Antoine Levar Griffin v. State of Maryland, No. 74, September Term 2010.

EVIDENCE – AUTHENTICATION – ELECTRONICALLY STORED INFORMATION – SOCIAL NETWORKING – MYSPACE

Pages allegedly printed from MySpace were not properly authenticated pursuant to Maryland Rule 5-901, because someone other than the purported creator could have created the profile and also posted the comment in question, when the State identified only the date of birth of the creator and her visage in a photograph on the site.

IN THE COURT OF APPEALS OF MARYLAND

No. 74

September Term, 2010

ANTOINE LEVAR GRIFFIN

v.

STATE OF MARYLAND

Bell, C.J.
Harrell
Battaglia
Greene
Murphy
Adkins
Barbera,

JJ.

Opinion by Battaglia, J.
Harrell and Murphy, JJ., dissent.

Filed: April 28, 2011

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

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

---

[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).

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]
>
> 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:

---

[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.

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

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 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

---

[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.

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 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 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.
> [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 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, 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 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:

---

[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.

> 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).

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:

> 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 chose

---

[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

(continued...)

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 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

---

[9](...continued)

> 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/.

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.

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

---

[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).

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. 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, 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).

In the present case, Griffin argues that the State did not appropriately, for evidentiary purposes, authenticate the 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 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 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*, 926 N.E.2d 1162 (Mass. 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, testified that she had spent the evening of the murder

---

[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.").

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 "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 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*, 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 supremacist groups who took responsibility for 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]

Similarly, the State relies upon an unreported opinion, *State v. Bell*, 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 improperly admitted "online conversations and

---

[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 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 e-mail heading itself); *Commonwealth v. Amaral*, No. 09-P-2284, 2011 Mass. App. LEXIS 107, at *7 (Mass. App. Ct. Jan. 26, 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).

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 *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.

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 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.

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 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: What's Evidence Between "Friends"?*, Boston Bar J., Jan.– Feb. 2009, at 5, 7.

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

---

[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).

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*, 891 N.Y.S.2d 511 (N.Y. App. Div. 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 court concluded that such testimony provided ample authentication linking the MySpace messages in question to Clevenstine himself.[15]

---

[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." (continued...)

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.

[15](...continued)
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.

IN THE COURT OF APPEALS

OF MARYLAND

No. 74

September Term, 2010

ANTOINE LEVAR GRIFFIN

v.

STATE OF MARYLAND

Bell, C.J.,
Harrell
Battaglia
Greene
Murphy
Adkins
Barbera,

JJ.

Dissenting Opinion by Harrell, J.,
which Murphy, J., joins.

Filed: April 28, 2011

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 . . . ." __ Md. __, __, __ A.3d __, __ (2011) (Majority slip op. at 14).

Maryland Rule 5-901 ("Requirement of authentication or identification") derives from and is similar materially to Federal Rule of Evidence 901.[1] *See Washington v. 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

---

[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.

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. Drombowski*, 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 Dickens v. State*, 175 Md. App. 231, 239, 927 A.2d 32, 37 (2007) (citing *United States v.*

---

[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).

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 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 the trial court to instruct the jury that "if they were not satisfied of the identity of the paper . . . , then they

[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.").

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.