Vermont Bar Association
139th Annual Meeting Seminar Materials

Evidence in Practice

October 13, 2017
Hilton Burlington
Burlington, VT

Speakers:

Hon. Tom Carlson
Hon. David Fenster
Hon. Thomas Zonay
John Evers, Esq., Moderator

419 Md. 343
Court of Appeals of Maryland.

Antoine Levar GRIFFIN
v.
STATE of Maryland.

No. 74, Sept. Term, 2010.
|
April 28, 2011.

Synopsis

Background: Defendant was convicted in the Circuit Court, Cecil County, Richard E. Jackson, J., of second-degree murder, first-degree assault, and use of a handgun in the commission of a felony or crime of violence. The assault conviction merged into the murder conviction. Defendant appealed. The Court of Special Appeals affirmed, 192 Md.App. 518, 995 A.2d 791. Defendant petitioned for a writ of certiorari, and the stated filed a conditional cross petition. Both petitions were granted.

Holdings: The Court of Appeals, Battaglia, J., held that:

[1] the state did not sufficiently authenticate pages that allegedly were printed from defendant's girlfriend's profile on a social-networking website, and

[2] error in trial court's admission of the pages was reversible error.

Reversed and remanded within instructions.

Harrell, J., dissented and filed opinion in which Murphy, J., joined.

West Headnotes (6)

[1] Criminal Law
Documentary evidence

Defendant preserved for appellate review his challenge to the authenticity of pages that allegedly were printed from his girlfriend's profile on a social-networking website; defendant explicitly objected to the admission of the printed pages. Md.Rule 5–901.

1 Cases that cite this headnote

[2] Criminal Law
Telecommunications

The state did not sufficiently authenticate pages that allegedly were printed from defendant's girlfriend's profile on a social-networking website, and thus the pages, which allegedly contained a statement by the girlfriend that "snitches get stitches," were inadmissible at a murder trial, even though the pages contained a picture of the girlfriend, her birth date, and her location; the state did not ask the girlfriend whether the profile was hers and whether its contents were authored by her, and the picture, birth date, and location were not authenticating distinctive characteristics, given the prospect for abuse and manipulation of a social-networking website by someone other than the purported creator or user. Md.Rule 5–901(b)(1, 4).

8 Cases that cite this headnote

[3] Criminal Law
Documentary and demonstrative evidence

Error in trial court's admission of unauthenticated pages that allegedly were printed from defendant's girlfriend's profile on a social-networking website was reversible error at a murder trial; the pages, which allegedly contained a statement by the girlfriend that "snitches get stitches," were used to show that the girlfriend had threatened a key witness, the state highlighted the "stitches" posting during closing argument, and the state again referenced the pages during rebuttal argument, asserting that the girlfriend had employed the website as a tool of intimidation against a witness for the state. Md.Rule 5–901(b)(1, 4).

1 Cases that cite this headnote

[4] **Criminal Law**
Telecommunications

One method for authenticating printouts of a profile and a posting on a social-networking website would be to ask the purported creator if she indeed created the profile and also if she added the posting in question, which would constitute testimony of a witness with knowledge that the offered evidence is what it is claimed to be. Md.Rule 5–901(b)(1).

9 Cases that cite this headnote

[5] **Criminal Law**
Telecommunications

One method for authenticating printouts of a profile and a posting on a social-networking website 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 profile and posting in question. Md.Rule 5–901(b).

9 Cases that cite this headnote

[6] **Criminal Law**
Telecommunications

One method for authenticating printouts of a profile and a posting on a social-networking website may be to obtain information directly from the website 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. Md.Rule 5–901(b).

9 Cases that cite this headnote

Attorneys and Law Firms

****416** Katherine P. Rasin, Asst. Public Defender (Paul B. DeWolfe, Public Defender, Baltimore, MD), on brief, for petitioner/cross-respondent.

Robert Taylor, Jr., Asst. Atty. Gen. (Douglas F. Gansler, Atty. Gen. of Maryland, Baltimore, MD), on brief, for respondent/cross-petitioner.

Argued by BELL, C.J., HARRELL, BATTAGLIA, GREENE, MURPHY, ADKINS and BARBERA, JJ.

Opinion

BATTAGLIA, J.

***346** In this case, we are tasked with determining the appropriate way to authenticate, for evidential purposes, electronically stored information printed from a social ****417** networking website, [1] in particular, MySpace. [2]

[1] Antoine Levar Griffin, Petitioner, seeks reversal of his convictions in the Circuit Court for Cecil County, contending that the trial judge abused his discretion in admitting, without proper authentication, what the State alleged were several pages printed from Griffin's girlfriend's MySpace profile. [3] The Court of Special Appeals determined that the trial judge did not abuse his discretion, *Griffin v. State,* 192 Md.App. 518, 995 A.2d 791 (2010), and we granted Griffin's Petition for Writ of Certiorari, 415 Md. 607, 4 A.3d 512 (2010), to consider the two questions, which we have rephrased:

> 1. Did the trial court err in admitting a page printed from a MySpace profile alleged to be that of Petitioner's girlfriend? [4]
>
> ***347** 2. Did the trial court err in allowing the prosecutor to define reasonable doubt incorrectly over defense objection, including saying "it means this, do you have a good reason to believe that somebody other than Mr. Griffin was the person that shot Darvell Guest ... I'm not asking you whether you can speculate and create some construct of hypothetical possibilities that would have somebody else be the shooter.... I'm asking you the question, do you have right now any reason, any rational reason to believe that somebody other than he was the shooter or gunman?" [5]

The State presented a conditional cross-petition, which we also granted, in which one question was posed:

> 1. Is Griffin's challenge to the probative value of the evidence preserved for appellate review? [6]

****418** We shall hold that the pages allegedly printed from Griffin's girlfriend's MySpace profile were not properly authenticated pursuant to Maryland Rule 5–901,[7] and shall, therefore, reverse ***348** the judgment of the Court of Special Appeals and remand the case for a new trial.

Griffin was charged in numerous counts with the shooting death, on April 24, 2005, of Darvell Guest at Ferrari's Bar in Perryville, in Cecil County. During his trial, the State sought to introduce Griffin's girlfriend's, Jessica Barber's, MySpace profile to demonstrate that, prior to trial, Ms. Barber had allegedly threatened another witness called by the State. The printed pages contained a MySpace profile in the name of "Sistasouljah," describing a 23 year-old female from Port Deposit, listing her birthday as "10/02/1983" and containing a photograph of an embracing couple. The printed pages also contained the following blurb:

> FREE BOOZY!!!! JUST REMEMBER SNITCHES GET STITCHES!! U KNOW WHO YOU ARE!!

When Ms. Barber had taken the stand after being called by the State, she was not questioned about the pages allegedly printed from her MySpace profile.

Instead, the State attempted to authenticate the pages, as belonging to Ms. Barber, through the testimony of Sergeant John Cook, the lead investigator in the case. Defense counsel objected to the admission of the pages allegedly printed from Ms. Barber's MySpace profile, because the State could not sufficiently establish a "connection" between the profile and posting and Ms. Barber, and substantively, the State could not say with any certainty that the purported "threat" had any ***349** impact on the witness's testimony; the latter argument is not before us.

Defense counsel was permitted to voir dire Sergeant Cook, outside of the presence of the jury, as follows:

[Defense Counsel]: How do you know that this is her [MySpace] page?....

[Sergeant Cook]: Through the photograph of her and Boozy on the front, through the reference to Boozy, [ ] the reference [to] the children, and [ ] her birth date indicated on the form.

[Defense Counsel]: How do you know she sent it?

[Sergeant Cook]: I can't say that.

[The Court]: I failed—I am sorry. I misrepresented. I failed to realize there is a photograph there. It's in the block ****419** that says "Sistasouljah," and then there's a photograph of a person that looks like Jessica Barber to me.

[Defense Counsel]: When was it sent?

[Sergeant Cook]: That is a MySpace page. That wasn't particularly sent. That is on the web, and it's accessible to whoever views MySpace. It is open to the public.

[Defense Counsel]: I understand that. When did it get posted?

[Sergeant Cook]: The print date on the form, printed on 12/05/06.

[The Court]: You can tell by looking at it because that's when he went to it.

[Defense Counsel]: So that would have been after the first trial. So how could that possibly affect [the witness]? He said it was before the first trial.

[The 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.

***350** [Assistant State's Attorney]: That's correct.

[The Court]: It's weak. I mean, there is no question it's weak, but that's what it is offered for.

The trial judge, thereafter, indicated that he would permit Sergeant Cook to testify in support of authentication of the redacted portion of the pages printed from MySpace, containing the photograph "of a person that looks like Jessica Barber" and the Petitioner, allegedly known as "Boozy," adjacent to a description of the woman as a 23 year-old from Port Deposit, and the blurb, stating "FREE BOOZY!!!! JUST REMEMBER SNITCHES GET STITCHES!! U KNOW WHO YOU ARE!!"

In lieu of Sergeant Cook's testimony, while maintaining his objection to the admissibility of the redacted MySpace page, defense counsel agreed to the following stipulation:

> If asked, Sergeant Cook would testify that he went onto the Internet to the website known as MySpace.... [F]rom that site he downloaded some information of a posting that someone had put there.
>
> That posting contains a photograph which the witness would say he recognizes as a photograph of Jessica ... Barber, who testified, ... that she is the defendant's live-in fiance; and that it also contains a date of birth, to wit October 2nd, 1983, which the witness would testify is the date of birth that Jessica Barber gave as her date of birth.
>
> When the exhibit, the download, comes to you, you are going to see that it has a great—that most of its content has been redacted; that is, blacked out. That's because some of it, in my judgment, might tend to be inflammatory without proving anything one way or the other. There is one portion of it that will not be redacted when it comes to you, and this is the only portion of it which you should consider. And you certainly should not speculate as to what any of the redacted portions may be.
>
> The portion that will not be redacted says, just remember snitches get stitches. You will see that. The phrase is, just remember snitches get stitches.... And ... the witness ***351** would testify that the date it was retrieved was ... December 5, 2006.

Whether the MySpace printout represents that which it purports to be, not only a MySpace profile created by Ms. Barber, ****420** but also upon which she had posted, "FREE BOOZY!!!! JUST REMEMBER SNITCHES GET STITCHES!! U KNOW WHO YOU ARE!!," is the issue before us.

With respect to social networking websites in general, we have already had occasion, in *Independent Newspapers, Inc. v. Brodie,* 407 Md. 415, 424 n. 3, 966 A.2d 432, 438 n. 3 (2009), to describe those sites as "sophisticated tools of communication where the user voluntarily provides information that the user wants to share with others." [8] A number of social networking websites, such as MySpace, enable members "to create online 'profiles,' which are individual web pages on which members [can] post photographs, videos, and information about their lives and interests." *Doe v. MySpace, Inc.,* 474 F.Supp.2d 843, 845 (W.D.Tex.2007).

Anyone can create a MySpace profile at no cost, as long as that person has an email address and claims to be over the age of fourteen:

> MySpace users create profiles by filling out questionnaire-like web forms. Users are then able to connect their profiles to those of other users and thereby form communities. MySpace profiles contain several informational sections, known as "blurbs." These include two standard blurbs: "About Me" and "Who I'd Like to Meet." Users may supplement those blurbs with additional sections about their interests, general additional details, and other personal information. MySpace profiles also incorporate several ***352** multimedia features. For instance, users may post photos, music, videos, and web logs to their pages.

Richard M. Guo, *Stranger Danger and the Online Social Network,* 23 Berkeley Tech. L.J. 617, 621 (2008) (footnotes omitted). After a profile is established, the user may invite others to access her profile, as a "friend," who if the user accepts the befriending, can access her profile pages without further ado:

> Users establish virtual communities by linking their profiles in a process known as "friending" or "connecting." One user requests to add another as a friend, and the recipient may either accept or reject the

> invitation. If the recipient accepts, the profiles are linked and the connected members are generally able to view one another's online content without restriction. The network created by the linking process allows a user to chat with friends, display support for particular causes, "join interest groups dedicated to virtually any topic," and otherwise "hang out."

Nathan Petrashek, Comment, *The Fourth Amendment and the Brave New World of Online Social Networking,* 93 Marq. L.Rev. 1495, 1499–1500 (2009–2010) (footnotes omitted). Although a social networking site generally requires a unique username and password for the user to both establish a profile and access it, posting on the site by those that befriend the user does not. *See* Samantha L. Miller, Note, *The Facebook Frontier: Responding to the Changing Face of Privacy on the Internet,* 97 Ky. L.J. 541, 544 (2008–2009); Eric Danowitz, *MySpace Invasion: Privacy Rights, Libel, and Liability,* 28 J. Juv. L. 30, 37 (2007).

****421** The identity of who generated the profile may be confounding, because "a person observing the online profile of a user with whom the observer is unacquainted has no idea whether the profile is legitimate." Petrashek, 93 Marq. L.Rev. at 1499 n. 16. The concern arises because anyone can create a fictitious account and masquerade under another person's name or can gain access to another's account by obtaining the user's username and password:

> ***353** Although it may seem that, as creators of our own online social networking profiles, we are able to construct our own online persona, this is not always the case. There is no law that prevents someone from establishing a fake account under another person's name, so long as the purpose for doing so is not to deceive others and gain some advantage. Moreover, fragments of information, either crafted under our authority or fabricated by others, are available by performing a Google search ... forever. Thus, online social networking poses two threats: that information may be (1) available because of one's own role as the creator of the content, or (2) generated by a third party, whether or not it is accurate.

David Hector Montes, *Living Our Lives Online: The Privacy Implications of Online Social Networking,* Journal of Law and Policy for the Information Society, Spring 2009, at 507, 508. For instance, in one circumstance, Sophos, a Boston-based Internet security company, created a profile for a toy frog named "Freddi Staur," and nearly 200 Facebook [9] users ***354** chose to add the frog as a "friend." Miller, 97 Ky. L.J. at 542. [10]

The possibility for user abuse also exists on MySpace, as illustrated by *United States v. Drew,* 259 F.R.D. 449 (D.C.D.Cal.2009), in which Lori Drew, a mother, was prosecuted under the Computer Fraud and ****422** Abuse Act, 18 U.S.C. § 1030, for creating a MySpace profile for a fictitious 16 year-old male named "Josh Evans." Drew had contacted a former friend of her daughter's, Megan Meier, through the MySpace network, using the Josh Evans screen name or pseudonym, and began to "flirt with her over a number of days." *Id.* at 452. Drew then had "Josh" inform Megan that he no longer "liked her" and that "the world would be a better place without her in it," after which Megan killed herself. *Id.* Thus, the relative ease with which anyone can create fictional personas or gain unauthorized access to another user's profile, with deleterious consequences, is the *Drew* lesson.

The potential for fabricating or tampering with electronically stored information on a social networking site, thus poses significant challenges from the standpoint of authentication of printouts of the site, as in the present case. Authentication, nevertheless, is generally governed by Maryland Rule 5–901, which provides:

> (a) **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.

***355** Potential methods of authentication are illustrated in Rule 5–901(b). The most germane to the present inquiry are Rules 5–901(b)(1) and 5–901(b)(4), which state:

> (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. [11]

(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.

We and our colleagues on the Court of Special Appeals have had the opportunity to apply the tenets of Rule 5–901(b)(4) to a toxicology report, *State v. Bryant,* 361 Md. 420, 761 A.2d 925 (2000), to recordings from 911 emergency calls, *Clark v. State,* 188 Md.App. 110, 981 A.2d 666 (2009), and to text messages received on the victim's cellular phone, *Dickens v. State,* 175 Md.App. 231, 927 A.2d 32 (2007), but neither we nor our appellate brethren heretofore has considered the Rule's application to authenticate pages printed from a social networking site.

Rather, we turn for assistance to the discussion in *Lorraine v. Markel American Insurance Co.,* 241 F.R.D. 534 (D.Md.2007), wherein Maryland's own Magistrate Judge Paul W. ***356** Grimm, a recognized authority on evidentiary issues concerning electronic evidence, outlined issues regarding authentication of electronically stored information, in e-mail, websites, digital photographs, computer-generated documents, ****423** and internet postings, etc. with respect to Rule 901 of the Federal Rules of Evidence:

(a) **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.

(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 that a matter is what it is claimed to be.

* * *

(4) *Distinctive Characteristics and the Like.* Appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances.

Regarding Rule 901(a), Judge Grimm iterated in *Lorraine* that 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," to insure trustworthiness. *Id.* at 541–42. Judge Grimm recognized that authenticating electronically stored information presents a myriad of concerns because "technology changes so rapidly" and is "often new to many judges." *Id.* at 544. Moreover, the "complexity" or "novelty" of electronically stored information, with its potential for manipulation, requires greater scrutiny of "the foundational requirements" than letters or other paper records, to bolster reliability. *Id.* at 543–44, quoting Jack B. Weinstein & Margaret A. Berger, *Weinstein's Federal Evidence* § 900.06[3] (Joseph M. McLaughlin ed., Matthew Bender 2d ed.1997).

[2] In the present case, Griffin argues that the State did not appropriately, for evidentiary purposes, authenticate the ***357** pages allegedly printed from Jessica Barber's MySpace profile, because the State failed to offer any extrinsic evidence describing MySpace, as well as indicating how Sergeant Cook obtained the pages in question and adequately linking both the profile and the "snitches get stitches" posting to Ms. Barber. The State counters that the photograph, personal information, and references to freeing "Boozy" were sufficient to enable the finder of fact to believe that the pages printed from MySpace were indeed Ms. Barber's.

We agree with Griffin and disagree with the State regarding whether the trial judge abused his discretion in admitting the MySpace profile as appropriately authenticated, with Jessica Barber as its creator and user, as well as the author of the "snitches get stitches" posting, based upon the inadequate foundation laid. We differ from our colleagues on the Court of Special Appeals, who gave short shrift to the concern that "someone other than the alleged author may have accessed the account and posted the message in question." *Griffin,* 192 Md.App. at 542, 995 A.2d at 805. While the intermediate appellate court determined that the pages allegedly printed from Ms. Barber's MySpace profile contained sufficient indicia

of reliability, because the printout "featured a photograph of Ms. Barber and [Petitioner] in an embrace," and also contained the "user's birth date and identified her boyfriend as 'Boozy,' " the court failed to acknowledge the possibility or likelihood that another user could have created the profile in issue or authored the "snitches get stitches" posting. *Id.* at 543, 995 A.2d at 806.

We agree with Griffin that the trial judge abused his discretion in admitting ****424** the MySpace evidence pursuant to Rule 5–901(b)(4), because the picture of Ms. Barber, coupled with her birth date 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 ***358** 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. [12]

In so holding, we recognize that other courts, called upon to consider authentication of electronically stored information on social networking sites, have suggested greater scrutiny because of the heightened possibility for manipulation by other than the true user or poster. In *Commonwealth v. Williams,* 456 Mass. 857, 926 N.E.2d 1162 (2010), the Supreme Judicial Court of Massachusetts considered the admission, over the defendant's objection, of instant messages a witness had received "at her account at MySpace." *Id.* at 1171. In the case, the defendant was convicted of the shooting death of Izaah Tucker, as well as other offenses. The witness, Ashlei Noyes, ***359** testified that she had spent the evening of the murder socializing with the defendant and that he had been carrying a handgun. She further testified that the defendant's brother had contacted her "four times on her MySpace account between February 9, 2007, and February 12, 2007," urging her "not to testify or to claim a lack of memory regarding the events of the night of the murder." *Id.* at 1172. At trial, Noyes testified that the defendant's brother, Jesse Williams, had a picture of himself on his MySpace account and that his MySpace screen name or pseudonym was "doit4it." She testified that she had received the messages from Williams, and the document printed from her MySpace account indicated that the messages were in fact sent by a user with the screen name ****425** "doit4it," depicting a picture of Williams. *Id.*

The Supreme Judicial Court of Massachusetts determined that there was an inadequate foundation laid to authenticate the MySpace messages, because the State failed to offer any evidence regarding who had access to the MySpace page and whether another author, other than Williams, could have virtually-penned the messages:

> Although it appears that the sender of the messages was using Williams's MySpace Web "page," there is no testimony (from Noyes 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. Analogizing a MySpace [message] to a telephone call, a witness's 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." Here, while the foundational testimony established that the messages were sent by someone with access to Williams'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.

Id. at 1172–73 (citations omitted). The court emphasized that the State failed to demonstrate a sufficient connection between ***360** the messages printed from Williams's alleged MySpace account and Williams himself, with reference, for example, to Williams's use of an exclusive username and password to which only he had access. The court determined that the error in admitting the improperly authenticated MySpace messages "did not create a substantial likelihood of a miscarriage of justice," however, and, therefore, did not reverse Williams's

conviction, because Noyes's testimony was significantly overshadowed "by the testimony of two witnesses to the murder who identified Williams as the shooter." *Id.* at 1173.

Similarly, in *People v. Lenihan,* 30 Misc.3d 289, 911 N.Y.S.2d 588 (N.Y.Sup.Ct.2010), Lenihan challenged his second degree murder conviction because he was not permitted to cross-examine two witnesses called by the State on the basis of photographs his mother had printed from MySpace, allegedly depicting the witnesses and the victim making hand gestures and wearing clothing that suggested an affiliation with the "Crips" gang. The trial judge precluded Lenihan from confronting the witnesses with the MySpace photographs, reasoning that "[i]n light of the ability to 'photo shop,' edit photographs on the computer," Lenihan could not adequately authenticate the photographs. *Id.* at 592.

In *United States v. Jackson,* 208 F.3d 633 (7th Cir.2000), Jackson was charged with mail and wire fraud and obstruction of justice after making false claims of racial harassment against the United Parcel Service in connection with an elaborate scheme in which she sent packages containing racial epithets to herself and to several prominent African–Americans purportedly from "racist elements" within UPS. *Id.* at 635. At trial, Jackson sought to introduce website postings from "the Euro–American Student Union and Storm Front," in which the white supremacist groups gloated about Jackson's case and took credit for the UPS mailings. *Id.* at 637. The court determined that the trial judge was justified in excluding the evidence because it lacked an appropriate foundation, namely that Jackson had failed to show that the web postings by the white ****426** supremacist groups who took responsibility for ***361** the racist mailings "actually were posted by the groups, as opposed to being slipped onto the groups' websites by Jackson herself, who was a skilled computer user." *Id.* at 638.

The State refers us, however, to *In the Interest of F.P.,* 878 A.2d 91 (Pa.Super.Ct.2005), in which the Pennsylvania intermediate appellate court considered whether instant messages were properly authenticated pursuant to Pennsylvania Rule of Evidence 901(b)(4), providing that a document may be authenticated by distinctive characteristics or circumstantial evidence. In the case, involving an assault, the victim, Z.G., testified that the defendant had attacked him because he believed that Z.G. had stolen a DVD from him. The hearing judge, over defendant's objection, admitted instant messages from a user with the screen name "Icp4Life30" to and between "WHITEBOY Z 404." *Id.* at 94. Z.G. testified that his screen name was "WHITEBOY Z 404" and that he had printed the instant messages from his computer. In the transcript of the instant messages, moreover, Z.G. asked "who is this," and the defendant replied, using his first name. Throughout the transcripts, the defendant threatened Z.G. with physical violence because Z.G. "stole off [him]." *Id.* On appeal, the court determined that the instant messages were properly authenticated through the testimony of Z.G. and also because "Icp4Life30" had referred to himself by first name, repeatedly accused Z.G. of stealing from him, and referenced the fact that Z.G. had told high school administrators about the threats, such that the instant messages contained distinctive characteristics and content linking them to the defendant. *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. [13]

***362** Similarly, the State relies upon an unreported opinion, *State v. Bell,* 2009 WL 1395857, 2009 Ohio App. LEXIS 2112 (Ohio Ct.App.2009), in which the defendant, convicted of multiple counts of child molestation, asserted that the trial judge ****427** improperly admitted "online conversations and email messages" on MySpace, purportedly involving Bell and one of his victims. The defendant argued that the messages were not properly authenticated, because his laptop "was turned on after it was seized," which he asserted altered hundreds of files on the hard drive. *Id.* at *4, 2009 Ohio App. LEXIS 2112 at *10. The appellate court rejected that argument because defense counsel had expressly approved the admission of the MySpace emails and messages. Griffin, in the present case, however, explicitly objected to the authenticity of the MySpace printout.

[3] In the case sub judice, the MySpace printout was used to show that Ms. Barber had threatened a key witness, who the State had characterized as "probably the most important witness in this case;" the State highlighted the importance of ***363** the "snitches get stitches" posting during closing argument, as follows:

> Sergeant Cook told you that he went online and went to a website called MySpace and found a posting that had been placed there by the defendant's girlfriend, Jessica Barber, recognized her picture, able to match up the date of birth on the posting with her date of birth, and the posting included these words, "Free Boozy. Just remember, snitches get stitches. You know who you are."

In addition, during rebuttal argument, the State again referenced the pages printed from MySpace, asserting that Ms. Barber had employed MySpace as a tool of intimidation against a witness for the State. It is clear, then, that the MySpace printout was a key component of the State's case; the error in the admission of its printout requires reversal.

In so doing, we 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. *See, e.g.,* 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). A number of authentication opportunities come to mind, however.

[4] **[5]** 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, i.e. "[t]estimony of a witness with knowledge that the offered evidence is what it is claimed to be." Rule 5–901(b)(1). The second option 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. One commentator, who serves as Managing Director and Deputy General Counsel ***364** of Stroz Friedberg, [14] a computer forensics firm, notes that, "[s]ince a user unwittingly leaves an evidentiary trail on her computer simply by using it, her computer will provide evidence of her web usage." Seth P. Berman, et al., *Web 2. 0:* ****428** *What's Evidence Between "Friends"?,* Boston Bar J., Jan.-Feb.2009, at 5, 7.

[6] A third method may be to obtain information directly from the social networking website 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. This method was apparently successfully employed to authenticate a MySpace site in *People v. Clevenstine,* 68 A.D.3d 1448, 891 N.Y.S.2d 511 (2009). In the case, Richard Clevenstine was convicted of raping two teenage girls and challenged his convictions by asserting that the computer disk admitted into evidence, containing instant messages between him and the victims, sent via MySpace, was not properly authenticated. Specifically, Clevenstine argued that "someone else accessed his MySpace account and sent messages under his username." *Id.* at 514. The Supreme Court of New York, Appellate Division, agreed with the trial judge that the MySpace messages were properly authenticated, because both victims testified that they had engaged in instant messaging conversations about sexual activities with Clevenstine through MySpace. In addition, an investigator from the computer crime unit of the State Police testified that "he had retrieved such conversations from the hard drive of the computer used by the victims." *Id.* Finally, the prosecution was able to attribute the messages to Clevenstine, because a legal compliance officer for MySpace explained at trial that "the messages on the computer disk had been exchanged by users of accounts created by [Clevenstine] and the victims." *Id.* The ***365** court concluded that such testimony provided ample authentication linking the MySpace messages in question to Clevenstine himself. [15]

JUDGMENT OF THE COURT OF SPECIAL APPEALS REVERSED. CASE REMANDED TO THAT COURT WITH INSTRUCTIONS TO REVERSE THE JUDGMENT OF THE CIRCUIT COURT FOR CECIL COUNTY AND REMAND THE CASE TO THE CIRCUIT COURT FOR A NEW TRIAL. COSTS IN THIS COURT AND IN THE COURT OF SPECIAL APPEALS TO BE PAID BY CECIL COUNTY.

HARRELL and MURPHY, JJ., dissent.

HARRELL, J., dissenting in which MURPHY, J., joins.

I dissent from the Majority Opinion's holding that "the picture of Ms. Barber, coupled with her birth date and

location, were not sufficient 'distinctive characteristics' on a MySpace profile to authenticate its [redacted] printout....” 419 Md. 343, 357, 19 A.3d 415, 424 (2011).

Maryland Rule 5–901 (“Requirement of authentication or identification”) derives from and is similar materially to Federal Rule of Evidence 901.[1] *See* ***366** *Washington v.* ****429** *State,* 406 Md. 642, 651, 961 A.2d 1110, 1115 (2008). Thus, federal cases construing the federal rule are almost direct authority impacting on our construction of a Maryland analog rule. *See Higgins v. Barnes,* 310 Md. 532, 543, 530 A.2d 724, 729 (1987) (“Maryland courts have traditionally relied on the federal courts' interpretations of analogous rules as persuasive authority....”). In construing and applying Federal Rule 901, federal courts have held almost unanimously that “a document is properly authenticated if a *reasonable juror could find in favor of authenticity.*” *United States v. Gagliardi,* 506 F.3d 140, 151 (2d Cir.2007) (emphasis added); *see United States v. Twitty,* 72 F.3d 228, 232 (1st Cir.1995); *United States v. Rawlins,* 606 F.3d 73, 82 (3d Cir.2010); *United States v. Branch,* 970 F.2d 1368, 1370 (4th Cir. 1992); *United States v. Logan,* 949 F.2d 1370, 1377 n. 12 (5th Cir. 1991); *United States v. Jones,* 107 F.3d 1147, 1150 n. 1 (6th Cir. 1997); *United States v. Dombrowski,* 877 F.2d 520, 525 (7th Cir.1989); *United States v. Tank,* 200 F.3d 627, 630 (9th Cir.2000); *United States v. Blackwell,* 694 F.2d 1325, 1331 (D.C.Cir.1982). Although, to date, we have not enunciated such a standard, because I think that the “reasonable juror” standard is consistent with Maryland Rule 5–901—requiring only “ evidence *sufficient to support a finding* that the matter in question is what its proponent claims” (emphasis added)—I would adopt it.[2] *See* ***367** *Dickens v. State,* 175 Md.App. 231, 239, 927 A.2d 32, 37 (2007) (citing *United States v. Safavian,* 435 F.Supp.2d 36, 38 (D.D.C.2006)) (stating that “the burden of proof for authentication is slight”).

Applying that standard to the present case, a reasonable juror could conclude, based on the presence on the MySpace profile of (1) a picture of a person appearing to Sergeant Cook to be Ms. Barber posing with the defendant, her boyfriend; (2) a birth date 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.

I am not unmindful of the Majority Opinion's analysis relating to the concern that someone other than Ms. Barber could access or create the account and post the ****430** threatening message. The record, however, suggests no motive to do so. The technological heebie jeebies[3] discussed in the Majority Opinion go, in my opinion, however, not to the admissibility of the print-outs under Rule 5–901, but rather to the weight to be given the evidence by the trier of fact. *See Hays v. State,* 40 Md. 633, 648 (1874) (holding that where there was evidence that a paper was what it purported to be, it was not error for ***368** the trial court to instruct the jury that “if they were not satisfied of the identity of the paper ..., then they should not consider it all”); LYNN MCLAIN, MARYLAND EVIDENCE—STATE AND FEDERAL § 901:1 (2001) (stating that “authentication of an item is only the first step”).

It has been said that the “purpose of authentication is to ... filter untrustworthy evidence.” *Phillip M. Adams & Assocs., L.L.C. v. Dell, Inc.,* 621 F.Supp.2d 1173, 1184 (D.Utah 2009). 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. *See Gerald v. State,* 137 Md.App. 295, 304, 768 A.2d 140, 145 (2001) (stating that, after a trial court admits a document as being authenticated properly, “the ultimate question of authenticity is left to the jury”). 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. Accordingly, I dissent.

Judge MURPHY authorizes me to state that he joins in the views expressed in this dissent.

All Citations

419 Md. 343, 19 A.3d 415

Footnotes

1 The term “website” refers to “a collection of documents and related files that are owned or organized by a particular individual or organization.” Jonathan Wilson, *What's In a Web Site?,* Ga. B.J., Apr. 1999, at 14, 14.

2 “MySpace is a ‘social networking’ website where members can create ‘profiles' and interact with other members. Anyone with Internet access can go onto the MySpace website and view content which is open to the general public such as a music area, video section, and members' profiles which are not set as ‘private.’ However, to create a profile, upload and display photographs, communicate with persons on the site, write ‘blogs,’ and/or utilize other services or applications on the MySpace website, one must be a ‘member.’ Anyone can become a member of MySpace at no charge so long as they meet a minimum age requirement and register.” *United States v. Drew,* 259 F.R.D. 449, 453 (D.C.D.Cal.2009).

3 To establish a “profile,” a user needs only a valid email account. Patricia Sanchez Abril, *A (My)Space of One's Own: On Privacy and Online Social Networks,* 6 Nw. J. Tech. & Intell. Prop. 73, 74 (2007). Generally, a user creates a profile by “filling out a series of virtual forms eliciting a broad range of personal data,” culminating in a multimedia collage that serves as “one's digital ‘face’ in cyberspace.” Nathan Petrashek, Comment, *The Fourth Amendment and the Brave New World of Online Social Networking,* 93 Marq. L.Rev. 1495, 1499 (Summer 2010).

4 In his Petition for Writ of Certiorari, Griffin presented three questions pertaining to the MySpace evidence, namely:

> 1. What evidence is required to authenticate a printout from a social networking website?
>
> 2. Did the court err in admitting what the State claimed was a printout from petitioner's girlfriend's MySpace profile containing highly prejudicial content without properly authenticating the material as having been posted by petitioner's girlfriend?
>
> 3. Did the Court of Special Appeals err in finding that the prejudice to petitioner from the admission of the MySpace page did not outweigh its probative value?

5 Because of our disposition of the first issue, we need not and will not address the second question presented.

6 To the extent that the question presented in the State's cross-petition concerns the preservation of Griffin's challenge to the authenticity of the MySpace evidence, the authenticity issue was clearly preserved for appellate review by Griffin's explicit objection to the admission of the printed pages. Insofar as the State contends that Griffin failed to preserve his challenge to the probity of the MySpace evidence, we need not and will not address that issue, because evidence that has not been properly authenticated is inadmissible, regardless of its probity or potentially prejudicial effect.

7 Rule 5–901, describing the requirement of authentication or identification, provides, in pertinent part:

> (a) **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.
>
> (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.

8 Social networking websites, which offer a framework in which users interact and create content themselves, is an application of “Web 2.0,” a phrase that does not refer to any specific new technology, but refers instead to the “participatory nature of how a website's content is created and delivered.” Seth P. Berman, Lam D. Nguyen & Julie S. Chrzan, *Web 2.0: What's Evidence Between “Friends”?,* Boston Bar J., Jan.-Feb.2009, at 5, 5.

9 Facebook, the behemoth of the social networking world, allows users to build a profile and interact with “friends” in much the same way as MySpace:

> Facebook prompts new users to supply their name, e-mail address, sex, and birth date. Perhaps as a vestige of Facebook's restrictive roots, users are also asked to name any high schools, colleges, or universities attended. Users may build upon this foundation by supplying additional information in any of four sections that compose the profile: “Basic Information,” which includes the user's current city, hometown, relationship status, and political and religious views; “Personal Information,” which includes interests, activities, and favorite music, movies, and books; “Contact Information,” which includes websites, addresses, phone numbers, and instant messaging screen names; and “Education and Work,” which is largely self descriptive. “Status” posts allow users to update their profiles with up-to-the-minute information, offering users a virtual soapbox to their online community.

Facebook's community element is perhaps more sophisticated than that of MySpace. The web site's design makes it easy for users to "compile lists of their friends, post public comments on friends' profiles, ... send private messages to other users[,] ... [and] create groups of people with similar interests...." Members may upload photographs, and both Facebook and MySpace allow users to "tag" their friends in the image. Tagging "creates a link [in] the individual's profile from the photograph, making users easily identifiable, even when the viewer of the photograph is not 'friends' with the photograph's subjects."

Petrashek, 93 Marq. L.Rev. at 1506–07 (footnotes omitted).

10 Sophos apparently conducted the study to demonstrate that it "was able to acquire highly personal information from [forty percent] of the nearly 200 Facebook users who chose to add 'Freddie Staur' as a friend in their Facebook accounts." Mint.com, *HOWTO: Protect Your Privacy on Facebook, MySpace, and LinkedIn* (Sept. 6, 2007), http://www.blog.mint.com/blog/moneyhack/howto-protect-your-privacy-on-facebook-myspace-and-linkedin/.

11 We add this section to highlight 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. *See United States v. Barlow,* 568 F.3d 215, 220 (5th Cir.2009) (reasoning that testimony of witness who had posed as a minor female that the transcripts fairly and fully reproduced the online chats was sufficient to authenticate them for admission); *United States v. Gagliardi,* 506 F.3d 140, 151 (2d Cir.2007) (reasoning that chat room logs were properly authenticated as having been sent by the defendant through testimony from witnesses who had participated in the online conversations).

* * *

12 The dissent minimizes as "the technological heebie jeebies" the challenges inherent in authenticating, for evidentiary purposes, social networking websites. *None* of the authorities cited by the dissent in support of its conclusion, however, even addresses the authentication of social networking sites. Only one case, *United States v. Gagliardi,* 506 F.3d 140, 151 (2d Cir.2007), involves digital communications, namely Internet chat room conversations, which the Second Circuit recognized were appropriately authenticated by witnesses who had participated in the "chats," clearly persons "with knowledge." *See* Federal Rule 901(b)(1).

In addition, the "reasonable juror" standard to which the dissent refers is apparently derived from the federal analogue to Maryland Rule 5–104(b), concerning "relevance conditioned on fact," a protocol not addressed in this case, which we discuss in footnote 15, infra. *See United States v. Logan,* 949 F.2d 1370, 1377 n. 12 (5th Cir.1991) (reasoning that in determining whether to admit evidence of disputed authenticity, the court should utilize the protocol established in Federal Rule 104(b), namely that "the judge [ ] make a preliminary determination [as to] whether a jury could reasonably conclude" that the evidence is what it purports to be).

Finally, authentication of evidence must be addressed by the trial court whether or not motive to fabricate or manipulate is raised by anyone or is in issue. *See* Lynn McLain, 6A *Maryland Evidence—State and Federal* § 901:1 (2001) ("Under Maryland law, generally ... an object, writing, telephone conversation, or tape recording is not self-authenticating. Some evidence other than the item or reported conversation itself is required to establish that it is what its proponent says it is, or comes from the source which its proponent professes.").

13 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. *See Independent Newspapers, Inc. v. Brodie,* 407 Md. 415, 423, 966 A.2d 432, 437 (2009) (contrasting emails and instant messages with a "different category of Internet communications, in which users post statements to the world at large without specification," such as on social networking sites). *See also United States v. Safavian,* 435 F.Supp.2d 36, 41 (D.D.C.2006) (reasoning e-mails could be authenticated by comparison by the jury with those e-mails that had already been independently authenticated through the contents or in the email heading itself); *Commonwealth v. Amaral,* 78 Mass.App.Ct. 671, 674, 941 N.E.2d 1143, 1147 (2011) (reasoning that "[t]he actions of the defendant himself served to authenticate the e-mails," because one e-mail indicated that defendant would be at a certain place at a certain time and the defendant appeared at that place and time, and in another email, defendant provided his telephone number and immediately answered when the investigator called that number); *Dickens v. State,* 175 Md.App. 231, 238–40, 927 A.2d 32, 36–37 (2007) (reasoning text messages received on victim's cell phone were properly authenticated because the phone number on one message showed that it had come from defendant's phone and other messages referenced the defendant's right to see the couple's minor child and their wedding vows).

14 According to the firm's website, Stroz Friedberg is a technical services firm specializing in the areas of computer forensics, mobile phone forensics, electronic discovery, data breach, cybercrime response, and investigations. Stroz Friedberg LLC

—Who We Are, http://www. strozfriedberg.com/methodology/xprGeneralContent1.aspx?xpST=Methodology (last visited Apr. 26, 2011).

15 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, however, have not been asked in this case to address the efficacy of the Rule 5–104(b) protocol.

1 Federal Rule of Evidence 901 provides, in pertinent part:

> (a) 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.
>
> (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 that a matter is what it is claimed to be.
>
> * * *
>
> (4) Distinctive characteristics and the like. Appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances.

2 Professor McLain explains:

> The item will be properly authenticated if its proponent has offered foundation evidence that the judge finds would be sufficient to support a finding by a reasonable trier of fact that the item is what it is purported to be. 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. In a jury trial, the judge need not be personally satisfied, by even a preponderance of the evidence, that the proffered item is authentic; the judge must find the authentication requirement met, if a reasonable jury could find the evidence to be what its proponent claims it to be.

LYNN MCLAIN, MARYLAND EVIDENCE—STATE AND FEDERAL § 901:1 (2001).

3 "Heebie jeebies" is an idiom used to describe anxiety, apprehension, or jitters; attributed to William Morgan ("Billy") De Beck, a cartoonist, in the 26 October 1923 edition of the *New York American. See also* LOUIS ARMSTRONG & THE HOT FIVE, HEEBIE JEEBIES (Okeh Records 1926) ("Say, I've got the heebies, I mean the jeebies, talkin about the dance, the heebie jeebies.").

85 A.3d 682
Supreme Court of Delaware.

Tiffany PARKER, Defendant Below–Appellant,
v.
STATE of Delaware, Plaintiff Below–Appellee.

No. 38, 2013.
|
Submitted: Nov. 6, 2013.
|
Decided: Feb. 5, 2014.

Synopsis

Background: Defendant was convicted in the Superior Court, New Castle County, of second-degree assault. Defendant appealed.

Holdings: The Supreme Court, Ridgely, J., held that:

[1] evidentiary rule governing authentication of evidence was appropriate standard for determining admissibility of social media network evidence, and

[2] post on defendant's social media network page indicating her involvement in assault was sufficiently authenticated as having been authored by defendant.

Affirmed.

West Headnotes (4)

[1] Criminal Law
Reception and Admissibility of Evidence

The Supreme Court reviews a trial judge's evidentiary rulings for abuse of discretion.

1 Cases that cite this headnote

[2] Criminal Law
Discretion of Lower Court

An "abuse of discretion" occurs when a court has exceeded the bounds of reason in view of the circumstances, or so ignored recognized rules of law or practice to produce injustice.

1 Cases that cite this headnote

[3] Criminal Law
Telecommunications

In determining admissibility of social media network evidence, trial court would make initial determination whether there was sufficient evidence that proffered evidence was what proponent claimed it to be, and if it so found, then it was up to jury to decide whether to accept or reject evidence. Rules of Evid., Rules 104, 901(b).

8 Cases that cite this headnote

[4] Criminal Law
Telecommunications

Post on defendant's social media profile page indicating her involvement in assault was sufficiently authenticated as having been authored by defendant; substance of post referenced physical altercation with victim, it was created on same day as altercation and referenced fight, and victim testified that she viewed defendant's post through mutual friend and that she "shared" post and published it to her own profile page. Rules of Evid., Rule 901(b).

7 Cases that cite this headnote

***682** Court Below: Superior Court of the State of Delaware in and for New Castle County, ID No. 01112001354.
Upon appeal from the Superior Court. **AFFIRMED.**

Attorneys and Law Firms

Santino Ceccotti, Esquire, of Wilmington, Delaware, for Appellant.

Andrew J. Vella, Esquire, of the Department of Justice, Wilmington, Delaware, for Appellee.

Before HOLLAND, BERGER, JACOBS, and RIDGELY, Justices, and NOBLE, Vice Chancellor, constituting the Court en banc.

Opinion

RIDGELY, Justice:

Defendant-below/Appellant, Tiffany Parker, appeals from a Superior Court jury conviction of Assault Second Degree. Parker claims that the Superior Court erred in admitting statements posted on her Facebook ***683** profile. The Superior Court admitted the evidence under Rule 901 of the Delaware Rules of Evidence. Parker argues that we should adopt the rule set forth in *Griffin v. State,* a Maryland Court of Appeals decision, to authenticate social media evidence. Under the Maryland approach, social media evidence may only be authenticated through the testimony of the creator, documentation of the internet history or hard drive of the purported creator's computer, or information obtained directly from the social networking site. Unless the proponent can demonstrate the authenticity of the social media post to the trial judge using these exacting requirements, the social media evidence will not be admitted and the jury cannot use it in their factual determination. Under this approach, social media evidence is only authenticated and admissible where the proponent can convince the trial judge that the social media post was not falsified or created by another user.

Conversely, the State advocates for the Texas approach, under which a proponent can authenticate social media evidence using any type of evidence so long as he or she can demonstrate to the trial judge that a jury could reasonably find that the proffered evidence is authentic. The Texas approach involves a lower hurdle than the Maryland approach, because it is for the jury—not the trial judge—to resolve issues of fact, especially where the opposing party wishes to challenge the authenticity of the social media evidence.

The Superior Court adopted the Texas approach and found that Parker's social media post was sufficiently authenticated by circumstantial evidence and by testimony explaining how the post was obtained. On appeal, Parker claims that social media evidence requires greater scrutiny than other evidence and should not be admitted unless the trial judge is convinced that the evidence has not been falsified. We disagree. We conclude that the Texas approach better conforms to the requirements of Rule 104 and Rule 901 of the Delaware Rules of Evidence, under which the jury ultimately must decide the authenticity of social media evidence. A trial judge may admit a relevant social media post where the proponent provides evidence sufficient to support a finding by a reasonable juror that the proffered evidence is what the proponent claims it to be. We find no abuse of discretion by the trial court in admitting the social media evidence in accordance with the Delaware Rules of Evidence. Accordingly, we affirm.

Facts and Procedural History

On December 2, 2011, Tiffany Parker and Sheniya Brown were engaged in a physical altercation on Clifford Brown Walk in the City of Wilmington. The disagreement was over Facebook messages regarding a mutual love interest. Felicia Johnson was driving by when she observed the confrontation and later testified that Parker appeared to be "getting the best of the pregnant girl [Brown]." Bystanders eventually separated the two, but the fight resumed when Brown returned with a knife. Bystanders again intervened, and shortly thereafter officers from the Wilmington Police Department separated the women.

Parker was indicted on one count of Assault Second Degree and one count of Terroristic Threatening. Parker argued that her actions were justified because she was acting in self-defense. The State sought to introduce Facebook entries that were allegedly authored by Parker after the altercation to demonstrate her role in the incident and discredit Parker's self-defense argument. The Facebook entries originated from Parker's Facebook account and stated:

> ***684** bet tht [sic] bitch didnt [sic] think [I] was going to see her ass ... bet she wont [sic] inbox me no more, # caughtthatbitch
>
> ....
>
> ... [ctfu]. this girl is crazy. she really got these ppl [sic] thinkin [sic] that [I] was on some nut shit ... first of all she hit me first ... if you really want to put it out there since you shared i ... See more

> ... [I] told you go head [sic] and you inboxed [sic] me back still being disrespectful ... [I] told you say no more [sic] ... [I] seen [sic] you today ... we said our words you put your hands on me ... [I] hit you back. WE [sic] ... See more [1]

The State's exhibit depicting Parker's Facebook posts also included her picture, the name "Tiffanni Parker," and a time stamp for each entry, stating that they were posted on December 2, 2011. [2] Brown "shared," or reposted, this Facebook post on her own Facebook page.

The State used testimony from Brown, as well as circumstantial evidence, to authenticate the Facebook entries. Over Parker's objection, the trial court admitted the Facebook post into evidence, finding that the State had sufficiently authenticated it. The court noted that there was ample Delaware case law that relied upon distinguishing characteristics to appropriately authenticate emails and handwritten letters. [3] As a result, Brown's testimony explaining how she viewed and shared Parker's post and the post itself, which contained distinctive circumstances or characteristics, satisfied Rule 901's authentication requirements. The trial court concluded that "[a]ny further inquiry was for the jury to decide." [4]

The jury acquitted Parker of the Terroristic Threatening charge and convicted her of Assault Second Degree. This appeal followed.

Discussion

[1] **[2]** We review a trial judge's evidentiary rulings for abuse of discretion. [5] "An abuse of discretion occurs when a court has ... exceeded the bounds of reason in view of the circumstances, [or] ... so ignored recognized rules of law or practice ... to produce injustice." [6]

Under the Delaware Rules of Evidence, "[a]ll relevant evidence is admissible, except as otherwise provided," and "[e]vidence which is not relevant is not admissible." [7] All preliminary questions related to the admissibility of evidence are determined under Rule 104 by the trial judge. [8] ***685** But where "the relevancy of evidence depends upon the fulfillment of a condition of fact, the court shall admit it upon, or in the court's discretion subject to, the introduction of evidence sufficient to support a finding of the fulfillment of the condition." [9] Nonetheless, where evidence is admitted, a party may introduce additional relevant evidence to support or discount its weight or credibility. [10]

By their nature, social media posts and other similar electronic communications are creatures of, and exist on, the Internet. Rule 901(a) provides that "[t]he 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." [11] Rule 901(b) provides examples of authentication that comply with the rule. In relevant part, authentication of social media evidence can include: (1) testimony from a witness who states that the evidence is what it is claimed to be, [12] (2) distinctive characteristics of the evidence itself, such as "[a]ppearance, contents, substance, internal patterns or other distinctive characteristics, taken in conjunction with circumstances," that can authenticate the documentary evidence, [13] or (3) evidence that shows that the documentary evidence is accurately produced through a process or system. [14] These are not the exclusive ways to authenticate social media posts. [15]

Social Media Evidence Defined

Social media has been defined as "forms of electronic communications ... through which users create online communities to share information, ideas, personal messages, and other content (as videos)." [16] Through these sites, users can create a personal profile, which usually includes the user's name, location, and often a picture of the user. [17] On many sites such as Facebook or Twitter, a user will post content—which can include text, pictures, or videos—to that user's profile page delivering it to the author's subscribers. [18] Often these posts will include relevant evidence for a trial, including party admissions, inculpatory or exculpatory photos, or online communication between users. But there is a genuine concern that such evidence could be faked or forged, leading some courts to impose a high bar for

the admissibility ***686** of such social media evidence. [19] Other courts have applied a more traditional standard, "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." [20] This approach recognizes that the risk of forgery exists with any evidence and the rules provide for the jury to ultimately resolve issues of fact.

The Maryland Approach

The higher standard for social media authentication is best exemplified by the Maryland Court of Appeals' decision in *Griffin v. State.* There, the state sought to introduce a post from the MySpace profile of Jessica Barber, the defendant's girlfriend, stating, "snitches get stitches." [21] In order to prove that the post was written by Barber, the state sought to authenticate the evidence using the picture of Barber, coupled with her birth date and location, displayed on her MySpace profile. [22] The state did not ask Barber to authenticate the page on the stand or introduce electronic records definitively showing that Barber had authored the post.

The Maryland Court of Appeals held that the state failed to properly authenticate Barber's post and thus did not adequately link both the profile and the "snitches get stitches" posting to Barber. [23] As the Court explained, the trial court "failed to acknowledge the possibility or likelihood that another user could have created the profile in issue or authored the 'snitches get stitches' posting." [24] Thus, to properly authenticate similar social media posts, the Court held that the admitting party should either (1) ask the purported creator if she created the profile and the post, (2) search the internet history and hard drive of the purported creator's computer "to determine whether that computer was used to originate the social networking profile and posting in question," or (3) obtain information directly from the social networking site to establish the appropriate creator and link the posting in question to the person who initiated it. [25] Several courts have followed the reasoning of *Griffin* out of the concern that social media evidence could be a fake, a digital alteration of an alleged creator's profile, or a posting by another using the alleged creator's profile. [26]

The Texas Approach

The alternative line of cases is best represented by a Court of Criminal Appeals of Texas case, *Tienda v. State.* [27] In *Tienda,* the state introduced into evidence the names and account information associated with three MySpace profiles that tended to indicate the defendant's knowledge of or ***687** responsibility for a murder. [28] Several of the posts complained about the author's electronic monitor, which the defendant wore prior to trial. [29] On appeal, the defendant argued that the state did not properly authenticate the MySpace profile or the individual posts to attribute them to the defendant. The Court explained that "the best or most appropriate method for authenticating electronic evidence will often depend upon the nature of the evidence and the circumstances of the particular case." [30] This could include "direct testimony from a witness with personal knowledge, ... comparison with other authenticated evidence, or ... circumstantial evidence." [31] And rather than imposing a requirement that the proponent prove that the social media evidence was not fraudulent, the Texas Court explained that the standard for determining admissibility is whether "a jury could reasonably find [the] proffered evidence authentic." [32]

Ultimately, the Texas Court found that the state had sufficiently authenticated the defendant's MySpace posts and pictures. The Court explained that the combination of facts—including photos, contextual references to the defendant's life, and the posts about his ankle monitor—was circumstantial evidence "sufficient to support a finding by a rational jury that the MySpace pages that the State offered into evidence were created by the [defendant]." [33] Further, the Court explained that it was the province of the jury to assess and weigh the evidence presented by the state to determine whether it was the defendant, rather than some unidentified conspirators or fraudsters, who created and maintained the MySpace pages. [34] Courts in Arizona and New York have followed the rationale of *Tienda v. State.* [35] The premise of the Texas approach is that the jury—and not the trial judge—ultimately resolves any factual issue on the authentication of social media evidence.

The Jury Should Make the Ultimate Finding on Social Media Evidence

[3] We conclude that social media evidence should be subject to the same authentication requirements under the Delaware Rules of Evidence Rule 901(b) as any other evidence. "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." [36] Although we are mindful of the concern that social media evidence could be falsified, the existing Rules of Evidence provide an appropriate framework for determining admissibility. Where a proponent seeks to introduce social media evidence, he or she may use any form of verification available under Rule 901—including witness testimony, corroborative circumstances, distinctive characteristics, ***688** or descriptions and explanations of the technical process or system that generated the evidence in question—to authenticate a social media post. Thus, the trial judge as the gatekeeper of evidence may admit the social media post when there is evidence "sufficient to support a finding" by a reasonable juror that the proffered evidence is what its proponent claims it to be. [37] This is a preliminary question for the trial judge to decide under Rule 104. If the Judge answers that question in the affirmative, the jury will then decide whether to accept or reject the evidence. [38]

No Abuse of Discretion in Admitting Parker's Facebook Post

[4] Applying this rule to the proceeding below, the trial court did not abuse its discretion when it admitted Parker's Facebook posts. The trial court specifically rejected the Maryland approach and adopted the Texas rule. [39] At trial, the court explained that Delaware follows the "distinguishing characteristics" rationale, noting that Delaware courts have authenticated handwritten letters from inside prison based on the nicknames of the parties involved and references to the crimes. [40] The trial court further noted that the Court of Chancery has authenticated an email through distinctive characteristics using only the sender's email address. [41] As a result, the trial court concluded that the State had adequately authenticated Parker's social media post using witness testimony and circumstantial evidence. [42]

Having applied the same rule of law that we validate today, we agree with the trial court that the post was sufficiently authenticated in accordance with Rules 104 and 901. First, the substance of the Facebook post referenced the altercation that occurred between Parker and Brown. Although the post does not mention Brown by name, it was created on the same day after the altercation and referenced a fight with another woman. Second, Brown's testimony provided further authenticating evidence. Brown testified that she viewed Parker's post through a mutual friend. Thereafter, Brown "shared" the post and published it on her own Facebook page. Collectively, this evidence was sufficient for the trial court to find that a reasonable juror could determine that the proffered evidence was authentic. [43] The trial court did not abuse its discretion in admitting Parker's Facebook post.

Conclusion

The judgment of the Superior Court is **AFFIRMED.**

All Citations

85 A.3d 682

Footnotes

1 State's Exhibit 5, *State v. Parker,* No. 01112001354 (Del.Super.Ct.2012).
2 *Id.*
3 *State v. Parker,* No. 1112001354, mem. op. at 4 (Del.Super.Ct. Oct. 9, 2012).
4 *Id.* at 5.
5 *Manna v. State,* 945 A.2d 1149, 1153 (Del.2008) (citing *Pope v. State,* 632 A.2d 73, 78–79 (Del.1993)).
6 *Culp v. State,* 766 A.2d 486, 489 (Del.2001) (alteration in original) (omissions in original) (internal quotation marks omitted) (quoting *Lilly v. State,* 649 A.2d 1055, 1059 (Del.1994)).

7 D.R.E. 402.

8 Rule 104(a) provides:

> Preliminary questions concerning the qualification of a person to be a witness, the existence of a privilege, or the admissibility of evidence shall be determined by the court, subject to the provisions of paragraph (b) of this rule. In making its determination it is not bound by the rules of evidence except those with respect to privileges.

D.R.E. 104(a).

9 D.R.E. 104(b).

10 Rule 104(e) provides: "This rule does not limit the right of a party to introduce before the jury evidence relevant to weight or credibility." D.R.E. 104(e).

11 D.R.E. 901(a).

12 D.R.E. 901(b)(1).

13 D.R.E. 901(b)(4).

14 D.R.E. 901(b)(9).

15 *See* D.R.E. 901(b) (providing that the "examples of authentication or identification" listed in Rule 901(b) are "[b]y way of illustration only, and not by way of limitation").

16 Honorable Paul W. Grimm et al., *Authentication of Social Media Evidence,* 36 Am. J. Trial Advoc. 433, 434 (2013) (quoting *Definition of Social Media,* Merriam–Webster, http://www.merriam-webster. com/dictionary/social% 20media (last visited Feb. 5, 2014)).

17 *See* danah m. boyd & Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship,* 13 J. Computer–Mediated Comm. 210, 213 (2007). Relatedly, many users also create fake user profiles. *See* Katharina Krombholz et al., *Fake Identities in Social Media: A Case Study on the Sustainability of the Facebook Business Model,* 4 J. Service Sci. Res. 175, 177 (2012) (noting that five to six percent of registered Facebook accounts are fake accounts).

18 *See* Grimm et al., *supra,* at 435.

19 *E.g., Griffin v. State,* 419 Md. 343, 19 A.3d 415, 423 (2011); *see also* Grimm et al., *supra,* at 441–54 (collecting cases).

20 Grimm et al., *supra,* at 441.

21 *Griffin,* 19 A.3d at 418, 423.

22 *Id.* at 418–19, 424.

23 *Id.* at 423.

24 *Id.* at 423 (quoting *Griffin v. State,* 192 Md.App. 518, 995 A.2d 791, 806 (2010), *rev'd,* 419 Md. 343, 19 A.3d 415 (2011)).

25 *Id.* 427–28.

26 *E.g., St. Clair v. Johnny's Oyster & Shrimp, Inc.,* 76 F.Supp.2d 773, 774 (S.D.Tex.1999); *People v. Beckley,* 185 Cal.App.4th 509, 110 Cal.Rptr.3d 362, 367 (2010); *State v. Eleck,* 130 Conn.App. 632, 23 A.3d 818, 825 (2011); *Commonwealth v. Williams,* 456 Mass. 857, 926 N.E.2d 1162, 1172–73 (2010).

27 358 S.W.3d 633 (Tex.Crim.App.2012).

28 *Tienda,* 358 S.W.3d at 635.

29 *Id.* at 636.

30 *Id.* at 639.

31 *Id.* at 638.

32 *Id.*

33 *Id.* at 645.

34 *Id.* at 646.

35 *E.g., State v. Assi,* 2012 WL 3580488, at *3 (Ariz.Ct.App. Aug. 21, 2012); *People v. Valdez,* 201 Cal.App.4th 1429, 135 Cal.Rptr.3d 628, 633 (2011); *People v. Clevenstine,* 68 A.D.3d 1448, 891 N.Y.S.2d 511, 514 (2009). Notably, this approach has been praised by Judge Paul Grimm, District Court Judge for the District of Maryland, and his colleagues in their recent article, *Authentication of Social Media Evidence. See generally* Grimm et al., *supra.*

36 D.R.E. 901(a).

37 Grimm et al., *supra,* at 457 (citing *Lorraine v. Markel Am. Ins. Co.,* 241 F.R.D. 534, 542 (D.Md.2007)).

38 D.R.E. 901(a); *see also* Grimm et al., *supra,* at 455–56.

39 *Parker,* mem. op. at 4–5.

40 *Id.* (citing *Smith v. State,* 902 A.2d 1119, 1125 (Del.2006)).

41 *Id.* mem. op. at 5 (citing *Paron Capital Mgmt., LLC v. Crombie,* 2012 WL 214777, at *2 (Del.Ch. Jan. 24, 2012)).

42 D.R.E. 901(b)(4).

43 Although not explicitly considered by the trial court, we note that the proffered evidence was a print out of the Facebook page that displayed a photo of Parker and listed “Tiffanni Parker” as the content's creator. While a photo and a profile name alone may not always be sufficient evidence to satisfy the requirements of Rule 901, they are certainly factors that the trial court may consider.

End of Document

448 N.J.Super. 78
Superior Court of New Jersey,
Appellate Division.

STATE of New Jersey, Plaintiff–Respondent,
v.
Terri HANNAH, Defendant–Appellant.

Argued October 6, 2016
|
Decided December 20, 2016

Synopsis

Synopsis

Background: Following her conviction in municipal court, defendant was convicted after a trial de novo in the Superior Court, Law Division, Cumberland County, of simple assault. Defendant appealed.

Holdings: The Superior Court, Appellate Division, Leon, J.A.D., held that:

[1] traditional evidence authentication rules applied to post on social media website;

[2] post was sufficiently authenticated;

[3] municipal court did not violate sequestration order by allowing witnesses to remain in courtroom after testifying; and

[4] alleged improper adverse inference made by municipal court was irrelevant on appeal.

Affirmed.

West Headnotes (16)

[1] Criminal Law
Necessity and scope of proof
Criminal Law
Reception and Admissibility of Evidence

Considerable latitude is afforded a trial court in determining whether to admit evidence, and that determination will be reversed only if it constitutes an abuse of discretion; under that standard, an appellate court should not substitute its own judgment for that of the trial court, unless the trial court's ruling was so wide of the mark that a manifest denial of justice resulted.

Cases that cite this headnote

[2] Criminal Law
Telecommunications

Traditional rules for authentication of evidence applied to post on social media website that was allegedly written by defendant and was admitted as evidence in her prosecution for assault; fact that post was created on the Internet and could have been forged did not set it apart from other writings so as to warrant new authentication standards. N.J. R. Evid. 901.

Cases that cite this headnote

[3] Criminal Law
Sufficiency of evidence;standard of proof in general

Authentication of evidence does not require absolute certainty or conclusive proof; only a prima facie showing of authenticity is required. N.J. R. Evid. 901.

1 Cases that cite this headnote

[4] Criminal Law
Authentication and Foundation

The requirement that evidence be authenticated was not designed to be an onerous burden. N.J. R. Evid. 901.

1 Cases that cite this headnote

[5] Criminal Law
Questions of law or fact

Criminal Law
Authentication and Foundation

In a bench trial, considering the judge's dual role with regard to the admission and weight of evidence challenged as inauthentic, the better practice in such a circumstance will often warrant the admission of the document and then a consideration by the judge, as factfinder. N.J. R. Evid. 901.

Cases that cite this headnote

[6] **Criminal Law**
Telecommunications

Post on social media website allegedly written by defendant was sufficiently authenticated to be admissible in assault prosecution, despite defendant's assertion that she had not written the post; post contained details about altercation that led to defendant's prosecution, victim testified that the post was made in response to her communications with defendant, and post bore defendant's photo and her "handle" on the website. N.J. R. Evid. 901.

Cases that cite this headnote

[7] **Criminal Law**
Circumstantial evidence in general

A prima facie showing of the authenticity of evidence may be made circumstantially. N.J. R. Evid. 901.

1 Cases that cite this headnote

[8] **Criminal Law**
Circumstantial evidence in general

Under the reply doctrine, a writing may be authenticated by circumstantial evidence establishing that it was sent in reply to a previous communication. N.J. R. Evid. 901.

Cases that cite this headnote

[9] **Criminal Law**
Trial de novo

In conducting trial de novo following defendant's conviction for simple assault in municipal court, Law Division did not commit plain error by relying on evidence of social media website's policies that was not before the municipal court, since there was ample other evidence supporting the trial court's decision not to credit defendant's denial that she wrote a post referencing victim.

Cases that cite this headnote

[10] **Criminal Law**
Power and duty of court

The purpose of the rule allowing for sequestration of witnesses is to prevent prospective witnesses from hearing what the other witnesses detail in their evidence. N.J. R. Evid. 615.

Cases that cite this headnote

[11] **Criminal Law**
What constitutes violation of rule

Municipal court did not violate sequestration order by allowing two witnesses to remain in courtroom after they testified in assault prosecution; neither witness was not able to hear the other's testimony before he or she testified, neither witness was recalled to the stand, and there was no evidence that second witness was coached by first witness. N.J. R. Evid. 615.

Cases that cite this headnote

[12] **Criminal Law**
Mootness

On defendant's appeal of her assault conviction following a trial de novo, which was conducted after her conviction in municipal court, defendant's argument that municipal court drew improper adverse inference against her was irrelevant; given that the Law Division declined to draw such an inference, defendant's argument solely challenged the actions of the municipal court,

which was outside the scope of appellate review.

Cases that cite this headnote

[13] Criminal Law
Trial de novo

A trial de novo in the Law Division provides a reviewing court with the opportunity to consider the matter anew.

Cases that cite this headnote

[14] Criminal Law
Trial de novo

A trial de novo by definition requires the trier to make his own findings of fact.

Cases that cite this headnote

[15] Criminal Law
Trial de novo

On a trial de novo following a conviction in municipal court, the Superior Court judge reviews the transcript and makes an independent determination of the sufficiency of the evidence presented.

Cases that cite this headnote

[16] Criminal Law
Matters or Evidence Considered

Appellate review of a municipal appeal to the Law Division is limited to the action of the Law Division and not that of the municipal court.

1 Cases that cite this headnote

****101** On appeal from Superior Court of New Jersey, Law Division, Cumberland County, Municipal Appeal No. 01–15.

Attorneys and Law Firms

John P. Morris argued the cause for appellant.

Kim L. Barfield, Assistant Prosecutor, argued the cause for respondent (*Jennifer Webb–McRae*, Cumberland County Prosecutor, attorney; *Elizabeth K. Tornese*, Assistant Prosecutor, of counsel and on the brief).

Before Judges Fisher, Leone, and Vernoia.

Opinion
The opinion of the court was delivered by

LEONE, J.A.D.

***81** Defendant Terri Hannah appeals her July 10, 2015 conviction for simple assault after a trial de novo in the Law Division, following her conviction in municipal court. She argues that a Twitter posting was improperly admitted into evidence, citing a Maryland case requiring that social media postings must be ***82** subjected to a greater level of authentication. We reject that contention, holding that New Jersey's current standards for authentication are adequate to evaluate the admission of social media postings. Under those standards, we find it was not an abuse of discretion to admit the tweet. Finding defendant's remaining claims lack merit, we affirm.

I.

The Law Division found the following facts based on the testimony in the Vineland Municipal Court. On September 22, 2012, Arnett Blake and his girlfriend, Cindy Edwards, attended a party at a community center. Defendant, Blake's ex-girlfriend, also attended the party.

****102** While in the bathroom, Edwards encountered defendant "making rude comments about her." While Edwards was still in the bathroom, defendant exited the bathroom, approached Blake, and said "I should F your girlfriend up." Later that night, defendant purposefully bumped into Blake.

As Edwards and Blake were in the lobby trying to leave the party, defendant quickly approached Blake with her closed fist in the air. Blake reacted by pushing defendant away, prompting security to grab him. When Edwards turned to say something, she saw defendant holding a high-heeled shoe, with which defendant struck Edwards in the face. Blake also saw defendant hit Edwards with a

shoe as he was being escorted outside. When defendant was brought outside, Edwards saw defendant did not have her shoes on.

Edwards and Blake went to the police station to report the incident and then went to the hospital, where Edwards received nine stitches. After the assault, defendant and Edwards had communications "back and forth" on Twitter. On December 28, 2012, Edwards saw defendant posted a tweet saying "shoe to ya face bitch."

***83** In municipal court, defendant offered a different version of events. Defendant testified she approached Blake and told him that she heard "hearsay ... saying that [she] was going to ... beat his girlfriend up." Defendant told Blake she "wanted to clear the air and let him know that [she was] not going to do anything to [his girlfriend]." Later during the party he "push[ed] [defendant] to the side." Defendant later saw Blake in the lobby and decided to ask him why he pushed her. She became aggressive and started yelling, and a security guard took her "straight out ... of the party." Defendant testified she never saw Edwards that night and never punched anyone or hit anyone with a shoe.

Defendant called as a witness a security guard at the party, who testified he saw defendant approaching a man "in an aggressive manner" and heard her make hostile remarks. "[B]efore she could do anything," the guard "snatched her up and ... took her out of the building." He told her she was not permitted to reenter the party. He did not see Blake or Edwards or see defendant hit anyone with a shoe.

Defendant was charged with aggravated assault, but the charge was downgraded to simple assault, a disorderly persons offense. *N.J.S.A.* 2C:12–1(a)(1). On January 12, 2015, the municipal court found defendant guilty and imposed a $307 fine plus costs and assessments. Defendant appealed. On June 5, 2015, the Law Division conducted a trial de novo, hearing oral argument. After reserving decision, the Law Division found defendant guilty of simple assault and imposed the same monetary penalties. The Law Division credited Edwards and Blake, found defendant not credible, and found the passage of two years compromised the security guard's recollection of the event.

On appeal to this court, defendant argues:

> POINT I—THE COURT'S ADMISSION OF THE TWEET (S–4), CLAIMED BY THE STATE TO HAVE BEEN POSTED BY THE DEFENDANT TO HER TWITTER ACCOUNT, WAS ERROR AS:
>
> (1) THE SUPERIOR COURT JUDGE MISTAKENLY ADOPTED WHAT HE BELIEVED TO BE THE DIFFERENT, MORE LENIENT TEXAS AUTHENTICATION STANDARD [RATHER THAN THE MARYLAND ***84** STANDARD] WITHOUT UTILIZING NEW JERSEY'S CIRCUMSTANTIAL EVIDENCE MODE OF ****103** AUTHENTICATION, *N.J.R.E.* 901, AND ASSESSING THE NON–PRODUCTION OF THE OTHER "DIFFERENT" SNAPSHOTS SUPPOSEDLY TAKEN BY THE ACCUSER IN AN ALLEGED EXCHANGE OF TWEETS BETWEEN ACCUSER AND DEFENDANT SOME THREE MONTHS AFTER THE ALLEGED ASSAULT;
>
> (2) THIS JUDGE IMPROPERLY AUTHENTICATED THE TWEET BY RELYING ON THE ACCUSER'S TESTIMONY AS WELL AS THAT OF THE DEFENDANT, WHO ONLY TESTIFIED AFTER THE STATE HAD RESTED;
>
> (3) WITH THIS JUDGE FINDING [SIC] THAT THE DEFENDANT'S JANUARY 12, 2015 MUNICIPAL COURT TESTIMONY WAS NOT CREDIBLE BECAUSE HE CONTRASTED HER TESTIMONY WITH EXHIBIT D–4 ATTACHED TO DEFENSE COUNSEL'S MAY 8, 2015 APPEAL BRIEF; AND,
>
> (4) THIS JUDGE ADMITTED THE TWEET, WITHOUT ANALYSIS AS TO THE TWEET'S RELEVANCE OR PROBATIVE VALUE.
>
> POINT II—THE SEQUESTRATION ORDER WAS IMPOSED AT THE START OF THE JANUARY 12, 2015 MUNICIPAL COURT TRIAL. THE SEQUESTRATION ORDER WAS NOT ENFORCED AS THE ALLEGED VICTIM WAS ALLOWED TO REMAIN IN THE COURTROOM BY THE JUDGE AFTER HER TESTIMONY; ALLOWING HER TO BE PRESENT WHILE HER BOYFRIEND TESTIFIED. THE BOYFRIEND'S EQUIVOCAL AND SEEMINGLY CONTRADICTORY OR "FORGETFUL" RESPONSES STRONGLY SUGGEST VISUAL CUES FROM THE ALLEGED

VICTIM. THE LAW DIVISION JUDGE'S WRITTEN OPINION IS DEVOID OF ANY CONSIDERATION OR DISCUSSION OF THAT ISSUE. THAT VIOLATION, BY ITSELF, SHOULD HAVE RESULTED IN REVERSAL AND REMAND TO THE MUNICIPAL COURT WITH STRICT ADHERENCE THEREAFTER TO THE SEQUESTRATION ORDER.

THIS DEFENDANT'S CONSTITUTIONAL RIGHTS TO DUE PROCESS AND A FAIR TRIAL WERE VIOLATED; NO SHOWING OF PREJUDICE IS REQUIRED IN THESE CIRCUMSTANCES. DEFENDANT'S CONSTITUTIONAL RIGHTS OVERRIDE ANY CONSTITUTIONAL RIGHTS OF A VICTIM OF CRIME. THIS TRIAL INVOLVED NOT A CRIME BUT A DISORDERLY PERSON'S OFFENSE. [CONSTITUTIONAL ASPECT NOT RAISED BELOW].

POINT III—THE RELIEF REQUESTED ON THE APPEAL SOUGHT REVERSAL AND REMAND FOR TRIAL IN THE MUNICIPAL COURT, *R.* 3:23–8(a)(2); RELIEF MANDATED FOR SUPPLEMENTATION OF THE MUNICIPAL COURT RECORD: (1) TO ALLOW DEFENDANT THE OPPORTUNITY TO RESPOND TO THE ADVERSE INFERENCE DETERMINATION MADE AGAINST HER BY THE MUNICIPAL COURT JUDGE, (2) TO ALLOW THE STATE TO ATTEMPT TO ESTABLISH AUTHENTICATION OF THE TWITTER POSTING, AND, (3) TO ALLOW THE MUNICIPAL COURT TO DEAL WITH THE, AS YET, UNRESOLVED ISSUE OF SEQUESTRATION VIOLATION ***85** SET FORTH IN POINT II ABOVE. *R.* 3:23–8 WAS AMENDED TO PERMIT ****104** SUCH SUPPLEMENTATION BY REMAND TO THE MUNICIPAL COURT, A REMEDIAL DEVICE NOT ACKNOWLEDGED BY THIS JUDGE.

II.

[1] Defendant argues a message sent on Twitter should not have been admitted as it was not properly authenticated. [1] "[C]onsiderable latitude is afforded a trial court in determining whether to admit evidence, and that determination will be reversed only if it constitutes an abuse of discretion." *State v. Kuropchak*, 221 *N.J.* 368, 385–86, 113 *A.*3d 1174 (2015) (citation omitted). "Under that standard, an appellate court should not substitute its own judgment for that of the trial court, unless 'the trial court's ruling "was so wide of the mark that a manifest denial of justice resulted." ' " *Ibid.* (citation omitted). We must hew to our standard of review.

The municipal court and the Law Division each admitted as Exhibit S–4 the following tweet allegedly posted by defendant on December 28, 2012: "No need for me to keep responding to ya stupid unhappy fake mole having ass.. how u cring [2] in a corner with a shoe to ya face bitch." The tweet displayed defendant's profile photo and defendant's Twitter handle, "@cirocgirl25." [3]

***86** Edwards testified she recognized the tweet as being written by defendant because it displayed defendant's picture. She also was familiar with defendant's Twitter handle, "@cirocgirl25." Moreover, Edwards testified the tweet was posted "in response to things that [Edwards] was saying" and they were communicating "back and forth." On December 28, 2012, Edwards went onto defendant's Twitter page, saw the posted tweet, and captured it as a screenshot. [4]

Defendant testified the Twitter page displayed a picture of her and her Twitter handle. However, she testified she did not author the tweet.

When the State sought to admit the tweet, defense counsel objected, arguing "[t]here's no way anybody besides Twitter can say that this came from [defendant]." In admitting the tweet, the municipal court ruled nothing "requires somebody to be here from Twitter. I think somebody can testify as to it as Ms. Edwards [did] and we go from there."

At the trial de novo, the Law Division classified the methods of authenticating a social media post into two camps: the Maryland ****105** approach and the Texas approach, respectively citing *Griffin v. State*, 419 *Md.* 343, 19 *A.*3d 415 (2011), and *Tienda v. State*, 358 *S.W.*3d 633 (Tex. Crim. App. 2012).

In *Griffin*, the Maryland Court of Appeals considered what the test should be for the authentication of printed

pages of a MySpace profile. *Griffin*, *supra*, 19 *A.*3d at 416–17. Citing "[t]he potential for abuse and manipulation of a social networking site by someone other than its purported creator and/or user," *Griffin* ruled that images from such a site require "greater scrutiny" than "letters and other paper records." *Id.* at 423–24 (concluding that ***87** "a printout of an image from such a site requires a greater degree of authentication"). The court suggested three possible methods of authentication. *Id.* at 427.

The first method was "to ask the purported creator if she indeed created the profile and also if she added the posting in question, i.e. '[t]estimony of a witness with knowledge that the offered evidence is what it is claimed to be.' " *Ibid.* (citation omitted). The second method was "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." *Ibid.* The third method was "to obtain information directly from the social networking website 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." *Id.* at 428.

In *Tienda*, the Texas Court of Criminal Appeals did not employ any of the three *Griffin* methods but concluded "there are far more circumstantial indicia of authenticity in this case than in *Griffin*—enough, we think, to support a prima facie case that would justify admitting the evidence and submitting the ultimate question of authenticity to the jury." *Tienda*, *supra*, 358 *S.W.*3d at 647. The Texas court found "the internal content of ... [the] MySpace postings —photographs, comments, and music—was sufficient circumstantial evidence to establish a prima facie case such that a reasonable juror could have found that they were created and maintained by" a particular individual. *Id.* at 642.

[2] Here, the Law Division found "[t]he Maryland approach is too strict in its authentication requirements," stating that its three methods "are unrealistic for a party to fulfill" and "create a higher bar than originally intended by the Rules." Accordingly, the Law Division "chose[ ] to adopt a rule of admissibility more similar to the Texas approach."

***88** Defendant argues that Texas follows the Maryland approach and that we should adopt the Maryland approach with its "three non-exclusive methods" of authentication. *Id.* at 647. We reject any suggestion that the three methods of authentication suggested in *Griffin* are the only methods of authenticating social media posts. We also reject *Griffin*'s suggestion that courts should apply greater scrutiny when authenticating information from social networks. *See Parker v. State*, 85 *A.*3d 682, 686–87 (Del. 2014) (rejecting the *Griffin* "greater scrutiny" approach and "conclud[ing] that social media evidence should be subject to the same authentication requirements under the Delaware Rules of Evidence Rule 901(b) as any other evidence"); *see also United States v. Vayner*, 769 *F.*3d 125, 131 n.5 (2d Cir. 2014) (noting that *Griffin* requires "greater scrutiny" and stating "we are skeptical that such scrutiny is required").

Rather, we agree with *Tienda*'s observation that

> ****106** [c]ourts and legal commentators have reached a virtual consensus that, although rapidly developing electronic communications technology often presents new and protean issues with respect to the admissibility of electronically generated, transmitted and/or stored information, including information found on social networking web sites, the rules of evidence already in place for determining authenticity are at least generally "adequate to the task."
>
> [*Tienda*, *supra*, 358 *S.W.*3d at 638–39 (citation omitted).]

Indeed, "jurisdictions across the country have recognized that electronic evidence may be authenticated in a number of different ways consistent with Federal Rule 901 and its various state analogs." *Id.* at 639.

"Despite the seeming novelty of social network-generated documents, courts have applied the existing concepts of authentication under Federal Rule 901 to them," including "the reply letter doctrine [and] content known only to the participants." 2 *McCormick on Evidence* § 227, at 108 (Broun ed., 2013).[5] *N.J.R.E.* 901 ***89** "generally follows Fed. R. Evid. 901" and incorporates both of those methods for authentication. Biunno, Weissbard & Zegas, *Current N.J. Rules of Evidence* [*Biunno*], 1991 Supreme Court Committee Comment & comment 3 on *N.J.R.E.* 901 (2016).

We need not create a new test for social media postings. Defendant argues a tweet can be easily forged, but so can

a letter or any other kind of writing. The simple fact that a tweet is created on the Internet does not set it apart from other writings. Accordingly, we apply our traditional rules of authentication under *N.J.R.E.* 901.

Though in "electronic" form, a tweet is a "writing." *See N.J.R.E.* 801(e). "The requirement of authentication of writings ... and the recognized modes of proving genuineness have been developed by case law over two centuries." *Biunno*, *supra*, comment 1 on *N.J.R.E.* 901 (2016). "Over the years authentication requirements have become more flexible, perhaps because the technology has become more commonplace." *Suanez v. Egeland*, 330 *N.J.Super.* 190, 195, 749 *A.*2d 372 (App. Div. 2000).

[3] **[4]** *N.J.R.E.* 901 provides: "The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter is what its proponent claims." Authentication " 'does not require absolute certainty or conclusive proof'—only 'a prima facie showing of authenticity' is required." *State v. Tormasi*, 443 *N.J.Super.* 146, 155, 128 *A.*3d 182 (App. Div. 2015) (quoting *State v. Mays*, 321 *N.J.Super.* 619, 628, 729 *A.*2d 1074 (App. Div.), *certif. denied*, 162 *N.J.* 132, 741 *A.*2d 99 (1999)). "This burden was not designed to be onerous." *State v. Hockett*, 443 *N.J.Super.* 605, 613, 129 *A.*3d 1116 (App. Div. 2016).

[5] " 'Courts are inclined to assess their role in authentication as that of a screening process[,]' and 'will admit as genuine writings which have been proved prima facie genuine ... leaving to the jury more intense review of the documents.' " *Konop v. Rosen*, 425 *N.J.Super.* 391, 411, 41 *A.*3d 773 (App. Div. 2012) ***90** (quoting *Biunno*, *supra*, comment 1 on *N.J.R.E.* 901 (2011)). In a bench trial, as here, "considering the judge's dual role with regard to its admission and weight, the better practice in such a circumstance will often ****107** warrant the admission of the document and then a consideration by the judge, as factfinder." *Tormasi*, *supra*, 443 *N.J.Super.* at 156–57, 128 *A.*3d 182.

[6] **[7]** Authenticity can be established by direct proof—such as testimony by the author admitting authenticity—but direct proof is not required. *Biunno*, *supra*, comment 2 on *N.J.R.E.* 901 (2016); *N.J.R.E.* 903. "A prima facie showing may be made circumstantially." *Konop*, *supra*, 425 *N.J.Super.* at 411, 41 *A.*3d 773. "Such circumstantial proof may include demonstrating that the statement 'divulged intimate knowledge of information which one would expect only the person alleged to have been the writer or participant to have.' " *Ibid.* (quoting *Biunno*, *supra*, comment 3(b) on *N.J.R.E.* 901 (2011)). Here, the tweet contained several such details, including "shoe to ya face," information that one would expect only a participant in the incident to have. [6]

[8] Additionally, under the reply doctrine, a writing "may be authenticated by circumstantial evidence establishing that it was sent in reply to a previous communication." *Mays*, *supra*, 321 *N.J.Super.* at 629, 729 *A.*2d 1074; *see Biunno*, *supra*, comment 3(c) on *N.J.R.E.* 901 (2016). Here, Edwards testified that the tweet was posted in response to her communications with defendant, as part of a "back and forth" between them. Moreover, the tweet said there was "[n]o need for me to keep responding to ya," apparently referring to Edwards who received a "shoe to ya face."

Defendant's Twitter handle, her profile photo, the content of the tweet, its nature as a reply, and the testimony presented at trial ***91** was sufficient to meet the low burden imposed by our authentication rules. Those facts established a prima facie case "sufficient to support a finding that the matter is what its proponent claims." *N.J.R.E.* 901. Other courts have admitted tweets applying their similar authentication standard. *See Wilson v. State*, 30 *N.E.*3d 1264, 1267–69 (Ind. Ct. App. 2015); *Sublet v. State*, 442 *Md.* 632, 113 *A.*3d 695, 720–21 (2015); *see also* 5 *Weinstein's Federal Evidence: Discovering and Admitting Computer–Based Evidence* § 900.07[4A] (Joseph M. McLaughlin ed., 2016).

[9] Defendant argues the Law Division cited not only the State's evidence but also defendant's testimony in the municipal court that the tweet bore her picture associated with her Twitter account. However, she cites no authority precluding the Law Division from considering the uncontested fact that the tweet bore defendant's photo and Twitter handle, which was established through the testimony of Edwards as well as defendant.

In the municipal court, defendant testified "[a]nybody can make a fake Twitter page and put your name on it and put something on there." She testified that because she deleted her Twitter account months before, someone could have taken the same Twitter handle and used it. After the

municipal court did not credit this claim, defendant tried to bolster her testimony by submitting new evidence to the Law Division, including printouts of Twitter policies showing that Twitter "is currently unable to accommodate individual requests for inactive or suspended usernames." The Law Division cited that policy as one of several reasons for finding that ****108** defendant's testimony was not credible and that she "did not actually delete her Twitter account and that she did, in fact, author and publish the Tweet in question."

Defendant now argues it was improper for the Law Division to rely on evidence that was not before the municipal court. Notably, defendant herself presented the Twitter policies to the Law Division and did not object to the court's consideration of them. Therefore, she must show at least plain error. However, she fails to show the court's consideration of the policies was "clearly ***92** capable of producing an unjust result." *R.* 2:10–2. There was ample other evidence supporting the court's decision not to credit defendant's denial that she wrote and posted the tweet.

The Law Division, like the municipal court, provided sufficient reasons for finding the tweet authentic, relevant, and admissible. Defendant's remaining arguments regarding authentication lack sufficient merit to warrant discussion. *R.* 2:11–3(e)(2). Accordingly, we find no abuse of discretion in admitting the tweet.

III.

The municipal court granted defendant's request for a sequestration order at the start of trial. On appeal, defendant argues for the first time that the order was violated when the State's witnesses were allowed to remain in the courtroom after testifying.

[10] *N.J.R.E.* 615 provides that, "[a]t the request of a party or on the court's own motion, the court may, in accordance with law, enter an order sequestering witnesses." "Its purpose is 'to prevent *prospective witnesses* from hearing what the other witnesses detail in their evidence[.]' " *State v. Williams*, 404 *N.J.Super.* 147, 160, 960 *A.*2d 805 (App. Div. 2008) (emphasis added) (quoting *State v. DiModica*, 40 *N.J.* 404, 413, 192 *A.*2d 825 (1963)), *certif. denied*, 201 *N.J.* 440, 991 *A.*2d 229 (2010); *see also Loigman v. Twp. Comm.*, 185 *N.J.* 566, 586, 889 *A.*2d 426 (2006) ("Sequestration of witnesses serves the salutary purpose of ensuring that a witness who is testifying not influence a witness who is about to testify.").

[11] Here, allowing the witnesses to remain in the courtroom after they testified "was no violation of a sequestration order or insult to the purpose of sequestration." *Williams*, *supra*, 404 *N.J.Super.* at 160, 960 *A.*2d 805. Edwards was the first witness to be examined by the State. After her testimony concluded, the municipal court told Edwards she "could step down." Edwards apparently remained in the courtroom without objection. Blake then entered the courtroom, testified, and was allowed to remain ***93** without objection. Neither Edwards nor Blake was recalled to the stand.

Defendant argues Blake was coached by Edwards. However, the record contains no evidence of Edwards coaching Blake. Accordingly, defendant cannot show plain error. *See id.* at 160–65, 960 *A.*2d 805; *see also id.* at 172–73, 960 *A.*2d 805 (Fisher, J.A.D., concurring); *R.* 2:10–2.

IV.

[12] Lastly, defendant argues the municipal court drew an adverse inference against her because she did not call the women who were with her at the party to testify. The municipal court stated: "I think the Court can draw some inferences from the fact that there's reference to Ms. Hannah's sister [and two other women] who [were] somewhere in the area .... And they're not here to testify about anything." However, the Law Division found ****109** that "the trial judge was not making an adverse inference."

We need not review whether the municipal court did or could draw such an inference because the Law Division itself declined to draw such an inference. The Law Division stated: "Even if this Court were to construe the trial judge's findings to include an adverse inference, there is sufficient evidence in the record to convict the defendant of simple assault without the alleged adverse inference."

[13] **[14]** **[15]** The Law Division "conduct[ed] a trial de novo on the record below." *R.* 3:23–8(a)(2). A trial de novo in the Law Division "provides a reviewing court with the opportunity to consider the matter anew." *State*

v. Kashi, 180 *N.J.* 45, 48, 848 *A*.2d 744 (2004) (citation omitted). "A trial de novo by definition requires the trier to make his own findings of fact." *State v. Kashi*, 360 *N.J.Super.* 538, 545, 823 *A*.2d 883 (App. Div. 2003) (quoting *State v. Ross*, *supra*, 189 *N.J.Super.* 67, 75, 458 *A*.2d 1299 (1983)), *aff'd*, 180 *N.J.* 45, 848 *A*.2d 744 (2004). "[T]he Superior Court judge reviews the transcript and makes an independent determination of the sufficiency ***94** of the evidence presented." *Ibid.* Here, "[n]othing precluded the Superior Court judge from making his own assessment of the sufficiency of the evidence contained within the record." *Ibid.* The Law Division did so without making the inference allegedly drawn by the municipal court.

[16] Thus, defendant's argument solely "challenge[s] the actions of the municipal court judge. However, appellate review of a municipal appeal to the Law Division is limited to 'the action of the Law Division and not that of the municipal court.' " *State v. Palma*, 219 *N.J.* 584, 591–92, 99 *A*.3d 806 (2014) (citations omitted). "For that reason, we do not consider defendant's arguments in respect of the municipal court judge's actions." *Ibid.*

Affirmed.

All Citations

448 N.J.Super. 78, 151 A.3d 99

Footnotes

1 "Twitter is self-described as 'an information network made up of 140–character messages called Tweets.' " *State ex rel. J.F.*, 446 *N.J.Super.* 39, 44 n.7, 140 *A*.3d 564 (App. Div. 2016) (citation omitted); *accord The Twitter Glossary*, Twitter, Inc., https://support.twitter.com/articles/166337# (last visited Dec. 13, 2016) (hereinafter *Glossary*). "These messages are posted to your profile, sent to your followers, and are searchable on Twitter search." *New User FAQs*, Twitter, Inc., https://support.twitter.com/articles/13920# (last visited Dec. 6, 2016).

2 Edwards interpreted "cring" as "crying." Defendant read "cring" as "cringe."

3 A Twitter " 'handle' is used to identify a particular user on Twitter and is formed by placing the @ symbol next to a username." *Roca Labs, Inc. v. Consumer Op. Corp.*, 140 *F.Supp.*3d 1311, 1319 n.4 (M.D. Fla. 2015). A Twitter "username is how you're identified on Twitter, and is always preceded immediately by the @ symbol." *Glossary*. A Twitter "header photo" is "[y]our personal image that you upload, which appears at the top of your profile." *Ibid.* This "profile photo" "appears next to each of your Tweets." *Ibid.*

4 "A 'screenshot' is a snapshot image of the information displayed on a computer screen at a given point in time." *State v. Ravi*, 447 *N.J.Super.* 261, 270 n.8, 147 *A*.3d 455 (App. Div. 2016).

5 *McCormick* notes that *Griffin* "imposed a heavier burden of authentication," but "[a]s with the advent of the telegraph, the computer, and the internet," "the perceived need for this additional burden may dissipate." *McCormick on Evidence*, *supra*, § 227, at 109–10.

6 In *Konop*, we cited with approval *Kalola v. Eisenberg*, 344 *N.J.Super.* 198, 200, 781 *A*.2d 77 (Law Div. 2001), which found a threatening phone call to the plaintiff dentist authenticated because the caller "identified himself as the defendant, referenced the plaintiff and described the dental work previously performed." *Konop*, *supra*, 425 *N.J.Super.* at 411–13, 41 *A*.3d 773.

358 S.W.3d 633
Court of Criminal Appeals of Texas.

Ronnie TIENDA, Jr., Appellant,
v.
The STATE of Texas.

No. PD–0312–11.
|
Feb. 8, 2012.

Synopsis

Background: Defendant was convicted in the District Court, Dallas County, Robert Burns, J., of murder and he appealed. The Dallas Court of Appeals, affirmed. Defendant filed petition for discretionary review.

[Holding:] The Court of Criminal Appeals, Price, J., held that evidence was sufficient to establish a prima facie showing that social-networking webpage proffered by State was authored by defendant.

Affirmed.

West Headnotes (8)

[1] Criminal Law
Authentication and Foundation

Evidence has no relevance if it is not authentically what its proponent claims it to be.

41 Cases that cite this headnote

[2] Criminal Law
Admission of Evidence Dependent on Preliminary Proof

Whether the proponent of evidence has made a threshold showing that would be sufficient to support a finding that the matter in question is what its proponent claims is a preliminary question of admissibility to be decided by the court. Rules of Evid., Rules 104(a), 901.

32 Cases that cite this headnote

[3] Criminal Law
Preliminary or introductory questions of fact

The ultimate question of whether an item of evidence is what its proponent claims it to be is for the fact-finder.

17 Cases that cite this headnote

[4] Criminal Law
Admission of Evidence Dependent on Preliminary Proof

In performing its gate-keeping function, the trial court itself need not be persuaded that proffered evidence is authentic; the preliminary question for the trial court to decide is simply whether the proponent of the evidence has supplied facts that are sufficient to support a reasonable jury determination that the evidence he has proffered is authentic. Rules of Evid., Rules 104(a), 901.

58 Cases that cite this headnote

[5] Criminal Law
Evidence dependent on preliminary proofs

Appellate review is deferential on appeal from a trial court's ruling on the preliminary question of whether the proponent of evidence has supplied sufficient evidence of authenticity; the standard is abuse of discretion. Rules of Evid., Rules 104(a), 901.

41 Cases that cite this headnote

[6] Criminal Law
Evidence dependent on preliminary proofs

If the trial court's ruling that a jury could reasonably find proffered evidence authentic is at least "within the zone of reasonable

disagreement," a reviewing court should not interfere. Rules of Evid., Rules 104(a), 901.

33 Cases that cite this headnote

[7] **Criminal Law**
Sufficiency of evidence;standard of proof in general
Criminal Law
Circumstantial evidence in general

Evidence may be authenticated in a number of ways, including by direct testimony from a witness with personal knowledge, by comparison with other authenticated evidence, or by circumstantial evidence. Rules of Evid., Rule 901.

32 Cases that cite this headnote

[8] **Criminal Law**
Telecommunications

Content of postings on social-networking webpage was sufficient circumstantial evidence to establish a prima facie showing that webpage was authored by defendant, thus supporting admission of proffered evidence over authenticity objection in murder prosecution; page contained numerous photographs of defendant, page referenced victim's death and music played at his funeral, page contained references to defendant's gang, author complained about his electronic monitor, which was a condition of defendant's house arrest while awaiting trial, author's name corresponded to defendant's name and nickname, and author's e-mail address corresponded to defendant's name. Rules of Evid., Rules 104(a), 901.

6 Cases that cite this headnote

Attorneys and Law Firms

***634** Leslie McFarlane, Dallas, for Ronnie Tienda, Jr.

Martin L. Peterson, Asst. D.A., Dallas, Lisa C. McMinn, State's Attorney, Austin, for State.

OPINION

PRICE, J., delivered the opinion for a unanimous Court.

The appellant was convicted of murder.[1] He pled true to one enhancement count, and the jury assessed punishment at thirty-five years' imprisonment. In an unpublished opinion, the Fifth Court of Appeals affirmed the appellant's conviction, holding that the trial court did not abuse its discretion in admitting evidence from MySpace pages that the State believed were created by the appellant.[2] We will affirm the judgment of the court of appeals.

FACTS AND PROCEDURAL POSTURE

David Valadez and his two passengers were the targets of a multiple car shootout while driving southbound in Dallas on I–35E towards I–30. The shooting was apparently the product of some tension displayed between two rival groups at a nightclub earlier that evening, where members of the appellant's group were "throwing" gang signs and "talking noise" to Valadez and his friends. Shortly after Valadez and his passengers left one nightclub to head to another "after hours" club, Valadez's car unexpectedly came under gunfire from a caravan of three or four cars also traveling southbound on I–35E towards I–30. The appellant was a passenger in one of the cars in the caravan.

Testimony at trial as to the appellant's specific involvement in the shooting varied widely. The witnesses agreed that the appellant was at least present during the shooting; however, there was inconsistent testimony as to who fired the first gunshots, whether the appellant was seen merely holding a gun or actually firing a weapon, which car the appellant was riding in, and from which car the fatal shots were fired. During the exchange of fire, Valadez was shot twice, causing him to lose control and crash his vehicle into the highway's center concrete divider. Valadez died as a result of the gunshot wounds shortly after being taken to a nearby hospital. Although cartridge casings consistent with at least two weapons were found at the scene of the shooting, the bullet recovered from the deceased's body could not be matched to a particular weapon, as no firearms were ever recovered.

During preparation of the State's case against the appellant, the deceased's sister, Priscilla Palomo, provided the State with information regarding three MySpace profile pages that she believed the appellant was responsible for registering and maintaining.[3] After subpoenaing MySpace.com for the general "Subscriber Report" associated with each profile account, the State ***635** printed out images of each profile page directly from the MySpace.com website, and then marked the profile pages and related content as State's exhibits for trial. The State used Palomo as the sponsoring witness for these MySpace accounts at guilt/innocence, and, over the appellant's running objection as to the authenticity of the profile pages, the State was permitted to admit into evidence the names and account information associated with the profiles, photos posted on the profiles, comments and instant messages linked to the accounts, and two music links posted to the profile pages.

The State had Palomo explain how she came across the profiles and brought them to the attention of the prosecutor. The trial judge sustained the appellant's first authentication objection when the prosecutor began asking Palomo questions about the specific content of the MySpace profiles prior to introducing any exhibits into evidence. After a brief sidebar conference at the bench with defense counsel off the record, the prosecutor marked the relevant MySpace profile printouts as numbered State's exhibits and had Palomo identify the printouts as the profiles she had found on MySpace. The prosecutor also offered into evidence the subscriber reports and accompanying affidavits subpoenaed from MySpace.[4] The judge then admitted the printouts of the profiles, over the appellant's objection that the State still had not laid the proper predicate to prove that the profiles were in fact what the State purported them to be, namely, declarations that the appellant himself had posted on his personal MySpace pages.

According to the subscriber reports, two of the MySpace accounts were created by a "Ron Mr. T," and the third by "Smiley Face," which is the appellant's widely-known nickname. The account holder purported to live in "D TOWN," or "dallas," and registered the accounts with a "ronnietiendajr@" or "smileys_ shit @" email address. The State introduced multiple photos "tagged" to these accounts because the person who appeared in the pictures at least resembled the appellant. The person is shown displaying gang-affiliated tattoos and making gang-related gestures with his hands.

The main profile pages of the MySpace accounts contained quotes boasting "You aint BLASTIN You aint Lastin" and "I live to stay fresh!! I kill to stay rich!!" Under the heading "RIP David Valadez" was a link to a song that was played by Valadez's cousin at Valadez's funeral. Another music link posted to one of the profiles was a song titled "I Still Kill." The instant messages exchanged between the account holder and other unidentified MySpace users included specific references to other passengers present during the shooting, circumstances surrounding the shooting, and details about the State's investigation ***636** following the shooting. The author of the messages made specific threats to those who had been "snitchin" and "dont run shit but they mouth," assigning blame to others for being the "only reason im on lock down and have this shit on my back." The author also generally boasted to another user that "WUT GOES AROUND COMES AROUND" and "U KNO HOW WE DO, WE DON'T CHASE EM WE REPALCE EM." The author accused: "EVERYONE WUZ BUSTIN AND THEY ONLY TOLD ON ME." Several of the instant messages also complained about the author's electronic monitor, which was a condition of the appellant's house arrest while awaiting trial.[5]

The State elicited additional testimony concerning the MySpace pages through a Dallas Police Department gang unit officer, Detective Daniel Torres, during guilt/innocence and through Valadez's mother during punishment. The officer testified regarding the common use of social networking media, such as MySpace, by gangs to stay in touch with members and to "promote" their gangs by bragging about participation in gang-related activities. At punishment, Valadez's mother was permitted to testify about how "devastated" she and her family were when they found the appellant's music link on his profile page with the title "RIP David Valadez," which in her eyes was the appellant's way of bragging about killing her son through the song that was played at his memorial. The appellant repeatedly objected, during both stages of trial, on the basis of improper authentication, hearsay, and relevance.

Through cross examination of Palomo, defense counsel elicited testimony regarding the ease with which a person could create a MySpace page in someone else's name and

then send messages, purportedly written by the person reflected in the profile picture, without their approval. Defense counsel emphasized that any case-specific facts that were referenced in the MySpace messages associated with these accounts were not facts solely within the defendant's knowledge, but were known to the deceased's family, friends, and practically any other third party interested in the case. Although the gang officer, Torres, testified to having prior experience using MySpace to investigate gang-related activity, when asked on cross examination whether he had any particular knowledge regarding how a MySpace account is created, he stated: "None, whatsoever." The officer acknowledged that anyone could create a MySpace page, but he had never created one himself.

During the appellant's guilt/innocence closing argument, counsel again emphasized the ease with which a MySpace account could be created or accessed without someone's approval and highlighted the State's failure to prove that the accounts were created by the appellant through any technological or expert evidence, for example, by tracing the IP address listed in the subscriber report to the appellant's personal computer. In sum, defense counsel argued that the MySpace evidence was never authenticated and was not credible evidence that the jury should consider in supporting a guilty verdict. The State's closing arguments during both phases of trial included multiple MySpace references and specific quotes from the profile pages. The jury found the appellant guilty and assessed punishment at thirty-five years in prison.

***637** On appeal, the appellant argued that the trial court erred in overruling his objections to the MySpace evidence. The court of appeals found sufficient "individualization" in the comments and photos on the MySpace pages to satisfy the factors laid out in Texas Rule of Evidence 901(b)(4) and admit the evidence as a "conditional fact of authentication" to support a "finding that the person depicted supplied the information." [6] In so ruling, the court of appeals relied for authority solely upon the opinion of an intermediate appellate court in Maryland that has since been reversed, as the appellant emphasizes now in his brief on the merits before this Court, by that state's highest appellate court. [7] We granted the appellant's petition for discretionary review to determine whether the court of appeals erred in holding that the trial court did not abuse its discretion in finding that the MySpace profiles were properly authenticated. We now affirm.

THE ARGUMENTS AND THE LAW OF AUTHENTICATION

The Arguments of the Parties

In his only issue for discretionary review, the appellant contends that the trial court erred in admitting into evidence the electronic content obtained from MySpace during both the guilt/innocence and punishment phases of his trial. The appellant broadly argues that the State failed to properly authenticate any of the evidence printed from the social networking website; and more specifically, that the "contents of a website cannot authenticate the website" itself. [8] In other words, he complains that the State did not prove that he was responsible for creating and maintaining the content of the MySpace pages by merely presenting the photos and quotes from the website that tended to relate to him. Therefore, the appellant concludes, the trial court erred in overruling his running objections under Texas Rules of Evidence Rule 901, [9] and the court of appeals should not have affirmed its ruling.

The State contends, in opposition, that the contents of the social networking pages in this case contained sufficiently distinctive information to justify conditionally submitting them to the jury for its ultimate finding whether "the matter in question is what its proponent claims" [10] —here, that the MySpace pages were created and maintained by the appellant. The specificity of the content, which the State characterized as "admissions" by the appellant, was sufficient to tie him to this particular evidence and allow the jury to consider it for that purpose. [11] At a minimum, the State argues, the trial court's decision was "within the zone of reasonable disagreement" and therefore should not be disturbed on appeal. [12]

Standard of Review and Applicable Law

[1] **[2]** **[3]** **[4]** Under Texas Rules of Evidence Rule 104(a), whether or not to admit evidence ***638** at trial is a preliminary question to be decided by the court. [13] A bedrock condition of admissibility of evidence in any

legal contest is its relevance to an issue in the case—that is to say, its tendency to make a fact of consequence to determination of the action more or less probable. [14] Evidence has no relevance if it is not authentically what its proponent claims it to be. Rule 901(a) of the Rules of Evidence defines authentication as a "condition precedent" to admissibility of evidence that requires the proponent to make a threshold showing that would be "sufficient to support a finding that the matter in question is what its proponent claims." [15] Whether the proponent has crossed this threshold as required by Rule 901 is one of the preliminary questions of admissibility contemplated by Rule 104(a). [16] The trial court should admit proffered evidence "upon, or subject to the introduction of evidence sufficient to support a finding of" authenticity. [17] The ultimate question whether an item of evidence is what its proponent claims then becomes a question for the fact-finder—the jury, in a jury trial. [18] In performing its Rule 104 gate-keeping function, the trial court itself need not be persuaded that the proffered evidence is authentic. The preliminary question for the trial court to decide is simply whether the proponent of the evidence has supplied facts that are sufficient to support a reasonable jury determination that the evidence he has proffered is authentic. [19]

[5] **[6]** Appellate review of a trial court's ruling on such a preliminary question of admissibility is deferential; the standard is abuse of discretion. [20] If the trial court's ruling that a jury could reasonably find proffered evidence authentic is at least "within the zone of reasonable disagreement," a reviewing court should not interfere. [21]

[7] Evidence may be authenticated in a number of ways, including by direct testimony from a witness with personal knowledge, by comparison with other authenticated evidence, or by circumstantial evidence. [22] Courts and legal commentators have reached a virtual consensus that, although rapidly developing electronic communications technology often presents new and protean issues with respect to the admissibility of electronically generated, transmitted and/or stored information, including information found on social networking web sites, the rules of evidence already in place for determining authenticity are at least generally "adequate to the ***639** task." [23] Widely regarded as the watershed opinion with respect to the admissibility of various forms of electronically stored and/or transmitted information is *Lorraine v. Markel American Insurance Co.* [24] There the federal magistrate judge observed that "any serious consideration of the requirement to authenticate electronic evidence needs to acknowledge that, given the wide diversity of such evidence, there is no single approach to authentication that will work in all instances." [25] Rather, as with the authentication of any kind of proffered evidence, the best or most appropriate method for authenticating electronic evidence will often depend upon the nature of the evidence and the circumstances of the particular case. [26]

Like our own courts of appeals here in Texas, [27] jurisdictions across the country have recognized that electronic evidence may be authenticated in a number of different ways consistent with Federal Rule 901 and its various state analogs. Printouts of emails, internet chat room dialogues, and cellular phone text messages have all been admitted into evidence when found to be sufficiently linked to the purported author so as to justify submission to the jury for its ultimate determination of authenticity. [28] Such prima facie authentication ***640** has taken various forms. In some cases, the purported sender actually admitted to authorship, either in whole or in part, [29] or was seen composing it. [30] In others, the business records of an internet service provider or a cell phone company have shown that the message originated with the purported sender's personal computer or cell phone under circumstances in which it is reasonable to believe that only the purported sender would have had access to the computer or cell phone. [31] Sometimes the communication has contained information that only the purported sender could be expected to know. [32] ***641** Sometimes the purported sender has responded to an exchange of electronic communications in such a way as to indicate circumstantially that he was in fact the author of the particular communication, the authentication of which is in issue. [33] And sometimes other circumstances, peculiar to the facts of the particular case, have sufficed to establish at least a prima facie showing of authentication. [34]

However, mindful that the provenance of such electronic writings can sometimes be open to question—computers can be hacked, protected passwords can be compromised, and cell phones can be purloined—courts in other cases

have held that not even the prima facie demonstration required to submit the issue of authentication to the jury has been satisfied.[35] That an email on its face purports ***642** to come from a certain person's email address, that the respondent in an internet chat room dialogue purports to identify himself, or that a text message emanates from a cell phone number assigned to the purported author—none of these circumstances, without more, has typically been regarded as sufficient to support a finding of authenticity.[36]

ANALYSIS

[8] In this case, the internal content of the MySpace postings—photographs, comments, and music—was sufficient circumstantial evidence to establish a prima facie case such that a reasonable juror could have found that they were created and maintained by the appellant. That circumstantial evidence included:

- The first MySpace business record I.D. is # 120841341. The official MySpace Subscriber Report lists the User as "First Name: ron; Last Name: mr.t" with an email address of "smileys_shit@." [Witnesses testified that the appellant's nickname is "Smiley."] The city is listed as "D TOWN."

- The Subscriber Report for MySpace User # 300574151 lists the owner as "First Name: ron; Last name: Mr. T" with an email address of "ronnietiendajr @." As with the first MySpace listing, the city for this listing is "D*Town." The zip code is 75212.

- The Subscriber Report for MySpace User # 435499766 lists the owner as "First Name: SMILEY; Last Name: FACE" with an email address of ronnietiendajr@. The city for this listing is "dallas" and the zip code is 75212.

- The first MySpace page of User # 120841341 offered into evidence contains ***643** a photograph of the appellant[37] under the title "SMILEY FACE." The photograph shows the appellant pulling a shirt up over the bottom half of his face. The tattoos on his arms, however, are clearly visible. There is a date stamp on the photograph of "03/01/2007 17:09."[38]

- To the right side of the appellant's photograph on that MySpace page is the following:

  "You aint BLASTIN

  You aint Lastin"

  Male

  21 years old

  D Town, Texas

  United States

  Last Login: 9/4/2007[39]

- Below the appellant's photograph and the caption on that MySpace page is the legend "RIP David Valadez" and a music button which, according to Priscilla Paloma, played the song that was played at David Valadez's funeral.

  - On the MySpace page for User # 300574151, there is a photograph of the appellant, bare-chested, with his gang tattoos—including "Tango Blast" written across his chest.[40]

- The MySpace page is titled "MR. SMILEY FACE" even though the Subscriber Report list the User's name as "ron Mr. T" and his email address as "ronnietiendajr@."

  - Beside the appellant's photograph on that MySpace page is the following:

  "I LOVE DRAMA SO

  MUCH CUZ MY LIFE

  IS SO ROUGH!!!

  ANYTHING ELSE

  WOULDN'T SEEM

  NORMAL!!!

  Male

  22 years old

  D*Town, Texas

United States

Last Login: 5/19/2008 [41]

*644 • Below the appellant's photograph and the caption on that MySpace page is the music button for the "50 Cent I Still Kill by dj Bali" sound clip.

• Below that caption is the following:

MR. SMILEY FACE'S INTERESTS

General AINT PROUD OF MY PAST BUT IM LIVIN N DA PRESENT N ALWAYS PLANIN 4 DA FUTURE!!! NS XV111 ST [42]

• Also on the MySpace Profile page for User # 300574151 is a later photograph of a bare-chested appellant, again showing his tattoo "Tango Blast." [43]

• That photograph carries the heading: Mr. ONE OF A KIND.

• Beside the appellant's photograph on that MySpace page is the following:

"DIS IS WHO I AM!!!

DON'T LIKE IT FUCK

YOU!!!"

Male

22 years old

D*Town, Texas

United States

Last Login: 9/5/2008 [44]

• On the right hand side of the page is the following statement: Mr.ONE OF A KIND I LIVE TO STAY FRESH!! I KILL TO STAY RICH!! N OTHER WORDS IMA GO TO WAR BOUT MY SHIT!!

• The MySpace User # 300574151 message page contains numerous messages to other MySpace users. [45] Only the 53 messages sent between 2:00 p.m. and 9:44 p.m. on September 21, 2008, were introduced into evidence. The messages that indicate that it is the appellant himself who is the creator, owner, and user of this MySpace account include the following:

• At 2:09 p.m. the User sent a message to User # 73576314: "SHIT CAN U BELIEVE I ALREADY BEEN ON DIS MONITOR A YEAR NOW AND SHIT AINT NO TELLING WHEN A NIGGA GONE GET OFF DIS HOE" [46]

• At 2:17 p.m. the User sent a message to the same User: "SHIT IT AINT ME IT THE STATE SETTIN IT OFF AND SINCE I HAVE SNITCHES ON ME THEY TRYNA GET A NIGGA LOCKED UP"

*645 • Also at 2:17 p.m., the User sent a message to User # 103410565: "U KNO ME AND U MY NIGGA SO U WANT TO FUCK HIM UP U KNO HOW WE DO, WE DONT CHASE EM WE REPALCE EM"

• At 2:21 p.m. the User sent another message to User # 103410565: "IS IT DAT FRIENDLY ASS NIGGA IN ALL DEM PIX AND SHIT JUS PLAY IT COO WUT GOES AROUND COMES AROUND YA FEEL ME"

• At 2:22 p.m. the User sent a message to User # 73576314: "MAN JESSE BOY HECTOR SNITCHIN ON ME I AINT TRIPPIN ON BEEF BUT TELLIN A WHOLE NOTHER BALL GAME DAT I DONT PLAY"

• At 2:27 p.m. the User sent a message to User # 12231226: "SHIT ON STILL ON A MONITOR SO I AINT BEEN NO WHERE IN A BOUT A YEAR NOW AND MY B DAY WAS O THA12TH U FO GOT BOUT ME" [47]

• At 2:35 p.m. the User sent a message to User # 73576314: "YEA Y U THINK IM ON DIS MONITOR MY NIGGA SHIT HATIN ASS NIGGAS WNNA TALK ALL DAT GANGSTA SHIT AND WEN THE GOIN GET TUFF DEM NIGGAS DON'T RUN SHIT BUT THEY MOUTH"

• At 2:42 p.m. the User sent a message to the same User: "YEA SHIT EVERYONE WUZ BUSTIN AND THEY ONLY TOLD ON ME"

- At 2:50 p.m. the User sent another message to the same User: "YEA SHIT U KNO I KEEP GANGST EVEN AFTER HECTOR SHOT AT NEW AT RUMORS WE STILL DIDNT TELL AND I KNO JESSE TOLD HIM WE WAS THERE CUZ WE SAW THEM AT THA CLUB BUT ITS COO IF I GET OFF MAN@!!!!!" [48]

This combination of facts—(1) the numerous photographs of the appellant with his unique arm, body, and neck tattoos, as well as his distinctive eyeglasses and earring; (2) the reference to David Valadez's death and the music from his funeral; (3) the references to the appellant's "Tango Blast" gang; and (4) the messages referring to (a) a shooting at "Rumors" with "Nu–Nu," (b) Hector as a "snitch," [49] and (c) the user having been on a monitor for a year (coupled with the photograph of the appellant lounging in a chair displaying an ankle monitor) sent from the MySpace pages of "ron Mr. T" or "MR. SMILEY FACE" whose email address is "ronnietiendajr@"—is sufficient to support a finding by a rational jury that the MySpace pages that the State offered into evidence were created by the appellant. This is ample circumstantial evidence—taken as a whole with all of the individual, particular details considered in combination—to support a finding that the MySpace pages belonged to the appellant and that he created and maintained them.

It is, of course, within the realm of possibility that the appellant was the victim of some elaborate and ongoing conspiracy. ***646** Conceivably some unknown malefactors somehow stole the appellant's numerous self-portrait photographs, concocted boastful messages about David Valadez's murder and the circumstances of that shooting, was aware of the music played at Valadez's funeral, knew when the appellant was released on pretrial bond with electronic monitoring and referred to that year-long event along with stealing the photograph of the grinning appellant lounging in his chair while wearing his ankle monitor. But that is an alternate scenario whose likelihood and weight the jury was entitled to assess once the State had produced a prima facie showing that it was the appellant, not some unidentified conspirators or fraud artists, who created and maintained these MySpace pages.

The court of appeals in this case relied upon the opinion of an intermediate court of appeals in Maryland in a case presenting similar facts. [50] But that intermediate appellate court's opinion has since been reversed on discretionary review. [51] In *Griffin v. State,* [52] involving a prosecution for murder and assault, the State proffered a printout of portions of a MySpace profile purporting to be that of Griffin's girlfriend. [53] Although the girlfriend testified at trial, the State did not attempt to authenticate the MySpace profile as genuinely hers through her testimony. [54] Instead, the lead investigator in the case testified that the MySpace profile identified itself as being that of "Sistasouljah," having the same date of birth as the girlfriend. [55] Also posted on the profile was a photographic image of the defendant with his girlfriend. [56] The State argued that the date of birth and the photograph provided sufficient indicia of authentication to justify admission of other postings on the MySpace profile that amounted to veiled threats against the State's principal witness against the defendant. [57] The Maryland Court of Appeals disagreed. [58] "Anyone can create a MySpace profile at no cost," the Court observed, and "anyone can create a fictitious account and masquerade under another person's name or can gain access to another's account by obtaining the user's username and password[.]" [59] Relying for "assistance" in its analysis upon *Lorraine,* the Maryland Court of Appeals concluded:

> 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 defendant's girlfriend] was its creator and the author of [the threatening language posted thereon]. [60]

Accordingly, the Maryland Court of Appeals held that the trial court had abused its discretion to find that the State had laid ***647** an adequate prima facie foundation for admission of the MySpace profile postings. [61]

Along the way, the Maryland Court of Appeals recognized that such postings may readily be authenticated, explicitly identifying three non-exclusive methods. [62] First, the proponent could present the testimony of a witness with knowledge; or, in other words, "ask the purported creator if she indeed created the profile

and also if she added the posting in question." [63] That may not be possible where, as here, the State offers the evidence to be authenticated and the purported author is the defendant. Second, the proponent could offer the results of an examination of the internet history or hard drive of the person who is claimed to have created the profile in question to determine whether that person's personal computer was used to originate the evidence at issue. [64] Or, third, the proponent could produce information that would link the profile to the alleged person from the appropriate employee of the social networking website corporation. [65] The State of Maryland failed to take advantage of any of these methods in *Griffin.* And it is true that the State of Texas has likewise failed to utilize any of them in the appellant's case. [66] Nevertheless, as we have explained, there are far more circumstantial indicia of authenticity in this case than in *Griffin*—enough, we think, to support a prima facie case that would justify admitting the evidence and submitting the ultimate question of authenticity to the jury. We hold that the court of appeals did not err to conclude that it was within the trial court's discretion to admit the MySpace postings, notwithstanding that the persuasive authority it relied upon for that proposition has since been overruled.

CONCLUSION

Because there was sufficient circumstantial evidence to support a finding that the exhibits were what they purported to be—MySpace pages the contents of which the appellant was responsible for—we affirm the trial judge and the court of appeals which had both concluded the same.

All Citations

358 S.W.3d 633

Footnotes

1 TEX. PENAL CODE § 19.02.

2 *Tienda v. State,* No. 05–09–00553–CR, 2010 WL 5129722, at *4–5 (Tex.App.-Dallas Dec. 17, 2010) (not designated for publication).

3 Social networking websites such as MySpace and Facebook "typically allow users to customize their own personal web pages (often known as 'profiles'), post photographs or videos, add music, or write a journal or blog that is published to the online world." John S. Wilson, Comment, *MySpace, Your Space, or Our Space? New Frontiers in Electronic Evidence,* 86 OR. L.REV. 1201, 1220 (2007).

4 A total of three subscriber reports were admitted into evidence, one for each MySpace account. Each of the three subscriber reports reflects a different "User # " and a different "Sign up IP" number. "A computer connected to the Internet is assigned an IP address, which can uniquely identify that computer at least for the time that it is connected." Andrew M. Grossman, Case Note & Comment, *No, Don't IM Me–Instant Messaging, Authentication, and the Best Evidence Rule,* 13 GEO. MASON L.REV. 1309, 1315–16 (Spring/Summer 2006). Oftentimes, the technology "can be made to yield a user's IP address, and in most cases, that address can be tied to a means of accessing the Internet and thus a person, just as a telephone number can be connected to the person paying for it." *Id.* at 1335. There was no testimony elicited at the appellant's trial, however, and nothing on the face of the one-page subscriber reports themselves, to explicitly indicate whether any of the three User # s are the appellant's or whether any of the three Sign up IP numbers corresponds to a computer either belonging to the appellant or to which he had access.

5 All quotes are as they appear in State's Exhibit 94, which contains printouts of messages between one of the MySpace accounts that the State asserted belonged to the appellant and various other unidentified MySpace users.

6 *Tienda, supra,* at *4–5.

7 Appellant's Brief, at 5–6. The court of appeals cited the opinion of the Court of Special Appeals of Maryland, *Griffin v. State,* 192 Md.App. 518, 995 A.2d 791 (2010), while acknowledging that the Maryland Court of Appeals had since granted discretionary review. *Tienda, supra,* at *5. The Maryland Court of Appeals subsequently reversed the judgment of the Court of Special Appeals of Maryland, in *Griffin v. State,* 419 Md. 343, 19 A.3d 415 (2011).

8 Appellant's Brief, at 5.

9 TEX.R. EVID. 901.

10 *Id.* 901(a).

11 State's Brief, at 1.

12 *Id.*
13 TEX.R. EVID. 104(a).
14 TEX.R. EVID. 401 & 402.
15 TEX.R. EVID. 901(a).
16 *See* TEX.R. EVID. 104(a), 901(a); *Druery v. State,* 225 S.W.3d 491, 502 (Tex.Crim.App.2007).
17 TEX.R. EVID. 104(b).
18 *Druery, supra.*
19 *Id.*
20 *Id.*
21 *Montgomery v. State,* 810 S.W.2d 372, 391 (Tex.Crim.App.1991) (opinion on reh'g).
22 *See* TEX.R. EVID. 901(b)(1), (3)–(4) ("**(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 that a matter is what it is claimed to be. * * * (3) *Comparison by trier or expert witness.* Comparison by the trier of fact or by expert witness with specimens which have been found by the court to be genuine. (4) *Distinctive characteristics and the like.* Appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances.").
23 Steven Goode, *The Admissibility of Electronic Evidence,* 29 REV. LITIG. 1, 7 (Fall 2009); *see* Sandra Hornberger, Comment, *Social Networking Websites: Impact on Litigation and the Legal Profession in Ethics, Discovery, and Evidence,* 27 TOURO L.REV. 279, 304–05 (2011) (opining that "the existing evidentiary rules sufficiently address any legal issues surrounding the admission of information obtained from social networking websites"); Katherine Minotti, Comment, *Evidence: The Advent of Digital Diaries: Implications of Social Networking Web Sites for the Legal Profession,* 60 S.C. L.REV. 1057, 1074 ("the current federal rules are adequate" to guide courts "when facing evidentiary issues regarding social networking web sites"); Grossman, *supra,* at 1311 ("judges may express the appropriate skepticism due instant messaging evidence within the framework of the Rules [of Evidence]."); *In the Interest of F.P., a Minor,* 878 A.2d 91, 95 (Pa.Super.Ct.2005) (rejecting the need to "create a whole new body of law just to deal with [the admissibility of] e-mails or instant messages" and opining that "e-mail messages and similar forms of electronic communication can be properly authenticated within the existing framework" of the rules of evidence); *State v. Eleck,* 130 Conn.App. 632, 640, 23 A.3d 818, 823 (2011) ("We agree that the emergence of social media such as e-mail, text messaging and networking sites like Facebook may not require the creation of new rules of authentication with respect to authorship.").
24 241 F.R.D. 534 (D.Md.2007). *See also* Paul W. Grimm, Michael V. Ziccardi & Alexander W. Major, *Back to the Future: Lorraine v. Markel American Insurance Co. and New Findings on the Admissibility of Electronically Stored Information,* 42 AKRON L. REV. 357 (2009).
25 *Lorraine, supra,* at 553–54.
26 *See, e.g., Druery, supra,* at 502–03 (authentication of letters); *DeLuna v. State,* 711 S.W.2d 44, 46 (Tex.Crim.App.1986) (photographs); *Ex parte Watson,* 606 S.W.2d 902, 905 (Tex.Crim.App.1980) (handwriting comparison).
27 *See, e.g., Manuel v. State,* 357 S.W.3d 66, 75 (Tex.App.-Tyler 2011, no pet.) (text messages); *Shea v. State,* 167 S.W.3d 98, 104–05 (Tex.App.-Waco 2005, pet. ref'd) (emails); *Massimo v. State,* 144 S.W.3d 210, 215–17 (Tex.App.-Fort Worth 2004, no pet.) (emails).
28 *See Jackson v. State,* 2009 Ark. App. 466, 320 S.W.3d 13 (2009) (Yahoo instant message conversations); *Bobo v. State,* 102 Ark.App. 329, 285 S.W.3d 270 (2008) (emails); *Hammontree v. State,* 283 Ga.App. 736, 642 S.E.2d 412 (2007) (internet instant message conversation); *Simon v. State,* 279 Ga.App. 844, 632 S.E.2d 723 (2006) (emails); *Ford v. State,* 274 Ga.App. 695, 617 S.E.2d 262 (2005) (internet chat room); *State v. Glass,* 146 Idaho 77, 190 P.3d 896 (App.2008) (on-line conversation); *People v. Chromik,* 408 Ill.App.3d 1028, 349 Ill.Dec. 543, 946 N.E.2d 1039 (2011) (text message); *People v. Downin,* 357 Ill.App.3d 193, 293 Ill.Dec. 371, 828 N.E.2d 341 (2005) (email); *Commonwealth v. Purdy,* 459 Mass. 442, 945 N.E.2d 372 (2011) (emails); *Commonwealth v. Amaral,* 78 Mass.App.Ct. 671, 941 N.E.2d 1143 (2011) (emails); *Kearley v. State,* 843 So.2d 66 (Miss.App.2002) (emails); *People v. Clevenstine,* 68 A.D.3d 1448, 891 N.Y.S.2d 511 (2009) (MySpace instant messages); *State v. Thompson,* 777 N.W.2d 617 (N.D.2010) (text messages); *In the Interest of F.P., a Minor,* 878 A.2d 91 (Pa.Super.Ct.2005) (instant messages); *State v. Taylor,* 178 N.C.App. 395, 632 S.E.2d 218 (2006) (text messages); *Bloom v. Commonwealth,* 262 Va. 814, 554 S.E.2d 84 (2001) (instant messages); *United States v. Gagliardi,* 506 F.3d 140 (2nd Cir.2007) (emails and internet chat room); *United States v. Barlow,* 568 F.3d 215 (5th Cir.2009) (Yahoo instant message conversations); *United States v. Tank,* 200 F.3d 627 (9th Cir.2000) (internet chat

room); *United States v. Simpson,* 152 F.3d 1241 (10th Cir.1998) (internet chat room); *United States v. Siddiqui,* 235 F.3d 1318 (11th Cir.2000) (email).

29 *Jackson, supra,* Ark. App. at 469, S.W.3d at 16 (defendant admitted to police that he had engaged in instant message conversations and acknowledged transcripts as accurate); *Bobo, supra* (defendant admitted sending emails, only denying some of the content); *Simon, supra,* Ga.App. at 847, S.E.2d at 726 (defendant admitted to two witnesses, including police officer, that he participated in the email exchange); *Ford, supra,* Ga.App. at 697, n. 7, S.E.2d at 266, n. 7 (defendant gave statement to police admitting to engaging in the on-line chat); *Kearley, supra,* at 70 (defendant admitted to police that he sent emails); *Thompson, supra,* at 621–22 (defendant's husband testified that he received text messages from what he knew to be her phone number and that she signed them in a distinctive manner with which he was familiar, and the defendant admitted sending text messages from her phone to her husband's phone that day); *Bloom, supra,* Va. at 821, S.E.2d at 87 (defendant admitted to police officer that he had communicated with instant message recipient on evening in question).

30 *Massimo, supra,* at 213 (defendant was "witnessed" to have sent similarly threatening email to recipient in the past); *Clevenstine, supra,* A.D.3d at 1450–51, N.Y.S.2d at 514 ("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 the defendant's MySpace account while on their computer").

31 *Bobo, supra,* Ark.App. at 335, S.W.3d at 275 (forensic computer expert testified that some of the emails "matched a temporary unique IP internet address for" the defendant's computer); *Hammontree, supra,* Ga.App. at 739, S.E.2d at 415 (internet message conversation originated from defendant's son's account, but messages signed by the defendant, he had access to son's computer, and son denied being author); *Chromik, supra,* Ill.App. at 1047–48, 349 Ill.Dec. 543, N.E.2d at 1056–57 (phone records show text messages sent from defendant's phone number at particular date and time alleged, and defendant admitted sending some of them, acknowledging accuracy of transcripts); *Purdy, supra,* Mass. at 450–51, N.E.2d at 381 (emails originated from email account bearing defendant's name and that he admitted was his, were found on computer he acknowledged was his, and contained information about his business that was, if not unique, then at least "unusual").

32 *Downin, supra,* Ill.App.3d at 195, 293 Ill.Dec. 371, N.E.2d at 344–45 (victim knew defendant personally, had exchanged emails with him in the past at an email address she knew to be his, and the email in issue came from his address, was responsive to an email she had sent him, and "contained information that would be known exclusively to" him); *Taylor, supra,* N.C.App. at 414, S.E.2d at 230–31 (text messages identified purported sender by name and described car he would be driving on a particular occasion); *Simpson, supra,* at 1250 (defendant identified himself by name and email address in the course of internet chat room communications, and search of his home revealed specific written information found next to his computer that had been conveyed to him via those communications); *Siddiqui, supra,* at 1322–23 (emails purported to come from defendant's known email address, referred to the author by defendant's nickname, and contained allusions to events and circumstances that only defendant could reasonably be expected to know about).

33 *Shea, supra,* at 105 (defendant called recipient to confirm that she had received his email); *Glass, supra,* Idaho at 82, P.3d at 901 (in on-line conversation, defendant identifies himself by his middle name and then appears at a time and place agreed to, and in a car accurately described, in the conversation); *Amaral, supra,* Mass.App.Ct. at 674, N.E.2d at 1147 (defendant included photo and phone number in emails, which proved to be his, and one email "indicated that [he] would be at a certain place at a certain time, and [he] appeared at that place and time"); *Bloom, supra* (defendant revealed his true name and certain biographical information that was accurate, and appeared at the time and place where he had agreed to meet recipient); *Gagliardi, supra,* at 143 (defendant showed up at meeting place arranged during the course of exchange of electronic messages); *Barlow, supra,* at 218 (defendant arranged via Yahoo instant messages to meet at a state park, and appeared at the appointed place and time, admitting to police that he was there to meet the recipient); *Tank, supra,* at 630–31 (defendant admitted that screen name used in text messages was his, and witnesses testified that "when they arranged a meeting with the person who used [that screen name], it was Tank who showed up").

34 *Manuel, supra,* at 76–77 (text messages originated from phone number that the recipient recognized to be the defendant's, from which number she had also received various voice messages from which she recognized the defendant's voice); *In the Interest of F.P., a Minor, supra,* at 95 (instant messages purportedly sent by defendant referenced him by name as the sender, and threats made and events discussed therein mirrored animosity that defendant had displaying toward recipient contemporaneously with the period during which messages were sent).

35 *See People v. Beckley,* 185 Cal.App.4th 509, 518, 110 Cal.Rptr.3d 362, 368–69 (2010) (purported roster of gang members which appeared on a web page printed from the internet was not properly authenticated where sponsoring

police officer did not know who compiled it and did not explain the basis for his assertion that the gang itself did so); *Eleck, supra,* Conn.App. at 642–43, A.3d at 824 (printout of instant message exchange from defendant's Facebook page not properly authenticated just because the messages appeared to come from the purported sender's Facebook account; the messages fail to "reflect distinct information that only [the sender] would have possessed regarding the defendant or the character of their relationship"); *Hollie v. State,* 298 Ga.App. 1, 3, 679 S.E.2d 47, 50 (2009) (though email showed on its face that it originated from purported sender's email address, "this alone does not prove its genuineness"); *Commonwealth v. Williams,* 456 Mass. 857, 869, 926 N.E.2d 1162, 1172–73 (2010) (message not properly authenticated, even though it came from purported sender's MySpace page, because "there is no testimony (from [the recipient] 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.[,]" and also no testimony circumstantially to "identify the person who actually sent the communication"); *People v. Lenihan,* 30 Misc.3d 289, 293, 911 N.Y.S.2d 588, 591–92 (2010) ("defendant could not authenticate" photographs taken from a MySpace website because he "did not know who took [them] or posted them on MySpace"); *Commonwealth v. Koch,* 39 A.3d 996, ——, 2011 WL 4336634, at *6 (Pa.Super.Ct.2011) (cell phone text messages require more for authentication "than mere confirmation that the number or address belonged to" the purported sender and were inadmissible in the absence of "contextual clues in the ... messages themselves tending to reveal the identity of the sender"); *United States v. Jackson,* 208 F.3d 633, 638 (7th Cir.2000) (posting on white supremacist group's internet web site not authenticated because no showing that the group actually posted it as opposed to the defendant "herself, who was a skilled computer user"); *St. Clair v. Johnny's Oyster & Shrimp, Inc.,* 76 F.Supp.2d 773, 774–75 (S.D.Texas 1999) (random posting on internet web site cannot be authenticated because untrustworthy, given that "[a]nyone can put anything on the Internet").

36 *See* Goode, *supra,* at 10 ("the mere fact that an e-mail bears a particular e-mail address will often prove inadequate to authenticate the identity of the author; typically courts demand at least a little more evidence"); *Purdy, supra,* Mass. at 451, N.E.2d at 381 ("Evidence that the defendant's name is written as the author of an e-mail or that the electronic communication originates from an e-mail or social networking Web site such as Facebook or MySpace that bears the defendant's name is not sufficient alone to authenticate the electronic communication as having been authored or sent by the defendant."); *Koch, supra,* at ——, 2011 WL 4336634, at *6 ("In the majority of courts to have considered the question, the mere fact that an e-mail bears a particular e-mail address is inadequate to authenticate the identity of the author; typically, court demand additional evidence.").

37 Priscilla Palomo, the witness who sponsored the exhibits, identified the MySpace photographs as being of the appellant. Detective Daniel Torres also identified them as being of the appellant. The trial judge could also compare the photographs of the person on the MySpace pages (during trial they were downloaded from a CD and were in color and enlarged for clarity; that CD is in the appellate record) with the appellant sitting at the defense table. Suffice it to say that the person in the MySpace photographs has distinctive features and very distinctive tattoos on his body, neck, and arms. In many of the photographs, he is wearing the same distinctive glasses and a square earring. Although some of the xeroxed copies of the photographs in the reporter's record are fuzzy and unclear, the ones on the CD are not. One witness, who was at the club with the appellant on the night of the murder, testified that the appellant has the number "18" tattooed on the back of his head. One of the witnesses in the car with David Valadez, recognized the appellant as the shooter because he had the number "18" tattooed on his head. One of the MySpace photos shows the appellant with the number "18" tattooed on his head. Furthermore, one of the State's witnesses had already identified a photograph of the appellant and his friend "Nu–Nu" taken on the night of David Valadez's murder. The appellant's appearance in that photograph matches his appearance in the MySpace photographs.

38 David Valadez was murdered on June 25, 2007, about four months later.

39 The appellant was 21 on this date. David Valadez was murdered a little more than two months earlier.

40 This photograph is an apparent self-portrait taken with a smart phone in a mirror. Detective Torres testified that "Tango Blast" and "NS" referred to a local street gang and that a person with these tattoos would be a member of the gang.

41 The appellant was 22 years old as of this date.

42 XVIII is the Roman numeral for 18. Detective Torres testified that the term "NS XV111 ST" means the North Side 18th Street, which is a particular "North Side gang located in the Grand Prairie are of the metroplex." The number 18 on the MySpace Page matches the number 18 tattooed on the back of the appellant's head.

43 This is another apparent self-portrait of the appellant taken with a smart phone in a mirror, showing his "Tango Blast" chest tattoo, as well as the tattoos on his arms, posted on the MySpace page for User # 435499766, registered to "SMILEY FACE" with an email address of "ronnietiendajr@."

44 The appellant was 22 years old as of this date.

45 Torres, the Dallas gang officer, testified that gang members frequently communicate with each other through electronic social media, including MySpace.

46 According to the Clerk's Record, the appellant was released on pretrial bond with an ankle monitor on October 24, 2007. One of the photographs on the MySpace page for User # 435499766 (registered to “SMILEY FACE” with an email address of “ronnietiendajr@”) is of the appellant lounging in a chair with a gold chain hanging down his chest, wearing bright white sneakers and an ankle monitor. Another MySpace photograph, associated with User # 120841341, shows the appellant and two friends “throwing gang signs” in front of what appears to be a club with the caption, “str8 outta jail and n da club.”

47 A pen packet introduced at the punishment phase of trial confirms that the appellant's date of birth is September 12th.

48 The prosecutor translated this message as: “Yeah, shit, you know I keep it gangster, even after Hector shot at Nu–Nu at Rumors, we still didn't tell. And I know Jesse told him we was there, ‘cause we saw them at the club, but it's cool if I get off, man.”

49 A witness by the name of Hector Gonzalez did indeed testify against the appellant at trial.

50 *Tienda, supra,* at *5 (citing *Griffin v. State,* 192 Md.App. 518, 995 A.2d 791 (2010)).

51 *Griffin v. State,* 419 Md. 343, 19 A.3d 415 (2011).

52 419 Md. 343, 19 A.3d 415 (2011).

53 *Id.,* Md. at 348, A.3d at 418.

54 *Id.*

55 *Id.*

56 *Id.*

57 *Id.*

58 *Id.,* Md. at 357, A.3d at 423.

59 *Id.,* Md. at 351 & 352, A.3d at 420 & 421.

60 *Id.,* Md. at 357–58, A.3d at 424.

61 *Id.,* Md. at 357, A.3d at 423.

62 *Id.,* Md. at 363–65, A.3d at 427–28.

63 *Id.,* Md. at 363, A.3d at 427.

64 *Id.*

65 *Id.,* Md. at 364, A.3d at 428.

66 The State never clearly laid out for the jury how a MySpace account is created and maintained, never defined the terms unique to MySpace technology, and never explained how an account holder accesses and uses his account in the regular course of MySpace activity.

End of Document

Vermont Rules of Evidence, Rule 901

RULE 901. REQUIREMENT OF AUTHENTICATION OR IDENTIFICATION

Currentness

(a) 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.

(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 that a matter is what it is claimed to be.

(2) *Nonexpert Opinion on Handwriting.* Nonexpert opinion as to the genuineness of handwriting, based upon familiarity not acquired for purposes of the litigation.

(3) *Comparison by Trier or Expert Witness.* Comparison by the trier of fact or by expert witness with specimens which have been authenticated.

(4) *Distinctive Characteristics and the Like.* Appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances.

(5) *Voice Identification.* Identification of a voice, whether heard firsthand or through mechanical or electronic transmission or recording, by opinion based upon hearing the voice at any time under circumstances connecting it with the alleged speaker.

(6) *Telephone Conversations.* Telephone conversations, by evidence that a call was made to the number assigned at the time by the telephone company to a particular person or business, if (A) in the case of a person, circumstances, including self-identification, show the person answering to be the one called, or (B) in the case of a business, the call was made to a place of business and the conversation related to business reasonably transacted over the telephone.

(7) *Public Records or Reports.* Evidence that a writing authorized by law to be recorded or filed and in fact recorded or filed in a public office, or a purported public record, report, statement, or data compilation, in any form, is from the public office where items of this nature are kept.

(8) *Ancient Documents or Data Compilation.* Evidence that a document or data compilation, in any form, (A) is in such condition as to create no suspicion concerning its authenticity, (B) was in a place where it, if authentic, would likely be, and (C) has been in existence 20 years or more at the time it is offered.

(9) *Process or System.* Evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result.

(10) *Methods Provided by Statute or Rule.* Any method of authentication or identification provided by statute or by other rules prescribed by the Supreme Court.

Editors' Notes

REPORTER'S NOTES
This rule is identical to Federal and Uniform Rules 901, with minor variations noted below.

Rule 901(a) sets out the basic standard for authentication or identification: "Evidence sufficient to support a finding that the matter in question is what its proponent claims." Note that the preliminary question of fact which the standard raises is technically one of conditional relevancy. Under Rule 104(b), the evidence whose authenticity must be established may be admitted "upon, or subject to," other evidence sufficient to support a finding of authenticity. The effect is to leave the ultimate determination of authenticity to the jury once the judge has found that there is sufficient evidence on the point to create a jury question. See Federal Advisory Committee's Notes to Rules 104(b), 901(a); McCormick, Evidence § 227 at 555 (2d ed. 1972).

The rule applies to the authentication of writings and to the authentication or identification of other objects that are offered as "real" evidence--that is, objects that were themselves actually involved in the events giving rise to the trial. Such "real" evidence can be distinguished from another class of objects that may be offered in evidence--those which serve merely to illustrate or clarify a point and are not offered for their direct probative force on any matter in issue in the case. When used in this way, maps, models, photographs, tape recordings, and the like are denominated "illustrative" evidence and are not subject to the requirement of Rule 901(a). The only basis upon which the admissibility of such evidence is tested is relevance. Illustrative evidence thus primarily presents questions under Rule 401 whether it is a sufficiently accurate depiction to have probative or illustrative value, and under Rule 403 whether that value is outweighed by the potential of the evidence for misleading the jury or unduly delaying or complicating the trial. See, generally, McCormick, supra § 212 at 527-28.

Vermont case law is consistent with Rule 901(a). See, e.g., State v. Hopkins, 56 Vt. 250, 258 (1883) (business entry inadmissible where no evidence that it was in proper handwriting); State v. Woodmansee, 128 Vt. 467, 474-75, 266 A.2d 448, 452 (1970) (authentication of handwriting specimens properly left to the jury on testimony of witnesses who claimed familiarity with alleged writer's handwriting); Knight v. Willey, 120 Vt. 256, 262, 138 A.2d 596, 600 (1958) (sufficiency of foundation as to authenticity of watch alleged to be gift from husband to wife was preliminary question for court); Burns v. Bombard, 128 Vt. 178, 180-81, 260 A.2d 219, 220 (1969) (damaged fender not positively identified or acknowledged as that in collision was properly excluded). Some Vermont cases suggest that authentication requires the proponent of certain kinds of real evidence to establish a continuous chain of custody of the evidence to eliminate any possibility of tampering. See, e.g., State v. Durling, 140 Vt. 491, 498-99, 442 A.2d 455, 458-59 (1981) (dictum). Although the need for a continuous chain of custody is often asserted, no Vermont case has required exclusion of evidence solely on this basis. See id.; State v. LaBelle, 138 Vt. 437, 438, 420 A.2d 851, 851 (1980); State v. Connarn, 138 Vt. 270, 274, 413 A.2d 812, 814 (1980); State v. Mecier, 138 Vt. 149, 152-53, 412 A.2d 291, 293 (1980) (in a 3-to-2 decision, the majority rejects the

argument of the concurring opinion that an "unbroken chain of custody" must be shown to allow admission of a tape recording); State v. Stevens, 137 Vt. 473, 477, 408 A.2d 622, 624 (1979).

Vermont cases also are in accord with the different treatment given to illustrative evidence under the rules. See State v. Mecier, 138 Vt. at 156, 412 A.2d at 295 (photographic evidence is admissible if relevance outweighs possible prejudicial effect); State v. Rebideau, 132 Vt. 445, 450, 321 A.2d 58, 61 (1974) (same); Beattie v. Traynor, 114 Vt. 495, 501, 49 A.2d 200, 201 (1946) (photograph admissible if it fairly represents object pictured and fact pictured is relevant); Hassam v. Safford Lumber Co., 82 Vt. 444, 449, 74 A. 197, 199 (1909) (map admissible to illustrate testimony if "sufficiently accurate to be helpful to the jury"). In a recent case involving a tape recording, the evidence went further than illustrating testimony. As a result, the court applied an authentication test similar to that in Rule 901(a). See State v. Mecier, 138 Vt. at 152-53, 412 A.2d at 293-94.

Especially with respect to documents, many of the authentication requirements in Vermont law have been found in statutes. These same statutes may also provide for exceptions to the hearsay rule and the best evidence rule. The multiple purposes of these statutes may lead to some confusion about their continuing effect after the adoption of the rules.

Statutes dealing with the authentication of real evidence are treated in three different ways under this Article. First, some authentication requirements are imposed by these rules only if they are contained in a statute. For example, under Rule 903 the testimony of a subscribing witness is necessary for authentication only when required by Vermont statute.

Second, some authentication methods found in statutes are authorized by these rules even though the method would not otherwise be effective under these rules. Thus, Rule 902(4) authorizes any method of certification of copies of public records that complies with statute or other rules of court; and Rule 901(b)(10) specifically saves any method of authentication provided by statute or rules of court.

Third, statutes that provide methods of authentication consistent with these rules are affected only in that the rules make formerly exclusive methods of authentication nonexclusive--that is, the proponent can always use any method of authentication provided for in these rules irrespective of what the statute states.

Examples of these three situations are discussed in the notes. Practitioners should be careful in choosing methods of authentication different from those provided in a statute, even when authorized by this Article, because the statute may also be directed at hearsay or best evidence requirements and may continue in effect according to its terms for those requirements.

Rule 901(b) contains a nonexhaustive list of authentication methods. Most of them are found in similar form in Vermont law. Pertinent cases under each example are summarized here:

(1) *Testimony of Witness With Knowledge.* See Tarbell & Whitham v. Gifford, 82 Vt. 222, 224, 72 A. 921, 921-22 (1909) (secretary of association authenticated its records and constitution by testimony as to their use and custody); State v. Savo, 141 Vt. 203, 211-12, 446 A.2d 786, 790-91 (1982) (stocking mask introduced on victim's identification that robber wore similar mask); State v. LaBelle, 138 Vt. at 438, 420 A.2d at 851-52 (breath sample admitted where officer and chemist identified it, despite errors in labeling the sample); State v. Connarn, 138 Vt. at 274, 413 A.2d at 815 (bag with drugs sold by defendant where officers testified that it was always in their custody although not sealed); State v. White, 129 Vt. 220, 227, 274 A.2d 690, 694 (1971) (marijuana taken from defendant at arrest properly admitted on testimony of narcotics agent and chemist that it was in their custody at all times); State v. Miner, 128 Vt. 55, 63, 258 A.2d 815, 820 (1969) (identification of defendant as person who called FBI by testimony of persons present with him at time); State v. Bean, 77 Vt. 384, 404, 60 A. 807, 813 (1905) (to show origin of hayrack stake used as murder weapon, another stake from same hayrack admitted on testimony of owner and witness who had seen second stake in place). Some statutes provide

for this method of authentication. See, e.g., 12 V.S.A. § 1700(b) (business records can be authenticated by custodian or other qualified witness).

The Uniform Rule includes the phrase "with knowledge" in the rule text. Omission of the phrase here does not eliminate the requirement of personal knowledge except in the case of an expert witness. See Rules 602, 703.

(2) *Nonexpert Opinion on Handwriting.* See State v. Ryder, 80 Vt. 422, 426-27, 68 A. 652, 654 (1908) (witnesses who had seen subject write on other occasions); Andrews v. Aldrich, 104 Vt. 235, 237, 158 A. 676, 677 (1932) (dictum: requisite familiarity may be gained by seeing subject write, receiving responsive letters from or sending responsive letters to subject, or incorporating or relying on letters from subject in business transactions); In re Diggins' Estate, 68 Vt. 198, 200, 34 A. 696, 697 (1896) (seeing name written once was sufficient); State v. Woodmansee, 128 Vt. at 474-75, 266 A.2d at 452-53 (warden's receipt of letters in usual course of business, upon which he communicated and acted). Cf. 14 V.S.A. § 110 (when witness to will is unavailable, will may be proved by testimony that the signature is in the handwriting of the testator). Vermont cases are silent on familiarity acquired for purposes of litigation, but would presumably reject such testimony on general grounds like those of Rule 403.

(3) *Comparison by Trier or Expert Witness.* See State v. Ryder, 80 Vt. at 426-27, 68 A. at 654 (comparison of handwriting by jury); State v. Bean, 77 Vt. at 404-05, 60 A. at 813 (comparison of hayrack stakes by jury); Davis v. Dunn, 90 Vt. 253, 256-60, 98 A. 81, 82-84 (1916) (comparison by expert of X-ray photographs to identify earlier photograph as plaintiff's wrist); State v. Kent, 83 Vt. 28, 30-35, 74 A. 389, 390-92 (1909) (comparison of writings with carved initials and dates in barn door).

(4) *Distinctive Characteristics and the Like.* See Whitney Wagon Works v. Moore, 61 Vt. 230, 239-40, 17 A. 1007, 1010 (1888) (retained copy of letter authenticated by comparison of its date and date of reply). Some cases in this area involve use of such techniques as ancillary to or corroborative of other methods. See State v. LaBelle, 138 Vt. at 438, 420 A.2d at 851-52 (officer's signature on box containing breath sample); State v. Reuschel, 131 Vt. 554, 559, 312 A.2d 739, 742 (1973) (letter identified because a reply to a letter written to author, and by handwriting); State v. Kent, 83 Vt. at 31-32, 74 A. at 390-91 (authentication of carvings through distinctive punctuation patterns, as well as handwriting); State v. Lacaillade, 131 Vt. 161, 163, 303 A.2d 131, 132 (1973) (speaker in telephone conversation identified in part through possession of knowledge peculiar to defendant).

(5) *Voice Identification.* See State v. Lacaillade, 131 Vt. at 163, 303 A.2d at 132-33 (officer calling defendant recognized voice from prior conversation).

(6) *Telephone Conversations.* See State v. Lacaillade, 131 Vt. at 163, 303 A.2d at 132-33 (officer testified that he called defendant at listed number and that person answering identified himself as defendant).

(7) *Public Records or Reports.* This example applies to public documents which cannot meet the requirements for self-authentication under Rule 902. Of course, such evidence must also meet hearsay objections before it is admissible. See Reporter's Notes to Rules 803(8)-(10). Vermont cases are consistent with the rule. See, e.g., Town of Ripton v. Town of Brandon, 80 Vt. 234, 238, 67 A. 541, 542-43 (1907) (grand list authenticated by town clerk's testimony that the list came from proper repository); cf. Isaacs v. Shattuck, 12 Vt. 668, 672 (1839) (document erroneously certified would have been admitted if shown to be in town clerk's handwriting).

(8) *Ancient Documents or Data Compilations.* The Vermont cases are consistent with the rule, except that they assert a 30-year time requirement and, for admissibility of deeds, require that possession of the property have been taken. Those requirements have been abandoned in the rule. See Federal Advisory Committee's Note to Rule 901(8). Note that, as with public documents, admission of ancient documents may also involve a hearsay problem. The requirements of the

ancient documents exception, Rule 803(16), will be met, however, by any document meeting the tests of the present rule. See Reporter's Notes to Rule 803(16).

For the Vermont cases, see, e.g., Aldrich v. Griffith, 66 Vt. 390, 404, 29 A. 376 (1893) (genuineness of surveyor's field book over 45 years old established by fact that it was found in town clerk's office); Williams v. Bass, 22 Vt. 352, 355 (1850) (where possession not shown, ancient record of deed not admitted); Booge's Ex'rs v. Parsons, 2 Vt. 456, 459-61 (1830) (unauthenticated record of deed over 40 years old found in proper place in record book in town clerk's handwriting admitted, where possession shown).

(9) *Process or System.* Examples on this point include evidence of the accuracy of systems such as computer storage and retrieval. See Westinghouse Elec. Supply Co. v. B.L. Allen, Inc., 138 Vt. 84, 101-02, 413 A.2d 122, 132 (1980); Federal Advisory Committee's Note to Rule 901(9).

(10) *Methods Provided by Statute or Rule.* In this paragraph "statute" is substituted for "Act of Congress" in the Federal Rule. The term would include any federal statute that purports to bind state courts. The paragraph departs from the Uniform Rule by not including the state Constitution as a source of authentication procedures. No such procedures have been found in the Vermont Constitution. Examples of authentication procedures saved are those in 14 V.S.A. § 2671 (a letter from a doctor can support a finding that a petitioner understands the nature of a guardianship); V.R.C.P. 30(f), 44; and V.R.Cr.P. 27.

Rules of Evid., Rule 901, VT R REV Rule 901
State court rules are current with amendments received through February 15, 2017.