to share with others."[3] These web-based applications allow users to create a personal profile, often containing a photograph of the user along with name, location, and the ability to "post" statements for others to view.[4] Social network sites range from social communities such as Facebook and MySpace to the professional network LinkedIn.[5]

The popularity of social media sites cannot be overstated. As one District Judge and legal scholar wrote: "Social media is ubiquitous, and it

---

[1] All background information comes from *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009).

[2] *Social Media,* MERRIAM-WEBSTER.COM, http://www.merriamwebster.com/dictionary/social%20media (last visited Sept. 24, 2015).

[3] Indep. Newspapers, Inc. v. Brodie, 966 A.2d 432, 437 n.3 (Md. 2009).

[4] Parker v. State, 85 A.3d 682, 685 (Del. 2014).

[5] U.S. JUD. CONF. COMM. ON CODES OF CONDUCT, RESOURCE PACKET FOR DEVELOPING GUIDELINES ON USE OF SOCIAL MEDIA BY JUDICIAL EMPLOYEES 9 (2010), http://www.uscourts.gov/uscourts/RulesAndPolicies/conduct/SocialMediaLayout.pdf.

is here to stay."[6] At the beginning of 2014, eighty-nine percent of 18-29 year olds with Internet access used social networking sites.[7] Facebook boasts 1.35 billion monthly active users as of September 30, 2014.[8] This equates to one out of every 5.5 people in the world.[9] The influential website has become a constant in many users' lives, with sixty-three percent of users reportedly accessing the site at least once a day.[10]

Given the great prevalence of social media today, it is not surprising that online content has made its way into courtrooms. After creating a profile, users will frequently post items such as text, pictures, or videos to their profile page. Often, these posts include relevant evidence for a trial.[11] Social media is offered in trials to show, among other things, a party's state of mind, intent, or motives.[12] Parties may wish to submit social media as evidence of communication between users, inculpatory or exculpatory photographs, or even party admissions.[13] Attorneys and judges are dealing with social media evidence more and more as the Internet and technology continue to advance.

II. DETERMINING AUTHENTICITY OF EVIDENCE IN GENERAL

Under the Federal Rules of Evidence, "[R]elevant evidence is admissible" unless otherwise provided and "[i]rrelevant evidence is not admissible."[14] This seemingly straightforward rule is complicated by subsequent limitations on what qualifies as "relevant." At the most basic level, a party who wishes to admit evidence must first ask, "Does this evidence have 'any tendency to make a fact more or less probable than it would be without the evidence?'"[15] If she can answer affirmatively, then that evidence has passed the first hurdle of relevance.

---

[6] Paul W. Grimm, Lisa Yurwit Bergstrom & Melissa M. O'Toole-Loureiro, *Authentication of Social Media Evidence*, 36 AM. J. TRIAL ADVOC. 433, 437 (2013).

[7] PEW RESEARCH INTERNET PROJECT, SOCIAL MEDIA UPDATE 2013 (Dec. 30, 2013), http://www.pewinternet.org/2013/12/30/social-media-update-2013/#.

[8] FACEBOOK NEWSROOM, http://newsroom.fb.com/company-info/ (last visited Nov. 8, 2014).

[9] *See* U.S. Census Bureau, *U.S. and World Population Clock*, CENSUS.GOV http://www.census.gov/popclock/ (last visited Nov. 10, 2014) (listing world population of 7.21 billion people).

[10] PEW RESEARCH INTERNET PROJECT, *supra* note 7.

[11] Parker v. State, 85 A.3d 682, 685 (Del. 2014).

[12] Grimm, *supra* note 6, at 438.

[13] *Id.*

[14] FED. R. EVID. 402.

[15] FED. R. EVID. 401(a).

Any tangible or demonstrative exhibits must then be authenticated in order to be relevant.[16] The proponent offering the piece of writing must produce evidence "sufficient to support a finding that the item is what the proponent claims it is."[17] For an exhibit such as a social media post, this would typically involve demonstrating that the writing has a connection to a specific person, through authorship or some other relation.[18]

It is easy to appreciate the importance of authentication when considering a document such as a letter. Suppose an attorney offers a letter at trial which she claims was written by the defendant. She declares that the letter perfectly demonstrates the defendant's state of mind at the time he wrote it. This would be very persuasive to the jury. The attorney's assertion can only be true, however, if the defendant actually did author the letter. If another person wrote it, then the jury has learned nothing new about the defendant's state of mind, and the letter is irrelevant. Authentication ensures that before the jury hears any evidence, the proponent has connected it to the trial in a way that ensures the evidence is actually what she claims it to be.

In Rule 901, the Federal Rules of Evidence offer multiple ways in which proponents can authenticate a particular item. The simplest technique is providing testimony from a witness who has knowledge that the evidence is what it claims to be.[19] Another method involves pointing to distinctive characteristics of the evidence that can authenticate the item.[20] For example, an email may state facts that only one person could know, or use a language pattern known to match a particular person.[21] The proponent may also demonstrate that the evidence was created by a process or system which produces accurate results.[22] Thus, an X-ray machine is assumed to create an authentic portrayal of the bones it has scanned.[23] These examples are not an exclusive list of authentication methods.[24] An attorney may use any number of methods to fulfill the authentication requirement.

---

[16] MCCORMICK ON EVIDENCE § 221 (Kenneth S. Broun et al. eds., 7th ed. 2014).
[17] FED. R. EVID. 901(a).
[18] MCCORMICK ON EVIDENCE, *supra* note 16.
[19] FED. R. EVID. 901(b)(1).
[20] FED. R. EVID. 901(b)(4).
[21] FED. R. EVID. 901 advisory committee's note.
[22] FED. R. EVID. 901(b)(9).
[23] FED. R. EVID. 901 advisory committee's note.
[24] *See id.* ("The examples are not intended as an exclusive enumeration of allowable methods but are meant to guide and suggest, leaving room for growth and development in this area of the law.").

Preliminary questions about the admissibility of evidence are decided by the trial judge.[25] This means that the court's role is to serve as a "gatekeeper" in deciding whether the proponent has offered evidence sufficient to meet the 901 authentication requirement.[26] He does not need to be satisfied that the evidence is actually what it purports to be,[27] only that it is reasonably possible for a jury to find that it is authentic.[28] After the court determines that the proponent has successfully met this threshold requirement, it is for the trier-of-fact to appraise the credibility and weight of the proffered evidence.[29] The jury must decide whether the item is what it seems to be.[30]

III. DETERMINING AUTHENTICITY OF SOCIAL MEDIA EVIDENCE

The state of the law regarding social media evidence admissibility is murky at best. Courts and academic writings have split the case law into two approaches. These can best be referred to as "The Maryland Approach" and "The Texas Approach."[31]

According to analysts, Maryland Approach courts are skeptical of social media evidence, finding the odds too great that someone other than the alleged author of the evidence was the actual creator.[32] The proponent must therefore affirmatively disprove the existence of a different creator in order for the evidence to be admissible.[33]

Courts following the Texas Approach are seen as more lenient in determining what amount of evidence a "reasonable juror" would need to be persuaded that the alleged creator did create the evidence.[34] The burden of production then transfers to the objecting party to demonstrate

---

[25] FED. R. EVID. 104(a).
[26] United States v. Vidacak, 553 F.3d 344, 349 (4th Cir. 2009).
[27] United States v. Safavian, 435 F. Supp. 2d 36, 38 (D.C. Cir. 2006).
[28] *Vidacak*, 553 F.3d at 349.
[29] FED. R. EVID. 104.
[30] In the event of a bench trial, the judge will act as trier-of-fact rather than a jury.
[31] I have adopted the terms "The Maryland Approach" and "The Texas Approach," first used in *Parker v. State*, 85 A.3d 682 (Del. 2014), as convenient titles for the two perceived methods.
[32] Grimm, *supra* note 6, at 455.
[33] *Id.*
[34] *See, e.g.,* United States v. Vayner, 769 F.3d 125 (2d Cir. 2014); State v. Assi, No. 1 CA-CR 10-0900, 2012 WL 3580488 (Ariz. Ct. App. Aug. 21, 2012); People v. Valdez, 135 Cal. Rptr. 3d 628 (Ct. App. 2011); People v. Clevenstine, 891 N.Y.S.2d 511 (N.Y. App. Div. 2009); Tienda v. State, 358 S.W.3d 633 (Tex. Crim. App. 2012); Manuel v. State, 357 S.W.3d 66 (Tex. Ct. App. 2011).

that the evidence was created or manipulated by a third party.[35] This second approach is viewed as "better reasoned" because it allows for proper interplay among the many rules that govern admissibility, including 901.[36]

A. The Maryland Approach

This first approach's seemingly higher standard for social media authentication is best exemplified by the Maryland Court of Appeals' decision in *Griffin v. State*.[37] The defendant in *Griffin* was charged with second-degree murder, first degree assault, and use of a handgun in commission of a felony.[38] The State offered printouts from a MySpace profile belonging to the defendant's girlfriend, Jessica Barber, to demonstrate that Barber had allegedly threatened one of the State's witnesses.[39] The page contained the statement: "FREE BOOZY [(the nickname for the defendant)]!!!! JUST REMEMBER SNITCHES GET STITCHES!! U KNOW WHO YOU ARE!!"[40] The printout displayed the name of the profile as "Sistahsouljah," and described details of the profile owner's life such as a birthday of 10/02/1983 and location of Port Deposit.[41] A photograph of Griffin and Barber embracing was also included.[42]

Rather than using Barber to authenticate the pages, the State attempted to use an investigator's testimony.[43] The lead investigator for the case, Sergeant John Cook, downloaded the information from MySpace.[44] Cook testified that he knew it was Barber's profile due to the photograph of her and Boozy, a reference to the children, and her birth date listed on the form.[45] Defense counsel objected because "the State could not sufficiently establish a 'connection' between the profile and posting and Ms. Barber."[46] The printouts were admitted and Griffin was convicted.

---

[35] *See Tienda*, 538 S.W.3d at 642–47.
[36] Grimm, *supra* note 6, at 456.
[37] Griffin v. State, 19 A.3d 415 (Md. App. 2011).
[38] Griffin v. State, 995 A.2d 791, 794 (Md. Ct. Spec. App. 2010).
[39] *Griffin*, 19 A.3d at 418.
[40] *Id.*
[41] *Id.*
[42] *Id.*
[43] *Id.*
[44] *Id.* at 348–50.
[45] *Id.* at 418.
[46] *Id.* at 348.

Griffin appealed the decision, asserting that the printouts were not properly authenticated and therefore inadmissible.[47] The Maryland Court of Special Appeals upheld the verdict. After another appeal request, the Maryland Court of Appeals accepted the case to decide whether the MySpace printout was representative of a profile created by Barber, and also whether she had posted the "SNITCHES GET STICHES" warning.[48]

The appellate court noted that very few courts in any jurisdiction had an opportunity to consider the authentication of pages printed from a social media site.[49] It stated that "[t]he potential for fabricating or tampering with electronically stored information on a social networking site" posed "significant challenges" when considering authenticity of site printouts.[50] The court nonetheless maintained that Rule 901 governed authentication.[51] This rule states that circumstantial evidence "such as appearance, contents, substance, internal patterns, location, *or other distinctive characteristics*" can be offered as evidence that the article is what it claims to be.[52] The court reversed and remanded, holding that a birthdate, location, reference to the defendant's nickname, and a photograph of the couple were not sufficiently "distinctive characteristics" to authenticate a MySpace printout.[53] When explaining its decision, it cited a concern that "someone other than the alleged author may have accessed the account and posted the message in question."[54]

In *State v. Eleck*, the defendant appealed his conviction of assault in the first degree by means of a dangerous instrument.[55] Eleck claimed on appeal that the trial court improperly excluded evidence that had been properly authenticated.[56] At a party with about twenty intoxicated teenagers in attendance, the defendant engaged two party guests in a

---

[47] *Id.* at 417.
[48] *Id.* at 419–20.
[49] *Id.* at 422.
[50] *Id.*
[51] *Id.* (citing the state law which is materially similar to Federal Rule of Evidence 901).
[52] *Id.* (emphasis added).
[53] *Id.* at 423–24.
[54] *Id.* at 423 (quoting Griffin v. State, 995 A.2d 791, 805 (Md. Ct. Spec. App. 2010)).
[55] State v. Eleck, 23 A.3d 818, 819 (Conn. App. Ct. 2011).
[56] *Id.*

physical altercation.[57] When the combatants were separated, Eleck's two opponents both discovered that they had suffered stab wounds.[58]

At his trial, Eleck offered printouts of Facebook messages allegedly received from a State's witness, another attendant of the party.[59] The defendant personally testified as to the authenticity of the printouts, stating that the user name belonged to the witness, the profile contained photographs of the witness, and that he had downloaded and printed the messages himself.[60] The State's witness admitted that the profile was hers, but claimed that her account had been hacked and she had not sent the messages in question.[61]

The appellate court affirmed the trial court's decision not to admit the evidence,[62] determining that even unique user names and passwords are not enough to eliminate the possibility of hackers.[63] The court explained that authenticating that a message came from a specific account is not sufficient evidence that it was authored by the account owner.[64] The messages themselves did not "reflect distinct information that only [the witness] would have possessed regarding the defendant or the character of their relationship."[65] The authorship had not been sufficiently authenticated.

Similarly, in *Commonwealth v. Williams*, an appellate court found that the prosecution had failed to offer adequate foundation as to the authorship of MySpace messages.[66] In this case, the defendant was convicted of murder in the first degree of one victim and assault with intent to commit murder of another victim.[67] At trial, the girlfriend of one of the victims testified about MySpace messages she received from the defendant's brother, warning her not to testify at trial.[68] The testimony was admitted without objection, but the defendant later unsuccessfully submitted motions to strike the testimony and declare a mistrial.[69]

---

[57] *Id.*
[58] *Id.*
[59] *Id.* at 820.
[60] *Id.*
[61] *Id.*
[62] *Id.* at 825.
[63] *Id.* at 822.
[64] *Id.*
[65] *Id.* at 824.
[66] Commonwealth v. Williams, 926 N.E.2d 1162, 1173 (Mass. 2010).
[67] *Id.* at 1165.
[68] *Id.* at 1172.
[69] *Id.* at 1171.

When reviewing the authentication issue, the appellate court compared the MySpace messages to a phone call: "[A] witness' testimony that he or she has received an incoming call from a person claiming to be 'A,' without more, is insufficient evidence to admit the call as a conversation with 'A.'"[70] Although the foundational testimony had established that "the messages were sent by someone with access to [the defendant's] MySpace Web page," there was no evidence regarding "the person who actually sent the message."[71] The court referenced a lack of evidence concerning how secure MySpace is, how a person accesses the page, and whether passwords or codes are used.[72] Allowing the jury to hear this testimony would create a high potential for prejudice, and the court ruled that the content of the messages should not have been admitted.[73]

B. The Texas Approach

Many courts have followed what has been termed the more lenient "Texas Approach."[74] This approach is best exemplified by *Tienda v. State*. After being convicted of murder, Tienda appealed the decision, claiming that the trial court should not have admitted evidence from MySpace pages alleged to be managed by the defendant.[75] The Fifth Circuit Court of Appeals affirmed the conviction, as did the Court of Criminal Appeals.[76]

The victim was traveling home from a nightclub when his car unexpectedly came under gunfire from a caravan of three or four cars on the same road.[77] Tienda, the appellant, was a passenger in one of the caravan's cars.[78] The Court admitted several MySpace accounts into evidence allegedly belonging to the appellant.[79] Each account was linked to email addresses including Tienda's name or nickname, had a profile name matching either Tienda's name or nickname, listed Tienda's

---

[70] *Id.* at 1172 (citing Commonwealth v. Hartford, 194 N.E.2d 401 (Mass. 1963)).
[71] *Id.* at 1172–73.
[72] *Id.* at 1172.
[73] *Id.* at 1173.
[74] *See, e.g.,* United States v. Vayner, 769 F.3d 125 (2d Cir. 2014); State v. Assi, No. 1 CA-CR 10-0900, 2012 WL 3580488 (Ariz. Ct. App. Aug. 21, 2012); People v. Valdez, 135 Cal. Rptr. 3d 628 (Ct. App. 2011); People v. Clevenstine, 891 N.Y.S.2d 511 (N.Y. App. Div. 2009); Tienda v. State, 358 S.W.3d 633 (Tex. Crim. App. 2012); Manuel v. State, 357 S.W.3d 66 (Tex. Ct. App. 2011).
[75] *Tienda*, 358 S.W.3d at 634.
[76] *Id.* at 634.
[77] *Id.*
[78] *Id.*
[79] *Id.* at 634–35.

hometown as the location, and contained photographs of a man who "resembled" Tienda.[80] The accounts contained postings such as, "You aint BLASTIN You aint Lastin"[81] and "EVERYONE WUZ BUSTIN AND THEY ONLY TOLD ON ME."[82]

In affirming the intermediate appellate and trial courts, the Court of Criminal Appeals compared the current case to *Griffin*, stating that "there [were] far more circumstantial indicia of authenticity in this case than in *Griffin*."[83] The combination of photographs, references to particular situations, and messages sent from accounts bearing the appellant's name—"taken as a whole with all of the individual particular details considered in combination"—was deemed sufficient for a reasonable jury to believe that Tienda created and maintained the profiles.[84]

In *People v. Clevenstine*,[85] the defendant was convicted of five counts of rape and six other charges such as sexual abuse and endangering the welfare of a child.[86] Clevenstine challenged that a computer disk with MySpace and Facebook messages between him and the victims had not been properly authenticated.[87] Both victims had testified that the defendant had messaged them through social media sites.[88] The State Police investigator had retrieved the conversations directly from the victims' hard drives.[89] A legal compliance officer from Facebook testified that the messages did originate from the purported accounts.[90] The defendant's wife also testified that she had seen the same sexually explicit messages on her husband's MySpace account on their home computer.[91] While the court recognized that the defendant's claim that someone else accessed his MySpace account was possible, "the likelihood of such a scenario presented a factual issue for the jury."[92]

---

[80] *Id.* at 634–36.
[81] *Id.* at 635.
[82] *Id.* at 636.
[83] *Id.* at 647.
[84] *Id.* at 645.
[85] 891 N.Y.D.2d 511 (N.Y. App. Div. 2009).
[86] *Id.* at 513.
[87] *Id.* at 514.
[88] *Id.*
[89] *Id.*
[90] *Id.*
[91] *Id.*
[92] *Id.*

IV. ARE THE TWO APPROACHES ACTUALLY DIFFERENT?

In just the past two years, the distinction between the Maryland Approach and the Texas Approach has been widening. The most likely source for the separation is Honorable Paul W. Grimm's 2013 article, *Authentication of Social Media Evidence*.[93] In this *American Journal of Trial Advocacy* article, Grimm clearly draws a line between what he sees as two separate approaches to social media authentication. The first approach involves courts setting "an unnecessarily high bar for the admissibility of social media evidence."[94] The second utilizes a different method, "determining the admissibility of social media evidence based on whether there was sufficient evidence of authenticity for a reasonable jury to conclude that the evidence was authentic."[95] This distinction has been reiterated often in the past two years.

Courts and attorneys have cited directly to Grimm's article in case opinions and briefs. A 2014 case, *Parker v. State*,[96] references the article before separating past cases into "The Maryland Approach" and "The Texas Approach."[97] It portrays *Griffin* and *Tienda* respectively as the prime examples of each method,[98] just as in Grimm's article.[99] The appellee's brief for *Harris v. State*,[100] quotes Grimm's article several times when asserting that *Griffin* set an "unnecessarily high bar" for authentication of social media evidence.[101] The appellant's brief in the currently pending case, *Sublet v. State*,[102] similarly references the article while claiming that a court was "inappropriately strict" in its interpretation of evidence law.[103] In citing Grimm, judges and attorneys are adopting the distinction between unnecessarily strict courts and those that are more lenient.

The distinction is also being reinforced in secondary sources. The *Practical Law* section of Westlaw informs litigators that most courts

---

[93] Grimm, *supra* note 6.
[94] *Id.* at 441.
[95] *Id.*
[96] 85 A.3d 682 (Del. 2014).
[97] *Id.*
[98] *See id.* at 686 (stating that the higher standard for social media evidence "is best exemplified by . . . *Griffin v. State*" and the "alternative line of cases" is best represented by *Tienda*).
[99] *See* Grimm, *supra* note 6, at 441, 449 (using *Griffin* and *Tienda* as the first cases to describe each approach).
[100] No. 42, slip op. (Md. Apr. 23, 2015).
[101] *Id.* at *31.
[102] No. 59 (Md. Apr. 23, 2015).
[103] *Id.* at *24 n.20.

employ a practice of admitting evidence "if the party demonstrates to the trial judge that a jury could reasonably find that the proffered evidence is authentic."[104] It then explains that other courts recommend a "higher standard."[105] It once again provides *Tienda* and *Griffin* as the two paradigms.[106] Another 2014 article, *The Pitfalls and Perils of Social Media in Litigation*, compares more lenient cases to those in which a "greater degree of authentication" is required.[107]

Dividing the case law into two such distinct categories ignores the similar reasoning behind the courts' decisions and fails to take into account rules that govern admissibility other than those in the Federal Rules of Evidence.

The state of case law as it pertains to social media evidence has evolved considerably in the past decade and a half. In 1999, one court deciding whether to admit printouts of a webpage declared, "There is no way Plaintiff can overcome the presumption that the information he discovered on the Internet is inherently untrustworthy. . . . *[A]ny evidence procured off the Internet is adequate for almost nothing*."[108] While courts sometimes still display a distrust of social media evidence,[109] they no longer discount it as completely useless. Courts and legal scholars have generally agreed that although rapidly developing technology may present new challenges, the existing rules of evidence regarding authenticity are "adequate to the task."[110]

Social media evidence is most often offered as evidence at trial as printouts of webpages. Determining admissibility of these printouts involves two steps: (1) "Printouts of web pages must first be

---

[104] Norman C. Simon & Samantha V. Ettari, *Social Media: What Every Litigator Needs to Know*, PRACTICAL LAW, (to access this article, log in to Westlaw Next; follow "Practical Law"; follow "Litigation"; search for "social media" in search bar; follow hyperlink for appropriate article) (last visited Sept. 27, 2015).
[105] *Id.*
[106] *Id.*
[107] PAUL RAGUSA & LAUREN EMERSON, THE PITFALLS AND PERILS OF SOCIAL MEDIA IN LITIGATION (2014), *available at* Westlaw 2014 WL 5465789.
[108] St. Clair v. Johnny's Oyster & Shrimp, Inc., 76 F. Supp. 2d 773, 774–75 (S.D. Tex. 1999) (emphasis added).
[109] *See, e.g.*, People v. Beckley, 110 Cal. Rptr. 3d 362, 366–67 (Ct. App. 2010) (stating that even unskilled, inexperienced users can utilize Photoshop to change photographs to produce false pictures) and State v. Eleck, 23 A.3d 818, 822 (Conn. App. Ct. 2011) (stating that "electronic communication . . . could be generated by someone other than the named sender").
[110] Steven Good, *The Admissibility of Electronic Evidence*, 29 REV. LITIG. 1, 7 (Fall 2009).

authenticated as accurately reflecting the content and image of a specific webpage on the computer," and then (2) in order to be relevant, the printout "must be authenticated as having been posted by that source."[111] The judge acts as a gatekeeper in determining whether the party offering the evidence has fulfilled this requirement of relevance.[112]

The cases listed as following the Maryland Approach are examples of proponents fulfilling the first requirement, but failing to satisfy or even address the second. These courts are not holding social media evidence to a higher standard than any other; they are recognizing that an important condition for admissibility has not been met.

The clearest example of this is the case listed as the exemplar Maryland Approach case, *Griffin v. State*. The oft-quoted holding states:

> 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 [the purported creator] was its creator and the author of the [relevant] language.[113]

While Grimm seems to focus on the first half of this statement, attributing the court's holding to an overly suspicious view of social media content, it is actually the second half that explains the decision. While an investigator's testimony demonstrated that the printouts were in fact downloaded from MySpace, the State failed to connect the statements to the purported creator. Unless they were posted by the alleged source, the warnings were not relevant to the case. The appellate court therefore correctly concluded that the printouts had been improperly admitted during the trial.

Tienda v. State, often presented in articles and opinions as the opposite of *Griffin*, explicitly compared its own situation to that of the Maryland case.[114] It held that a greater amount of circumstantial evidence supported a finding that "the MySpace pages belonged to the appellant *and that he created and maintained them*."[115] The difference between *Griffin* and *Tienda* was not a heightened admissibility standard. The difference was that only in the latter case did the advocate both

---

[111] MCCORMICK ON EVIDENCE, supra note 16, at § 227.
[112] FED. R. EVID. 104(b).
[113] Griffin v. State, 19 A.3d 415, 424 (Md. App. 2011).
[114] Tienda v. State, 358 S.W.3d 633, 647 (Tex. Crim. App. 2012).
[115] *Id.* at 645 (emphasis added).

authenticate the webpage *and* connect that page to the purported author/maintainer.

This failure to show authorship also occurred in *State v. Eleck*. The State's witness acknowledged that the Facebook account was hers.[116] This sufficiently authenticated the printout as representative of her account. The State could not, however, show that she sent the messages. The witness asserted that her account had been hacked,[117] and the court concluded that there was nothing inherent in the messages that identified her as the author.[118] Because the State was not able to authenticate the messages as being connected to the purported source, the MySpace statements were not relevant to the case and therefore inadmissible as evidence.

Similarly, MySpace messages offered in *Commonwealth v. Williams* were also ruled inadmissible. The court acknowledged the two-prong requirement for admitting communications by comparing the web messages to a phone call. A witness can state that she had a conversation, but for that conversation to be relevant it still must be shown that it was with the purported other person. The court found that although the foundational testimony had established that the person who sent the messages had access to the webpage, there was no evidence of who that person actually was. The court did not subscribe to any standard higher than that required of other evidence. The proponent simply failed to fulfill the requirements for admitting webpage printouts.

People v. Clavenstine is a case comparable to *Williams* while still following the more lenient Texas Approach. Here, the proponent offered MySpace messages taken directly from the victims' hard drives,[119] fulfilling the first requirement. The defendant's wife also testified that she had seen the messages on her husband's computer.[120] The messages were appropriately connected not only to the account, but also to the author himself. With both requirements satisfied, the evidence was admitted.

Numerous other cases that seemingly follow the Maryland Approach share this same element of failing to demonstrate connection to the purported author. In *Commonwealth v. Wallick*,[121] the proponent authenticated a photograph as coming from a MySpace page, but failed

---

[116] State v. Eleck, 23 A.3d 818, 820 (Conn. App. Ct. 2011).
[117] *Id.*
[118] *Id.* at 824.
[119] People v. Clevenstine, 891 N.Y.S.2d 511, 514 (N.Y. App. Div. 2009).
[120] *Id.*
[121] No. CP-67-CR-5884-2010 (Pa. Ct. Com. Pl. Oct. 2011).

to show who created/maintained the page.[122] An expert in *People v. Beckley* testified that a MySpace photograph was not forged, but no evidence was offered that the picture was what it purported to be—a girl flashing an alleged gang sign.[123] Even if the court in *United States v. Jackson* agreed that postings about white supremacist groups did appear on the web, it still noted a lack of evidence regarding whether the posts actually were posted by the groups.[124]

CONCLUSION

Courts using the Maryland Approach are not placing an excessively high bar on social media evidence, or even following a stricter standard than the Texas Approach cases. They are simply recognizing that evidence must be relevant before it may be presented to the jury. In the case of website printouts, this means showing that the content reflects a certain webpage *and* that it was posted by the purported source. Opinions and articles drawing a distinct line between "Maryland" and "Texas" approaches are actually just pointing out the cases in which the second requirement was not fulfilled. Viewing the differing opinions as two opposite approaches not only creates an artificial distinction, but also increases the probability that future courts will misinterpret the admissibility standards and create an actual divergence in analysis.

---

[122] Grimm, *supra* note 6, at 445 (quoting Commonwealth v. Wallick, No. CP-67-CR-5884-2010 (Pa. Ct. Com. Pl. Oct. 2011), slip. op. at 10–11).
[123] 110 Cal. Rptr. 3d 362, 365–67 (Ct. App. 2010).
[124] United States v. Jackson, 208 F.3d 633, 638 (7th Cir. 2000).