2011

Writings on the Wall: The Need for an Authorship-Centric Approach to the Authentication of Social-Networking Evidence

Ira P. Robbins

Forthcoming in Volume 13, Issue 1 of the *Minnesota Journal of Law, Science & Technology*
(Winter 2011)

Writings on the Wall: The Need for an Authorship-Centric Approach to the Authentication of Social-Networking Evidence

Ira P. Robbins*

ABSTRACT

People are stupid when it comes to their online postings. The recent spate of social-networking websites has shown that people place shocking amounts of personal information online. Unlike more traditional modes of communication, the unique nature of these websites allows users to hide behind a veil of anonymity. But while social-networking sites may carry significant social benefits, they also leave users—and their personal information—vulnerable to hacking and other forms of abuse. This vulnerability is playing out in courtrooms across the country and will only increase as social-networking use continues to proliferate.

This Article addresses the evidentiary hurdle of authenticating social-networking evidence, a novel legal issue confronting courts today. The Article explains and critiques four approaches used by different jurisdictions, concluding that each approach fails to adequately address the critical issue of authorship. The anonymous nature of social-networking websites, coupled with the extent of users' personal information available online, raises serious concerns about the authorship of any piece of evidence posted to one of these sites. Litigants are using social-networking postings in court, attributing authorship to a particular person without demonstrating a sufficient nexus between the posting and the purported author.

* Barnard T. Welsh Scholar and Professor of Law and Justice, American University, Washington College of Law. A.B. University of Pennsylvania; J.D. Harvard University. I am grateful to my superb and indispensable research assistants—Elizabeth Aniskevich, Dana Bucy, Kierstan Carlson, Jay Curran, Giulia Di Marzo, Christin Helms, Kara Karlson, Tracey Little, Laura Peterson, Libby Ragan, and Amy Smith—who taught me a great deal more than I ever taught them; to Andrew Robbins—the master guru of all things computer- and Internet-related—for invaluable editorial suggestions, for keeping me apprised of technological developments and of new ways to take over someone's identity on social-networking websites, and for steering me clear of unintended pitfalls; and to the American University Law School Research Fund, for providing summer financial support.

Absent this nexus, however, the evidence fails to meet even the low hurdle of authentication. To remedy this problem, this Article proposes that courts shift their focus from account ownership and content to authorship of the evidence. Working within the existing rules of evidence, this approach underscores the importance of fairness and accuracy in the outcome of judicial proceedings that involve social-networking evidence.

INTRODUCTION

People are stupid when it comes to their online postings.[1] Using social-networking sites, people document their every move no matter how foolish or incriminating. This propensity applies not only to ordinary citizens,[2] but also to lawyers,[3] judges,[4] and even members of Congress.[5] New York Congressman Chris

[1] I certainly do not mean to imply that people are not also stupid in other settings and contexts. I leave that discussion for others, however, as this is only a law review article and not a multi-volume treatise.

[2] News stories and law review articles abound with examples of idiotic behavior exhibited online. *See, e.g.*, Evan E. North, *Facebook Isn't Your Space Anymore: Discovery of Social Networking Websites*, 58 U. KAN. L. REV. 1279, 1279 (2010) (providing one example of an insurance company that persuaded an attorney to settle an accident claim after finding on Facebook and MySpace photographs and video of the attorney's client "snowboarding . . . [and] 'going off jumps on his snowboard at a high rate of speed'"). Edward Marshall, *Burglar Leaves his Facebook Page on Victim's Computer*, THE JOURNAL (Sept. 16, 2009), http://www.journal-news.net/page/content.detail/id/525232.html (describing the ill-fated Facebook status-check that led to the burglar's arrest after he stole two diamond rings in the same room as the computer—but not the computer); Jason Deans, *Facebook Juror Jailed for Eight Months*, GUARDIAN.CO.UK (June 16, 2011, 11:07 AM), http://www.guardian.co.uk/uk/2011/jun/16/facebook-juror-jailed-for-eight-months (explaining that juror Joanne Fraill was held in contempt of court and sentenced to eight months in jail for Facebook-messaging the defendant about the case and the pending charges while the jury was deliberating); Leah Hope, *Authorities Make String of Underage Drinking Arrests from Facebook Photos*, ABC7NEWS.COM, Jan. 14, 2008, http://abclocal.go.com/wls/ story?section=news/local&id=5890815 (reporting on charges filed against teenagers in a Chicago suburb for possession of alcohol by a minor that resulted from authorities' discovery of photographs posted on Facebook depicting the underage drinking at a house party); Mary Lynn Smith & Courtney Blanchard, *Facebook Photos Land Eden Prairie Kids in Trouble*, STAR TRIB. (Minneapolis), Jan. 9, 2008, at B1. Mary Lynn Smith & Courtney Blanchard, *Facebook Photos Land Eden Prairie Kids in Trouble*, STAR TRIB. (Minneapolis), Jan. 8, 2008, http://www.startribune.com/local/west/13549646.html (detailing the punishment of more than 100 students in a Minneapolis suburb after school administrators obtained photographs from Facebook of the students holding and consuming alcoholic beverages).

[3] After proudly posting on his Facebook page that he obtained a mistrial for his client, a New Jersey defense attorney was later mocked by the press because the mistrial occurred "due to the defense lawyer's [poor] trial performance." Debra Cassens Weiss, *Lawyer Who Never Tried a Case Proud of Murder Mistrial on Facebook, Humiliated in Interview*, ABAJOURNAL.COM (Apr. 5, 2011, 7:41 AM), http://www.abajournal.com/news/article/lawyer_who_never_tried_a_ case_proud_of_murder_mistrial_on_facebook_humiliat/?utm_source=maestro&utm_medium=email&utm_campaign=weekly_email. A prosecutor from Minnesota allegedly posted "keeping the streets safe from Somalians" to her Facebook account while prosecuting a Somali man for murder. Abby Simons, *Facebook Motion Thrown out Again*, STAR TRIB. (Minneapolis), Mar. 13, 2010, at B4. In Texas, a lawyer found herself caught in a lie when, after asking the judge for a continuance to attend a relative's funeral, the judge viewed the lawyer's Facebook profile, which showed that the lawyer was in fact on vacation. Molly McDonough, *Facebooking Judge Catches Lawyer in Lie, Sees Ethical Breaches*, ABAJOURNAL.COM (July 31, 2009, 3:16 PM), http://www.abajournal.com/news/article/facebooking_judge_catches_lawyers_in_lies_crossing_ethical_lines_abachicago/.

[4] A North Carolina judge received a public reprimand when he not only agreed to "friend" a lawyer who was appearing before him, but also proceeded to communicate with the lawyer via Facebook about the case as the trial

Lee's recent faux pas presents a prime example of such idiocy. Representative Lee sent flirtatious messages and shirtless photographs of himself to a woman via Craigslist while using his own name and an "e-mail address traceable to his Facebook page."[6] This momentary lapse in judgment forced the Congressman to resign from office in February 2011.[7]

More recently, New York Congressman Anthony Weiner followed suit by partaking in several inappropriate relationships using a variety of social-networking sites; most notably, Congressman Weiner sent a lewd photograph of himself to a college student via Twitter.[8] Even though the photograph message was traceable to his Twitter account, Representative Weiner adamantly denied having sent it, claiming that his account was hacked.[9] About a week later, Representative Weiner confessed that he had in fact sent the photograph[10] and, shortly thereafter, resigned due to political pressure.[11]

Gaffes like Representatives Lee's or Weiner's are sure to become increasingly common as more people put their personal lives online. This is especially true with social-networking websites like Facebook, MySpace, and Twitter. In recent years, these sites have become an ingrained part of our culture. Their popularity can be seen in a variety of ways: individuals use them to connect with friends; media outlets use them to get viewers' perspectives on the latest news;[12] companies and educational institutions use them to keep closer contact with their customers and students;[13] and non-profit organizations use them to garner support for their

---

progressed. Robert J. Ambrogi, *Facebook Friend Earns Judge a Reprimand*, LEGAL BLOG WATCH (June 1, 2009, 2:09 PM), http://legalblogwatch.typepad.com/legal_blog_watch/2009/06/facebook-friend-earns-judge-a-reprimand. html.

[5] *See* Roxanne Roberts & Amy Argetsinger, *The Chris Lee Scandal and the anonymity of the average congressman*, THE RELIABLE SOURCE (Feb. 14, 2011, 12:00AM), http://voices.washingtonpost.com/reliable-source/2011/02/the_chris_lee_scandal_and_the_anonymity_of_the_average_congressman.html; *see also* David A. Fahrenthold & Aaron Blake, *Congressman Resigns After Report of Online Flirting*, WASH. POST, Feb. 10, 2011, at A1.; Chris Cuomo, Chris Vlasto & Devin Dwyer, *Rep. Anthony Weiner: 'The Picture Was of Me and I Sent It,'* ABC7NEWS.COM, June 6, 2011, http://abcnews.go.com/Politics/rep-anthony-weiner-picture/story?id=13774605.

[6] Roberts & Argetsinger, *supra* note 5.

[7] Fahrenthold & Blake, *supra* note 5.

[8] Cuomo et al., *supra* note 5.

[9] *Id.*

[10] *Id.*

[11] David A. Fahrenthold & Paul Kane, *As Controversy Builds, Weiner Resigns*, WASH. POST, June 17, 2011, at A1.

[12] *See, e.g.*, CNN, FACEBOOK, http://www.facebook.com/cnn (last visited Sept. 16, 2011) ("The CNN fan page provides instant breaking news alerts and the day's newsiest and most talked about stories.").

[13] *See, e.g.*, *LLM Program in Law & Government - Washington College of Law - AU*, FACEBOOK, http://www.facebook.com/LawGovAUWCL (last visited Sept. 16, 2011) ("A page for Students, Alumni, Faculty and Friends of the LL.M. Program in Law & Government at American University Washington College of Law.").

causes.[14] But as the sites' popularity increases, so does their susceptibility for abuse.

Social-networking sites have become conduits for crimes and other wrongful behavior—such as harassment and bullying—because they are both easy to use and can be anonymous.[15] Consequently, these sites are beginning to play a critical role in litigation. Social-networking postings[16] have been entered as evidence in all forms of litigation, often against the alleged authors of the postings. This Article focuses on the authentication of this type of evidence at trial.

The authentication requirement is a preliminary evidentiary threshold, mandating that proponents of evidence provide proof "sufficient to support a finding that the matter in question is what its proponent claims."[17] Moreover, the requirement advances one of the major goals of the rules of evidence: to ensure that, in the end, the "truth may be ascertained and proceedings justly determined."[18] Considering the vulnerability of social-networking sites to exploitation, authentication is a critical component to guarantee, to the greatest extent possible, that juries are presented with reliable evidence, and that the proceedings are fair and just.[19]

Part I of this Article presents background information on typical uses of social-networking sites as well as examples of how people misuse these sites by creating fake accounts or hacking into other accounts to obtain or alter the owner's personal information. Part II outlines the various roles that social-networking sites play in litigation. Law-enforcement officials, as well as lawyers, increasingly are turning to social-networking sites to search for evidence or to gather information to impeach a witness's credibility. Part III discusses authentication requirements in general. Part IV provides an in-depth explanation of the current judicial approaches used to authenticate social-networking evidence. Part IV then critiques these approaches, specifically addressing courts' failures to require a demonstrated

---

[14] *See, e.g.*, *American Red Cross*, FACEBOOK, http://www.facebook.com/redcross (last visited Sept. 16, 2011) ("The American Red Cross is a humanitarian organization led by volunteers. We provide relief to victims of disaster and help people prevent, prepare for, and respond to emergencies.").

[15] *See, e.g.*, *infra* note 32.

[16] For the purposes of this paper, I refer to both postings and messages as "postings." See discussion *infra* Part I.A for a differentiation between private postings that are sent between users, known as messages, and public postings that are displayed on a user's public profile page.

[17] FED. R. EVID. 901(a).

[18] FED. R. EVID. 102.

[19] The court in *St. Clair v. Johnny Oyster & Shrimp*, 76 F. Supp. 2d 773 (S.D. Tex. 1999) was incredibly suspicious of all web-based evidence, stating that the Internet is "one large catalyst for rumor, innuendo, and misinformation" and that "hackers can adulterate the content on *any* web-site from *any* location at *any* time." *Id.* at 774–75 (emphasis in original). *But see* Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1153 (C.D. Cal. 2002) (declining to follow the "extreme view" taken by *St. Clair*). Despite the polar, and perhaps outdated, position espoused by the *St. Clair* court, it raised the issues that future courts deciding the authenticity of social-networking postings must consider: From where did the information come, who authored it, and did anyone alter it?

nexus between the postings being offered into evidence and the purported author of the postings. Finally, Part V advocates a new, authorship-centric approach to authentication. Working within Federal Rule of Evidence 901(b)(4), this Part recommends a set of factors that courts should consider when ruling on the authenticity of social-networking evidence. The Article concludes that authorship is critical to authentication. Courts should thus act as gatekeepers, considering these issues at the admissibility stage before admitting the evidence and allowing the finder of fact to weigh its reliability.

I. USES OF SOCIAL-NETWORKING SITES

Social-networking sites are websites that "link networks of individuals into online communities through personalized web 'profiles.'"[20] These sites established an Internet presence in the early 2000s and have seen a recent and drastic increase in popularity.[21] This Part discusses the general uses of social-networking sites, as well as common misuses—such as creating fake accounts and hacking.

A. General Uses

Social-networking sites facilitate interpersonal relationships and information exchanges by allowing individual users to search for others who are part of their social network and add them as "friends."[22] Each social-networking user creates a profile page. Facebook explicitly requires members to use their real names when

---

[20] Daniel Findlay, Comment, *Tag! Now You're Really "It" What Photographs on Social Networking Sites Mean for the Fourth Amendment*, 10 N.C.J.L. & TECH. 171, 180 (2008). In 2007, the two dominant social-networking sites were Facebook, founded in 2004 by an undergraduate at Harvard University, and MySpace, founded in 2003 by two Silicon Valley friends. John S. Wilson, Comment, *MySpace, Your Space, or Our Space? New Frontiers in Electronic Evidence*, 86 OR. L. REV. 1201, 1221–22 (2007); *see also* Danah M. Boyd & Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship*, 13 J. COMPUTER-MEDIATED COMM. (2007), http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html. Twitter has now taken over the number two spot, followed by MySpace and LinkedIn. *Top 15 Most Popular Social Networking*, EBIZMBA.COM, http://www.ebizmba.com/articles/social-networking-websites (last visited Sept. 16, 2011).

[21] *See* AMANDA LENHART ET AL., PEW RESEARCH CTR., SOCIAL MEDIA & MOBILE INTERNET USE AMONG TEENS AND YOUNG ADULTS 2 (2010), *available at* http://pewinternet.org/Reports/2010/Social-Media-and-Young-Adults.aspx (summarizing the increased use of social-networking among teens and both young and older adults). In particular, the use of social-networking sites has increased exponentially in the last few years. In 2009, Facebook membership exceeded 300 million users, and 73% of online teens use social-networking sites, up from 55% in November 2006 and 65% in February 2008. *Id.* at 2; Shannon Aswumb, *Social Networking Sites: The Next E-Discovery Frontier*, 66 BENCH & B. MINN. 23, 23 (2009), *available at* http://www.mnbar.org/bench andbar/2009/nov09/networking.html. In 2011, Facebook membership exceeded 750 million users. *Factsheet*, FACEBOOK, http://www.facebook.com/press/info.php?factsheet (last visited Sept. 16, 2011). The social-networking phenomenon is not limited to younger Internet users. Forty-seven percent of online adults use social-networking sites, representing a ten-percentage-point increase since November 2008. LENHART, *supra* note 21, at 3.

[22] *See* Boyd & Ellison, *supra* note 20, at 213.

creating profiles, but many other social-networking sites, such as MySpace, actually encourage the creation of pseudonymous accounts by permitting users to create profiles using nicknames, symbols, and incorrect capitalization.[23] These profiles display personal, identifying information such as birth dates, hometowns, alma maters, and relationship statuses. They are the medium through which users exchange anecdotes about their interests and activities.[24] Users also share photographs and videos, in which they may "tag," or identify, other users.[25] On most social-networking sites, users can send private messages to others as well as make comments on their own or other users' profile pages. These latter comments are not necessarily private; the number of people who can see them depends on both the specific social-networking site and the users' individual settings. Users govern their social-networking experiences by providing as much or as little information on their profile pages as they wish, and by controlling their privacy settings to restrict who can view and post information to these pages.[26]

While social-networking sites allow individuals to reconnect with old friends or find new ones with ease, they also are being used to harass, intimidate, and emotionally abuse or bully others. Malefactors can utilize pseudonyms to create fake accounts without the alleged account holder's knowledge or consent; they can also hack into legitimate accounts to access the vast quantities of personal information that the accounts contain.

B. Fake Accounts

[23] *Statement of Rights and Responsibilities*, FACEBOOK, http://www.facebook.com/terms.php (last visited Sept. 17, 2011); *Terms of Use Agreement*, MYSPACE.COM, http://www.myspace.com/help/terms (last visited Sept. 17, 2011).
[24] *See* Wilson, *supra* note 20, at 1220.
[25] Facebook defines "tagging" as follows: "A tag links a person, page, or place to something you post, like a status update or a photo." Help Center, FACEBOOK, http://www.facebook.com/help/?page=18947 (last visited Sept. 30, 2011).
[26] *See generally* Matthew J. Hodge, Comment, *The Fourth Amendment and Privacy Issues on the "New" Internet: Facebook.com and MySpace.com*, 31 S. ILL. U. L.J. 95, 107–09 (2006) (indicating that the default privacy setting on MySpace allows all users to see a profile, and that the default setting on Facebook allows all users within a "network" to view a profile). A user's privacy settings are not all-encompassing and can be prone to ambiguity, error, or outright fraud. *See, e.g.*, Dan Goodin, *Facebook Caught Exposing Millions of User Credentials*, THE REGISTER (U.K.) (May 10, 2011, 7:23 PM), http://www.theregister.co.uk/2011/05/10/facebook_user_credentials_leaked/ (stating that "Facebook has leaked access to millions of users' photographs, profiles and other personal information because of a years-old bug that overrides individual privacy settings," and that "Facebook over the years has regularly been criticized for compromising the security of its users"); Jason Kincaid, *New Facebook iPhone App Brings New Privacy Bugs With It*, TECHCRUNCH.COM (Sept. 8, 2009), http://techcrunch.com/2009/09/08/new-facebook-iphone-app-brings-new-privacy-bugs-with-it/ (describing iPhone Facebook application bug circumventing user privacy settings).

"Fake" accounts are social-networking accounts that are either created in one person's name by someone else or by a person using a pseudonym.[27] These accounts are often used as conduits for teasing and bullying.[28] The "Terms of Service," or user agreements, of many social-networking sites prohibit users from creating profiles that impersonate others, as well as from using the site to harass others or commit crimes.[29] Yet there is effectively no check on fake accounts or false profiles, unless someone lodges a complaint with the social-networking company.[30]

Regardless of these restrictions, social-networking users are increasingly making use of these sites for harassing behavior.[31] In addition, the anonymity of social-networking sites permits stalkers and bullies—using fake accounts—to take their harmful conduct above and beyond traditional harrying.[32] The infamous Lori Drew and Latisha Monique Frazier cases provide excellent examples. Drew, the mother of a thirteen-year-old girl, created a MySpace page with the picture of a

---

[27] *See, e.g.*, *infra* note 32 and accompanying text.

[28] *See, e.g.*, *infra* note 32 and accompanying text.

[29] *See Statement of Rights and Responsibilities*, *supra* note 23 and accompanying text.

[30] *E.g.*, Ki Mae Huessner, *Teens Sued for Fake Facebook Profile*, ABCNEWS.COM (Sept. 29, 2009), http://abcnews.go.com/Technology/AheadoftheCurve/teens-sued-fake-facebook-profile/story?id=8702282 (reporting the comments of a Facebook representative, stating that "the time it takes for the team to respond depends on the complaint[;] . . . reports of nudity, pornography and harassing personal messages are the highest priority complaints").

[31] At least two federal cases have addressed this problem. Students created false MySpace accounts with cut-and-pasted pictures from school-district websites and posted crude and embarrassing misinformation to mock their schools' principals. In one of the cases, a high-school student created an account in his principal's name, claimed that the principal smoked marijuana and drank alcohol at work, and referred to the principal as a "big whore," "big fag," and "big steroid freak." Layshock *ex rel*. Layshock v. Hermitage Sch. Dist., 496 F. Supp. 2d 587, 591 (W.D. Pa. 2007). Another case involved two eighth-grade students who created a fake account that portrayed their principal as a pedophile and a sex addict. J.S. *ex rel*. Snyder v. Blue Mountain Sch. Dist., 593 F.3d 286, 290-92 (3d Cir. 2010) (noting that one of the students helped to create the false page because she was "mad" at the principal for disciplining her for a dress code violation), *vacated, reh'g en banc granted*, 650 F.3d 915 (3d Cir. 2011). In *Snyder*, the account contained the principal's picture with the profile name "kidsrockmybed" and listed as among the principal's interests "fucking in my office [and] hitting on students and their parents." *Id.* at 291.

[32] *See, e.g.*, Jan Hoffman, *As Bullies Go Digital, Parents Play Catch-up*, N.Y. TIMES, Dec. 5, 2010, at A1 (recounting numerous stories of middle- and high-school students bullying one another via pseudonymous accounts on social-networking sites, and advising parents about ways to address such bullying). In one tragic case in the United Kingdom, an adult man who was a known sex offender created a fake Facebook profile using the picture of a good-looking teenage boy and pretended to be sixteen years old. *Ashleigh Hall Was 'Spitting Image' of Alleged Killer's Former Fiancée*, THE TELEGRAPH (U.K.) (Oct. 29, 2009), http://www.telegraph.co.uk/news/uknews/crime/6458211/Ashleigh-Hall-was-spitting-image-of-alleged-killers-former-fiancee.html [hereinafter *Ashleigh Hall*] (reporting the killer's use of Facebook in his crimes); James Slack & Paul Sims, *My Guilt at Letting that Evil Man Walk Free: Prostitute Held Hostage for 15 Hours by Facebook Killer Speaks of Regret*, MAIL ONLINE (U.K.) (Mar. 12, 2010), http://www.dailymail.co.uk/news/article-1256307/Facebook-warning-Peter-Chapman-admits-Ashleigh-Hall-murder.html (providing the picture used by the killer, and reporting that the murder led to a slew of complaints regarding Facebook's security measures). The man used the fake Facebook profile to lure in a teenage girl, whom he later raped and murdered. *See Ashleigh Hall*, *supra*. Other less egregious examples of misconduct on Facebook have also been reported, including one instance in which a teen's peers created a Facebook profile in his name and with his picture and depicted the teen as homosexual and racist; they used the false profile to "friend" nearly 600 people. Huessner, *supra* note 30.

fictitious sixteen-year-old boy named "Josh Evans."[33] Drew used this fake profile to torment her daughter's thirteen-year-old "nemesis," Megan Meier, who "had a history of depression and suicidal impulses."[34] Using the Evans profile, Drew flirted with Meier for a period of time, then abruptly told Meier that Evans "no longer liked her" and that "the world would be a better place without her in it."[35] Shortly thereafter, Meier killed herself.[36] Drew then deleted the fake account.[37]

Similarly tragic is the recent story of Latisha Monique Frazier. In August 2010, Frazier went missing shortly after leaving work for the day.[38] As if her disappearance was not difficult enough for her family, someone created a fake Facebook profile for Frazier and used it to threaten and harass her family.[39] The first message sent from this profile stated: "Your sister is dead and gone. I'm watching you! One more dead to go!"[40] After Frazier's family distributed fliers in the neighborhood to warn others about her disappearance, they received another message: "Her black ass has been gone . . . . Body parts in Rock Creek. Keep the fliers out of the . . . hood. We took them down."[41] Fortunately for Frazier's family, a local television station aired a story about this harassment, which ultimately led to the arrest of six people allegedly involved in her disappearance and murder.[42]

C. Hacking and Identity Theft

Beyond those who create fake accounts to threaten and harass others, people may break into existing social-networking accounts to acquire or modify information that the accounts contain. These hackers use a number of techniques to steal users' login data, including conning users into divulging their passwords and employing "malware that logs keystrokes."[43] Once hackers achieve access to a user's account,

---

[33] United States v. Drew, 259 F.R.D. 449, 452 (C.D. Cal. 2009).
[34] Jennifer Steinhauer, *Woman Found Guilty in Web Fraud Tied to Suicide*, N.Y. TIMES, Nov. 27, 2008, at A25; *see also Drew*, 259 F.R.D. at 452.
[35] *Drew*, 259 F.R.D. at 452.
[36] *Id.*
[37] *Id.*
[38] Sam Ford & Richard Reeve, *D.C. Family Threatened on Facebook*, TBD.COM (Jan. 23, 2011, 8:29 PM), http://www.tbd.com/articles/2011/01/d-c-family-receives-facebook-threats-46527.html.
[39] *Id.*
[40] *Id.*
[41] *Id.*
[42] *Id.*; Keith L. Alexander, *Suspect Arraigned in Slaying of District Woman*, WASH. POST, Jan. 24, 2011, http://www.washingtonpost.com/wp-dyn/content/article/2011/01/24/AR2011012405883.html; *see also* Keith L. Alexander, *No Landfill Search for Body of Slain Teen, D.C. Police Say*, WASH. POST, Mar. 3, 2011, http://www.washingtonpost.com/wp-dyn/content/article/2011/03/03/AR2011030304912.html.
[43] Riva Richmond, *Stolen Facebook Accounts for Sale*, N.Y. TIMES, May 3, 2010, at B3. Recently, Jesse William McGraw, the "former leader of an anarchistic hacking group called the Electronik Tribulation Army," was sentenced to more than nine years in prison after installing malware on computers at a Texas hospital where he worked as a

they have free reign over all personal information contained therein. They can use the account to distribute computer viruses and spam as well as to post and send messages that appear to come from the user.[44]

Notably, pervasive posting of personal information on social-networking sites has facilitated identity theft because hackers can obtain this information and use it for their own gain.[45] Users who post seemingly innocuous information to their social-networking profiles, such as full name and birth date, are particularly susceptible to identity theft.[46] A person's name and birth date, combined with certain personal details that are readily available from a social-networking profile, can supply enough information for an identity thief to apply for credit in that person's name or to hack into his or her existing credit accounts.[47]

In addition to misusing information from individual users' accounts, identity thieves are also targeting users' "friends" in a variation of the well-known "Nigerian scam."[48] Playing on the increased levels of trust users place in social-networking

---

security guard. Kevin Poulsen, *Leader of Hacker Gang Sentenced to 9 Years For Hospital Malware*, WIRED.COM (Mar. 18, 2011, 7:56 PM), http://www.wired.com/threatlevel/tag/anonymous/.

[44] *See* Richmond, *supra* note 43; Brian Krebs, *Hacker's Latest Target: Social Networking Sites*, WASH. POST, Aug. 9, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/08/08/AR2008080803671.html.

[45] *Cf.* U.S. DEP'T OF JUSTICE, IDENTITY THEFT AND IDENTITY FRAUD, http://www.justice.gov/criminal/fraud/websites/idtheft.html (defining identity theft as a crime "in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain").

[46] *See* Kevin D. Bousquet, *Facebook.com vs. Your Privacy – By a Private Investigator*, THE PRIVATE INVESTIGATION CENTRE (Apr. 25, 2007, 3:27 AM), http://corpainvestigation.wordpress.com/2007/04/25/facebookcom-vs-your-privacy-by-a-private-investigator/ (asserting that a person's identity can be stolen merely from the name and birth date and warning about the ease with which hackers can sign onto Facebook and "harvest" the personal information of hundreds of people).

[47] *See* Steve Lohr, *How Privacy Vanishes Online*, N.Y. TIMES, Mar. 16, 2010, at A1 (describing the process of "data mining," in which pieces of personal information available on the Internet can be used to predict and describe a picture of a person's identity with reasonable accuracy); *see also* Bousquet, *supra* note 46 (advising readers that many of the answers to typical verification questions asked by credit card companies and banks can be found on social-networking profiles, including mother's maiden name, dog's name, and high school). This threat is likely to worsen as methods of compiling personal data from various websites that people visit increase in sophistication because such data can reveal social patterns, which in turn, can be used to assist in identity theft. *See* Lohr, *supra*. For instance, researchers studying the correlations between Flickr and Twitter accounts were able to identify more than thirty percent of users of both online services despite the fact that users' e-mail addresses and names had been removed from the accounts. *Id.* It is not only hackers and identity thieves who possess this ability to post information that appears to come from the user. Indeed, some social-networking sites, such as Twitter, permit developers to create protocols "that [allow] users to approve application[s] to act on their behalf without sharing their password." *OAuth FAQ*, TWITTER, http://dev.twitter.com/pages/oauth_faq (last visited Sept. 18, 2011). Therefore, a user could grant an application access to his Twitter account, and the application can then post "tweets" directly to that account without the user's knowledge.

[48] *See Facebook ID Theft Targets "Friends,"* RED TAPE CHRON. (Jan. 30, 2009, 10:00 AM), http://redtape.msnbc.com/2009/01/post-1.html [hereinafter *Facebook ID Theft*]. Traditionally, the "Nigerian scam" involves a wrongdoer sending out e-mails with the hope of beguiling people into sending money. FIGHT IDENTITY THEFT, *Nigerian 419 Email Scam* (May 29, 2008), http://www.fightidentitytheft.com/internet_scam_nigerian.html. Here, the sender claims to have a large sum of money that he wants to transfer out of Nigeria, but needs money up-front to cover the transfer fees. The sender offers a third of the money as a reward for the receiver's generosity. *Id.*

sites, these thieves have started to impersonate social-networking site users and contact their network friends with plausible stories of being in trouble.[49] For instance, someone hacked into the Facebook account of a Microsoft employee, Bryan Rutberg, and posted his status to read: "BRYAN IS IN URGENT NEED OF HELP!!!"[50] The hacker then sent messages to Rutberg's friends and claimed that Rutberg "had been robbed at gunpoint while traveling in the United Kingdom and needed money to get home."[51] The messages provided money-transfer information for a Western Union in London.[52] In addition, the hacker changed Rutberg's login information so that Rutberg could not access his own account.[53] The hacker also "unfriended"[54] Rutberg's wife so that Rutberg could not use her account to notify his friends that he was not in any actual trouble and that a hacker had accessed his account.[55]

Between the growth in popularity of social-networking sites and the rising number of fake accounts and incidents of hacking, there is a clear need for vigilance to protect vulnerable personal information from exploitation. More importantly, however, this growth also signals that information from social-networking sites will begin to play a central role in both civil and criminal litigation.

II. SOCIAL-NETWORKING POSTINGS IN LITIGATION

The information posted on social-networking sites carries serious legal dangers, whether the poster is a general user, a creator of a fake account, a hacker, or an identify thief. As the use of social-networking increases in scope, the

---

[49] *See* Richmond, *supra* note 43 (commenting that because social-networking sites are often used to connect with people that users know, users are "more likely to believe a fraudulent message or click on a dubious link on a friend's wall."); *Facebook ID Theft*, *supra* note 48 (reasoning that the imploring message of a friend in trouble appearing next to the picture of that friend that appears on his or her social-networking account makes the story more convincing).

[50] *Facebook ID Theft*, *supra* note 48.

[51] *Id.* (indicating that Rutberg was inundated with phone calls from concerned friends shortly after the hacker changed Rutberg's status and sent messages).

[52] *See id.* (reporting that one generous friend was swindled out of $1200 when he sent money to the Western Union office indicated in the hacked message).

[53] *Id.*

[54] Social-networking users can "unfriend" others with whom they are friends. FACEBOOK HELP CTR., *Removing Friends*, http://www.facebook.com/help/?page=770 (last visited Sept. 18, 2011). This action removes both users from each other's friends list. *Id.*

[55] *Facebook ID Theft*, *supra* note 48. To make matters worse, it took Rutberg almost a full day to alert Facebook to the problem, as users cannot contact Facebook via phone, and Facebook did not respond to Rutberg's attempts to contact the company through its form complaint procedures. *Id.* Rutberg is not alone in falling victim to hackers. Other scammers have hacked into Facebook profiles and "chatted" to online friends of the hacked account, telling similar stories of being in trouble and in need of cash. *See, e.g.*, Peter Mychalcewycz, *Nigerian 419 Scammer Busted on Facebook Chat*, SWITCHED (Jan. 26, 2009, 6:03 PM), http://www.switched.com/2009/01/26/nigerian-419-scammer-busted-on-facebook-chat (revealing the transcript of one potential victim's chat over Facebook with a would-be Nigerian scammer who posed as a high-school friend of the potential victim).

information placed in the public sphere is playing an essential role in investigations and litigation. This information can establish direct links between individuals and criminal activity, providing a gold mine of personal details, messages, and photographs that litigators can use as evidence.[56] Often unbeknownst to the social-networking user, postings leave a permanent trail that law-enforcement agents and lawyers frequently rely upon in crime solving[57] and trial strategy.[58]

Attorneys and law enforcement agents often use social-networking postings and photographs to prove a suspect's direct involvement in a crime.[59] In some cases, people confess to crimes via postings made on their social-networking pages. For example, officers arrested eighteen-year-old Zakaria Wayso after he posted a status on his Facebook page confessing that he had shot his friend.[60] Wayso was arrested despite clarifying in the posting that the shooting was an accident and apologizing to the victim.[61] In other cases, people have accessed social-networking sites while in the process of committing a crime, easing the burden on law-enforcement officers.[62] While burglarizing a home, for instance, Jonathan G. Parker checked his Facebook account and forgot to log out; this led the police to him after the victim returned

---

[56] *See* Ronald J. Levine & Susan L. Swatski-Lebson, *Are Social Networking Sites Discoverable?*, LAW.COM (Nov. 13, 2008), http://www.law.com/jsp/article.jsp?id=1202425974937 ("Although these sites provide users with a sense of intimacy and community, they also create a potentially permanent record of personal information that becomes a virtual information bonanza about a litigant's private life and state of mind.").

[57] Daniel Sieberg, *Social Networking Sites Help Combat Crime*, CBSNEWS.COM, Mar. 13, 2009, http://www.cbsnews.com/stories/2009/03/13/eveningnews/main4864837.shtml (reporting that both MySpace and Facebook assist in criminal investigations by "maintaining a 24-hour law enforcement hotline, issuing manuals and request forms for police departments, and even training officers on how to better use their sites").

[58] *See, e.g.*, Aswumb, *supra* note 21, at 23 (describing how attorneys researched jurors on social-networking sites and then tailored their opening and closing arguments based on information found on jurors' profiles, such as lines from a juror's favorite book); *see also* Jeff John Roberts, *A New U.S. Law-Enforcement Tool: Facebook Searches*, REUTERS July 12, 2011, *available at* http://www.reuters.com/article/2011/07/12/us-facebook-idUSTRE76B49420110712 (reporting that the number of warrants authorized to search personal Facebook accounts for evidence in litigation has increased twofold since 2010 and that warrants have been requested by several government agencies, including the FBI).

[59] *See, e.g.*, Wilson, *supra* note 20, at 1225 (discussing a situation in Utah in which the Attorney General "filed sexual-exploitation charges against a twenty-seven-year-old man after law-enforcement authorities found on his MySpace profile photos of the man and two boys with whom he was not supposed to be in contact"); *cf.* Rafael A. Olmeda & Sofia Santana, *Police: Texts from Dead Woman's Phone Spurred Boyfriend to Lead Cops to Her Mutilated Body*, SUN SENTINEL, Apr. 16, 2010, http://www.sun-sentinel.com/news/broward/miramar/fl-miramar-murder-arrest-20100415,0,185168.story?4-16 (reporting that police caught a homicide suspect after using text messages to track the suspect and trick him into leading police to the victim's body). Police officers are also susceptible to having their social-networking postings used against them. *See* Erica Goode, *Police Lesson: Social Network Tools Have Two Edges*, N.Y. TIMES, Apr. 6, 2011, at A1, *available at* http://www.nytimes.com/2011/04/07/us/07police.html?_r=1 (reporting that, after a police officer who had listed his occupation as "human waste disposal" on Facebook and was later involved in a fatal off-duty shooting, the city was forced to adopt a new policy regarding law-enforcement officers' use of social-networking sites).

[60] Vince Tuss, *18-Year-Old Uses Facebook to Admit He Shot Companion*, STAR TRIB. (Minneapolis), Dec. 19, 2009, http://www.startribune.com/local/minneapolis/79692697.html.

[61] *See id.*

[62] *See* Marshall, *supra* note 2.

home and noticed Parker's Facebook page open on her laptop.[63] Also, those accused of criminal involvement at times have attempted to establish alibis using postings made on social-networking sites.[64] Despite suspicion over their true authors, these postings provide strong investigatory leads for law-enforcement officials, exculpatory evidence for the wrongfully accused, and persuasive evidence on which trial attorneys often rely.

Because social-networking evidence significantly influences how the judge and jury view a witness or a party to the litigation,[65] attorneys are learning to check social-networking sites routinely for messages and photographs that could work against their clients' interests.[66] As one lawyer stated:

> There is nothing worse than at sentencing to be confronted with your client's MySpace page, complete with statements showing a lack of remorse, inappropriate content or provocative pictures. Or, having a client who feels compelled to use the Web to announce to the world about the stash of drugs that the police didn't find when they searched his home.[67]

This information can bolster or destroy witnesses' or parties' credibility. In particular, tagged photographs[68] can easily cast a witness in an unflattering light; a quick glance through users' profiles could reveal photographs of them pole-dancing at a social event[69] or exhibiting their favorite tequila brand just days after a drunk-driving accident.[70] Joshua Lipton, a twenty-year-old college student who seriously injured a twenty-one-year-old woman while driving drunk, experienced the damage

---

[63] *See id.*

[64] *See, e.g.*, Vanessa Juarez, *Facebook Status Update Provides Alibi*, CNNJUSTICE (Nov. 13, 2009, 10:25 AM), http://www.cnn.com/2009/CRIME/11/12/facebook.alibi/index.html?iref=allsearch. One minute after Rodney Bradford updated his Facebook status with an inside joke directed at his pregnant girlfriend, two men were mugged at gunpoint across town. *Id.* When Bradford became a suspect, police placed him in a lineup and one of the victims positively identified him. *Id.* Bradford's Facebook status update was later used to persuade the district attorney not to press charges. *Id.*

[65] *See* Laurie Mason, *Defense Attorneys Trolling the Net, Too*, BUCKS CTY. COURIER TIMES, Aug. 23, 2008, http://www.highbeam.com/doc/1P3-1549445091.html ("A Halloween party photo of a suspect hoisting a bottle of tequila while awaiting trial for a fatal drunk driving crash speaks volumes to a sentencing judge. And jurors are not likely to find reasonable doubt when a defendant blogs about his large drug stash.").

[66] *See, e.g.*, Findlay, *supra* note 20, at 176-80 (offering examples of social-networking evidence being used against drunk driving defendants).

[67] Mason, *supra* note 65.

[68] *See* Help Center, *supra* note 25 (defining "tagging").

[69] Nate Anderson, *Google + Facebook + Alcohol = Trouble*, ARS TECHNICA (Jan. 19, 2006, 5:37 PM), http://arstechnica.com/old/content/2006/01/6016.ars.

[70] *See, e.g.*, *Face(book)ing the Music* (July 19, 2008, 12:32 AM), http://www.alexbitterman.com/site/2008/07/338/ (posting an article in which an attorney stated that he was "blindsided" by photographs of his client at trial holding a beer bottle, wearing a shirt representing a tequila brand, and a belt complete with plastic shot glasses on it).

that Facebook photographs can do to one's credibility.[71] Two weeks after the accident, Lipton attended a Halloween party dressed as a prisoner carrying a sign that read "Jail Bird" and allowed fellow party-goers to take and post photographs of him—clad in his offensive outfit—on Facebook.[72] At trial, the prosecutor compiled a PowerPoint presentation of these distasteful photographs accessible from Lipton's Facebook page.[73] The culmination of the prosecution's presentation was a photograph of Lipton in his "Jail Bird" costume, smiling with his tongue out and "his arm draped around a young woman wearing a sorority t-shirt," to which the prosecutor added his own rhetorical caption: "Remorseful?"[74] The judge was candid about the influence that the photographs had on his sentencing decision, stating: "Without question, the most disturbing and troubling photo is the one where the defendant is dressed up in a prison inmate costume for a Halloween party shortly after this horrific incident."[75] After describing the photographs as "sick, depraved, and disgusting,"[76] the judge added that the photographs gave new meaning to the old adage that "one picture is worth a thousand words."[77] Lipton received a two-year sentence in state prison.[78]

III. AUTHENTICATION OF SOCIAL-NETWORKING EVIDENCE

As social-networking sites play an increasingly important role in investigations and trial strategy, information from these sites becomes useful evidence for litigants.[79] Social-networking evidence assists litigants in their ultimate goal—to persuade the finder of fact that they have met their burdens of proof.[80] As with any evidence, litigants must overcome a number of evidentiary hurdles before a judge will admit social-networking postings into evidence. Lawyers and judges must figure out ways to deal with these admissibility questions, ensuring that the basic standards for reliability are met. The ease with which social-networking evidence can be altered, forged, or posted by someone other than

[71] Edward Fitzpatrick, *Facebook Photo Plays Role in DUI Accident Sentencing*, PROJO.COM (May 27, 2008, 6:55 PM), http://newsblog.projo.com/2008/05/facebook-photo.html.
[72] *Id.*
[73] *Face(book)ing the Music*, *supra* note 70 (explaining that one of the crash victims provided the prosecutor with photos accessible from Lipton's page).
[74] *Id.*; Fitzpatrick, *supra* note 71.
[75] Fitzpatrick, *supra* note 71.
[76] *Id.* (quoting the judge's statement about the photograph: "For this defendant to think of mocking and joking about his irresponsible, reckless and life-altering dangerous behavior—on Facebook, for others to see, dressed in a 'Jail Bird' prison costume for a Halloween party a mere two weeks after this incident—is sick, depraved and disgusting.").
[77] *Id.*
[78] *Id.*
[79] *See generally infra* Part II.
[80] *See generally infra* Part II.

the owner of the account should raise substantial admissibility concerns.[81] Thus, the authentication of social-networking evidence is the critical first step to ensuring that the admitted evidence is trustworthy and, ultimately, that litigants receive a fair and just trial.

Authentication requirements serve as "a threshold preliminary standard to test the reliability of evidence."[82] To authenticate evidence properly, the proponent must demonstrate that there is sufficient evidence "to support a finding that the matter in question is what its proponent claims."[83] For a textual posting, this requires linking the words of the posting to the purported author.[84] The Federal Rules of Evidence, and most state rules of evidence, provide a non-exhaustive list of ways in which a proponent may authenticate a piece of evidence.[85] Under Federal Rule of Evidence 901(b)(4), a piece of evidence may be authenticated by establishing its "distinctive characteristics."[86] According to the rule, distinctive characteristics including appearance, content, substance, and internal patterns are considered in conjunction with the particular circumstances.[87]

Traditional forms of electronic evidence, like e-mails, are frequently authenticated using the distinctive-characteristics approach under Rule 901(b)(4).[88] Social-networking evidence is different from other types of electronic evidence, however, because its characteristics and content often reveal nothing useful about the author.[89] With postings coming from fake accounts, or even accounts created

---

[81] *See, e.g.*, People v. Fielding, No. C-062022, 2010 WL 2473344, at *4–5 (Cal. Ct. App. June 18, 2010) (defendant arguing that the court should consider potential tampering with social-networking evidence).

[82] Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 544 (D. Md. 2007).

[83] FED. R. EVID. 901(a).

[84] Byron L. Warnken, *Social Networking Sites and Criminal Litigation*, PROF. BYRON L. WARNKEN'S BLOG (Jan. 3, 2011), http://professorwarnken.com/2011/01/03/social-networking-sites-and-criminal-litigation (arguing that authentication requires a showing that "the person to whom any words are attributable is actually that person and not another person").

[85] FED. R. EVID. 901(b); *see, e.g.*, Washington v. State, 961 A.2d 1110, 1115 (Md. 2008) (noting that the Maryland rule for authentication is identical to the federal rule); State v. Troutman, 327 S.W.3d 717, 722 (Tenn. Crim. App. 2008) (acknowledging that the Tennessee Rule of Evidence 901(a) is "virtually identical" to the Federal Rule of Evidence 901(a)); *see also Lorraine*, 241 F.R.D. at 544-49 (describing extensively the methods of authentication outlined in Rule 901(b) and providing examples of their use in federal cases).

[86] FED. R. EVID. 901(b)(4).

[87] *Id.*

[88] *Id.*; *see, e.g.*, United States v. Safavian, 435 F. Supp. 2d 36, 40 (D.D.C. 2006) (finding that e-mails were properly authenticated because they contained distinctive characteristics, such as the "@" symbol, as well as the names of the senders and recipients of the e-mails in their signature blocks). The *Safavian* court also permitted authentication of certain e-mails by comparison to other evidence. *Id.* at 40-41. Here, certain e-mails reflected the address "MerrittDC@aol.com," which alone was not sufficient to authenticate them. *Id.* The court, however, compared these e-mails to others that contained the "defendant's name and the name of his business, Janus-Merritt Strategies, LLC," in order to authenticate them. *Id.*

[89] Some might argue that social-networking posts are similar to chat-room messages because they are often "created by parties using anonymity-protecting 'screen names' on websites where the host cannot be assumed to know the content." Hon. Paul. W. Grimm et al., *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, 371 (2009). This

under nicknames, it is difficult to link a specific person to a specific posting. Thus, social-networking postings are comparable to postings on websites, where there is a real risk that individuals "other than the sponsor of the website" created the postings.[90] Accordingly, the proponent of evidence from a website might be required to demonstrate that the host was responsible for the content of the website because the host either created or authorized the content.[91]

Unlike with the other types of electronic evidence, few courts have wrestled specifically with authentication issues presented by evidence from social-networking sites. And, while courts that address the issue generally work within the existing framework of Federal Rule of Evidence 901(b)(4), or its state equivalent, the rulings vary widely. Rather than evaluate social-networking evidence on its own, some courts compare it to other forms of electronic evidence and find no substantive distinction.[92] Other courts seem to dismiss reliability concerns and admit the postings.[93] Still other courts find that, given the low bar for admissibility under the authentication rule, any reliability concerns go only to the weight of the evidence and not to its admissibility.[94] Much of the case law concerning the application of the federal rules for authentication comes from state courts that adopt the federal rules as their local law.[95] Part IV surveys these judicial approaches and discusses their shortcomings.

---

superficial similarity, however, is negated by the fact that many social-networking postings are made to an account owner's profile on a public "wall," which may be viewable by all friends of that account owner. Depending on the account owner's privacy settings, the wall may be viewable by *all* users of that social-networking site, which may be thousands or even millions of people.

[90] *Lorraine*, 241 F.R.D. at 555.

[91] *See* United States v. Jackson, 208 F.3d 633, 638 (7th Cir. 2000) (finding that website postings depicting white-supremacy groups taking credit for racist UPS mailings were properly excluded because the defendant failed to authenticate them). The defendant in *Jackson* "needed to show that the web postings . . . actually were posted by the groups, as opposed to being slipped onto the groups' web sites by [the defendant] herself." *Id.* Other courts have also found that URL addresses and date stamps are insufficient to authenticate web content, but that testimony from a witness with personal knowledge of the actual site could be sufficient. *See* Grimm, *supra* note 89, at 369 (surveying cases that have addressed the authentication of Internet websites).

[92] *See, e.g.*, Griffin v. State, 995 A.2d 791, 806 (Md. Ct. Spec. App. 2010) ("We see no reason why social media profiles may not be circumstantially authenticated in the same manner as other forms of electronic communication—by their content and context."), *rev'd and remanded*, No. 74, 2011 WL 1586683 (Md. Apr. 28, 2011).

[93] *See, e.g.*, People v. Goins, No. 289039, 2010 WL 199602, at *2 (Mich. App. Jan. 21, 2010) (finding that the content of an entry written on the complainant's MySpace page was properly authenticated by its descriptive content and that the defendant's concerns about the authorship of the posting were dismissed by the "unlikelihood" that the complainant gave her password to a third party).

[94] State v. Bell, 882 N.E.2d 502, 512 (Ohio Ct. Com. Pl. 2008); STEVEN GOODE & OLIN G. WELLBORN, COURTROOM HANDBOOK ON FEDERAL EVIDENCE 552 (2010) (stating that questions related to the genuineness of the evidence go to weight, not admissibility).

[95] *See supra* note 85 and accompanying text.

IV. CRITIQUE OF JUDICIAL APPROACHES TO AUTHENTICATION OF SOCIAL-NETWORKING EVIDENCE

Despite the demonstrated unreliability of information on social-networking sites, the current judicial approaches to authentication of such evidence have failed to require rigorous showings of authenticity.[96] The practical effect of this failure is that judges and juries have factored into their decisions potentially untrustworthy, even fallacious, pieces of evidence. Courts' lack of accurate and careful attention to the authenticity—and consequently, to the authorship—of social-networking postings can be categorized into four general, yet problematic, approaches. In the first approach, the court effectively shirks its gate-keeping function, deflecting all reliability concerns associated with social-networking evidence to the finder of fact. Under the second approach, the court authenticates a social-networking posting by relying solely on testimony of the recipient. The third approach requires testimony about who, aside from the owner, can access the social-networking account in question. With the fourth approach, the court focuses on establishing the author of a specific posting.

A. Punting Reliability Concerns to the Fact-Finder

In the first approach to authentication of social-networking evidence, the court fails to perform its essential gate-keeping function by ignoring the reliability concerns unique to this type of evidence at the authentication stage and by permitting all such concerns to go only to the weight of the evidence. In this situation, the fact-finder is left to interpret the reliability of the social-networking evidence without evidence of its authenticity. Leaving the fact-finder, often a jury, to consider potentially untrustworthy evidence is precisely what the court's role as gatekeeper is designed to prevent.[97]

People v. Fielding provides a good example of this faulty approach.[98] In *Fielding*, the California Court of Appeal found that MySpace messages were properly authenticated by the trial court and that any questions about authorship

[96] Judges may require rigorous showings of authenticity, and they should do so when it is possible that evidence could be altered, fabricated, or unreliable. *See* GEORGE L. PAUL, FOUNDATIONS OF DIGITAL EVIDENCE 43 (2008) (commenting on courts' ability to require a "more robust" showing to authenticate electronic evidence and comparing electronic evidence to other technologies in which courts have applied a more stringent standard of authentication, such as with tape recordings); 5 STEPHEN A. SALTZBURG ET AL., FEDERAL RULES OF EVIDENCE MANUAL § 901.02[2]-[3] (8th ed. 2002) (asserting that certain circumstances may justify a stronger showing to authenticate evidence than the prima facie standard that is typically required).

[97] *See* PAUL, *supra* note 96, at 43.

[98] *See generally* People v. Fielding, No. C-062022, 2010 WL 2473344 (Cal. Ct. App. June 18, 2010).

went only to weight, not admissibility.[99] The defendant faced charges of unlawful sexual intercourse with a minor, and the prosecution introduced printouts of MySpace messages sent between the defendant and the victim to prove its case.[100] The messages contained evidence of the alleged criminal conduct, including the following statements from the defendant: "[O]k so you only say [you] love me cuz you wanna fuck me?" and "I want to have sex."[101]

The defendant appealed her conviction, claiming in part that the MySpace messages had been improperly authenticated.[102] The defendant's primary arguments were: (1) that the alleged victim's father printed the messages from the victim's account and could have changed them; and (2) that the alleged victim testified that someone had previously hacked into his MySpace account, and, therefore, the messages may have been altered.[103] Despite these seemingly strong arguments justifying, at a minimum, an inquiry into the authenticity of the messages, the court found that the supposed alterations were "immaterial" and did not preclude authentication.[104] Instead, the court likened the messages to e-mails and relied on the reply doctrine[105] as well as the content of the messages to find in favor of authentication.[106] Any concerns that the "incriminating messages . . . were in fact sent or posted by someone else went to the weight of the evidence, not its admissibility."[107]

The *Fielding* court completely ignored obvious authorship concerns; its holding contravenes the court's gate-keeping function in such a situation. The onus is on the court to ensure that a defendant receives a fair trial. This obligation includes an assurance that the evidence that goes to a jury is reliable.[108] The *Fielding* court did not live up to these responsibilities.

B. Relying on Recipient Testimony

The Tennessee Court of Appeals used a different approach to authenticating social-networking postings and messages. It found that a message was properly

---

[99] *Id.* at *5.
[100] *Id.* at *1.
[101] *Id.* (second alteration in original)
[102] *Id.*
[103] *Id.* at *3–4 ("On cross-examination, the victim testified that somebody once 'hacked' into his MySpace account and changed the 'mood status' he had posted from 'I'm ready to win' to 'I'm ready to be gay.'").
[104] *Id.* at *5.
[105] "If a letter or telegram is sent to a person and a reply is received in due course purporting to come from that person, this is sufficient evidence of genuineness." Jazayeri v. Mao, 94 Cal. Rptr. 3d 198, 214 (Ct. App. 2009).
[106] Fielding, 2010 WL 2473344 at *4–5.
[107] *Id.* at *5.
[108] FED. R. EVID. 104(a) ("Preliminary questions concerning . . . the admissibility of evidence shall be determined by the court."); *see also* GOODE ET AL., *supra* note 94; PAUL, *supra* note 96, at 43.

authenticated when the recipient testified under oath that the posting accurately reflected the communications she had with the defendant.[109] In *Dockery v. Dockery*, a woman had a "'no contact' order of protection" issued against her ex-husband after multiple instances of alleged domestic violence.[110] The ex-husband later attempted to contact her by sending MySpace messages to her friend.[111] In the lower court proceeding, the recipient of the MySpace messages testified that she printed the conversations "directly from her computer" and that the printouts accurately reflected their conversation while "identif[ying] which party to the conversation was making a particular statement."[112] The court found her testimony alone sufficient to authenticate the messages as authored by the defendant; that finding was upheld on appeal.[113]

By relying solely on the recipient's testimony, the court failed to address the obvious reliability concerns with the MySpace messages. The court did not address the possibilities that the documents could have been altered, that the proponent could have been lying, or that someone other than the defendant could have authored the messages. The court's failure to make these basic inquiries undermined the fairness of the ultimate outcome of the case because potentially unreliable, inculpatory evidence was admitted against the defendant.[114]

C. Requiring Testimony About Potential Outside Access to an Account

The Supreme Judicial Court of Massachusetts took a different approach from the two discussed above. In *Commonwealth v. Williams*, the court held that the printouts of postings received on a witness's MySpace page had not been properly authenticated in the defendant's murder trial.[116] One of the prosecution's witnesses claimed that the defendant's brother had been urging her, via MySpace messages, either "not to testify or to claim lack of memory."[117] The account in question contained a photo of the defendant's brother, the name on the account matched his username, and the messages contained content that only someone familiar with the

[109] Dockery v. Dockery, No. E2009-01059-COA-R3-CV, 2009 WL 3486662, at *6 (Tenn. Ct. App. Oct. 29, 2009).
[110] *Id.* at *1–2.
[111] *Id.* at *5.
[112] *Id.* at *6.
[113] *Id.*
[114] *See* PAUL, *supra* note 96, at 50 (acknowledging the authenticity problems surrounding website printouts and pushing lawyers to ask questions such as: "[W]hat do we know about the [web page] before it was printed?", "Who had access to it?", and "Was it edited?").
[116] Commonwealth v. Williams, 926 N.E.2d 1162, 1172–73 (Mass. 2010).
[117] *Id.* at 1172.

pending criminal case would know.[118] Nonetheless, the court found that this evidence was not enough to authenticate the postings.[119]

The Supreme Judicial Court wanted testimony regarding the security of the MySpace account, the people who could access that MySpace page, and whether passwords were needed for such access.[120] The court likened the MySpace page to a telephone call, stating that "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.'"[121] The court was convinced only that the account belonged to the defendant's brother and not that he actually authored the messages.[122]

Until very recently, *Williams* was the only case that remotely recognized the importance of requiring some proof of authorship before a social-networking posting can be authenticated. To support claims that a specific person authored a posting, the *Williams* decision requires at least some evidence about who had access to the account from which the social-networking evidence at issue came.[123] In particular, the court noted that foundational testimony may be able to establish that *someone* with access to a particular social-networking account sent a message or created a posting, but the court found that such testimony cannot establish that a *specific* person authored the message or posting.[124] Recognizing the authorship questions inherent in social-networking evidence, the court even criticized counsel for failing to present expert testimony to prove that the defendant's brother was the only person with access to the MySpace account from which the messages were sent.[125] Although the Massachusetts court went further than the California and Tennessee courts regarding authentication of social-networking postings, its approach remains insufficient to address the authorship concerns unique to this type of evidence.

---

[118] *Id.*
[119] *Id.* at 1172–73.
[120] *Id.*
[121] *Id.*
[122] *Id.* at 1172 ("[I]t appears that the sender of the messages was using [the defendant's brother's] MySpace Web 'page.'").
[123] *Id.* at 1173 ("There was insufficient evidence . . . there [was] no testimony . . . regarding how secure such a Web page is, who can access a My[S]pace Web page, whether codes are needed for such access, etc.").
[124] *Id.* at 1172–73 ("[W]hile the foundational testimony established that the messages were sent by someone with access to [the] MySpace Web page, it did not identify the person who actually sent the communication.").
[125] *Id.* at 1173.

D. From Establishing the Account Owner to Establishing the Author of a Specific Posting

In *Griffin v. State*, the Maryland Court of Special Appeals authenticated MySpace postings by establishing the owner of the account on which the postings had appeared.[126] After the first trial ended in a mistrial, the prosecution's key witness changed his story.[127] During the second trial of the case, he clearly identified the defendant as the killer and testified that after he saw the victim and the defendant enter a bathroom alone, he heard gunshots.[128] The witness claimed that he changed his testimony because he felt intimidated by the defendant's girlfriend, Jessica Barber, and had lied the previous time to protect himself.[129] The crucial piece of evidence to support his claim of intimidation was a printout of a posting made on the MySpace page of "SISTASOULJAH" that stated, "JUST REMEMBER SNITCHES GET STITCHES!! U KNOW WHO YOU ARE!!"[130]

The trial court wrestled with how to authenticate this type of pseudonymous posting made on a social-networking website like MySpace.[131] Its solution was to focus not on the posting at issue, but rather on the owner of the account on which the allegedly threatening posting appeared.[132] The court looked to the distinctive characteristics of the MySpace profile page to link the account to Barber.[133] These characteristics included: Barber's photograph, birth date, hometown, and the defendant's nickname, "Boozy."[134] The investigator who accessed the profile page and printed the postings testified that he recognized the profile as belonging to Barber because of these details.[135] Relying on this testimony about the account owner, the court admitted the posting in question as properly authenticated.[136]

---

[126] Griffin v. State, 995 A.2d 791 (Md. Ct. Spec. App. 2010), *rev'd and remanded*, 19 A.3d 415 (Md. 2011).
[127] *Id.* at 794–95.
[128] *See id*. ("Gibbs testified that appellant was the only person, other than Guest, in the bathroom when the shots were fired.").
[129] *See id.* at 795 (noting that Gibbs explained his inconsistent testimonies during the first and second trials by pointing to threats he received from Jessica Barber before the first trial).
[130] *Id.* at 795–96.
[131] *Id.* at 796–97 (explaining how the testimony of Sergeant John Cook, the officer who printed out the MySpace postings in question, was offered to confirm that the MySpace profile in question belonged to Barber).
[132] *Id.* ("[T]he prosecutor asserted that the profile could be authenticated as belonging to Barber through the testimony of Sergeant John Cook, the Maryland State police investigator who printed the document.").
[133] *Id.*
[134] *Id.* at 796–97, 806.
[135] *Id.* at 796, 806. Although Barber testified as a witness at trial and could have authenticated the posting or admitted ownership of the "SISTASOULJAH" account, the prosecuting attorney did not ask her a single question about this issue. *Id.* at 796, 806.
[136] *Id.* at 797. The defendant was subsequently convicted of "second-degree murder, first-degree assault, and use of a handgun in the commission in a felony or crime of violence." *Id.* at 794. His conviction was upheld by the Court of Special Appeals. *Id.* at 811.

On appeal, the Maryland Court of Special Appeals acknowledged that both the Maryland Rules of Evidence and the Maryland Rules of Procedure failed to address authentication of anonymous postings made on social-networking sites.[137] The court relied on Maryland decisions as well as decisions from other jurisdictions applying the equivalent of Federal Rule of Evidence 901(b)(4) to decide the ultimate issue: "[W]hether the State adequately established the *author* of the cyber message in question."[138] In its analysis, the court also looked for guidance from rules for the authentication of other forms of electronic evidence;[139] it saw "no reason why social media profiles may not be circumstantially authenticated in the same manner as other forms of electronic communication."[140] Despite the court's noted concerns with pseudonymous postings, it authenticated the "SNITCHES GET STITCHES" posting as authored by Barber because the content of the MySpace *account* showed that it could reasonably belong to her.[141] The court never specifically linked Barber to the particular *posting*.[142]

Although the *Griffin* court acknowledged the questionable reliability of social-networking evidence, it nevertheless erroneously concluded that authentication of the account owner sufficed to authenticate the authorship of a posting found on that account.[143] Supporters of the *Griffin* approach argue that the content on Barber's profile combined with the references to the defendant should be sufficient to advance the evidence beyond the initial authentication hurdle.[144] Like the Maryland Court of Special Appeals, however, they fail to see the bigger picture. *Social-networking profiles and individual postings can be created by anyone at any time*. Any person familiar with Barber's or the defendant's situation could have created a profile in her name, hacked into her account, or, at the very least, posted

---

[137] *Id.* at 803.
[138] *Id.* (emphasis added).
[139] *Id.* at 806 ("[W]e regard decisions as to authentication of evidence from chat rooms, instant messages, text messages, and other electronic communications from a user identified only by a screen name as instructive to the extent that they address the matter of authentication of pseudonymous electronic messages based on content and context."). Most specifically, the court looked at its previous holding in *Dickens v. State*, where it authenticated anonymous text messages as authored by the defendant under Maryland Rule of Evidence 5-901(b)(4) by looking at the content and circumstance of the messages. *Id.* at 803–04. In its discussion of *Dickens*, the *Griffin* court suggested that *Dickens* also stands for the proposition that "circumstantial evidence may be sufficient to establish authorship of an electronic message" without further "technological data." *Id.* at 804.
[140] *Id.* at 806.
[141] *Id.* at 806–07.
[142] *See id.* at 806 (noting that the posting was never authenticated by Barber or by "expert information technology evidence"); *see also* Petitioner's Brief at 11–12, Griffin v. State, 19 A.3d 415 (Md. 2011) (No. 74), 2010 WL 5096820 at *10–11 ("The State failed to authenticate the statements on the MySpace page as statements made by Barber and failed to authenticate the page itself as having been created by Barber.") (footnote omitted).
[143] *Id.* at 806.
[144] *See* Brief of Respondent/Cross-Petitioner at 8, Griffin v. State, 19 A.3d 415 (Md. 2011) (No. 74), 2010 WL 5146302 at *8 ("Given the photograph, personal information, and repeated references to freeing 'Boozy,' it would not be unreasonable for a finder of fact to believe that the MySpace page was in fact Barber's.").

to her profile page.[145] In upholding the trial court's decision, therefore, the *Griffin* court incorrectly found that the jury had an adequate basis from which to determine that Barber was the author of the "SNITCHES GET STITCHES" posting that appeared on her profile page.

On April 28, 2011, the Maryland Court of Appeals saw the bigger picture and reversed the Court of Special Appeals, taking a major step toward an authorship-centric approach to the admission of social-networking evidence.[147] Judge Battaglia, for the 5-2 majority, posed the general question in the case as follows: "[W]e are tasked with determining the appropriate way to authenticate, for evidential purposes, electronically stored information printed from a social networking website, in particular, MySpace."[148] The court summarized the process of creating a profile on MySpace, reviewed the possibilities for abuse, and held "that the pages allegedly printed from Griffin's girlfriend's (Barber) MySpace profile were not properly authenticated."[149] The court remanded the case for a new trial.[150]

The Maryland Court of Appeals was most concerned that "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."[151] The majority stated that the lower court "gave short shrift to [this hacking] concern,"[152] agreeing with appellant Griffin:

> [T]he trial judge abused his discretion in admitting the MySpace evidence . . . 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.[153]

---

[145] *See* Petitioner's Brief, *supra* note 142, at 10–12.
[147] *Griffin*, 19 A.3d at 428.
[148] *Id.* at 416–17 (footnotes omitted). Judge Battaglia stated the more specific question this way: "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." *Id.* at 419–20.
[149] *Id.* at 418, 420, 421–22.
[150] *Id.* at 428.
[151] *Id.* at 421. "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." *Id.* at 422.
[152] *Id.* at 423.
[153] *Id.* at 423–24.

In a significant move, the majority called for "a greater degree of authentication."[154] Unfortunately, however, the court did not indicate with any specificity what that greater degree might require. Instead, the court noted three possibilities that "[came] to mind"[156]: (1) "ask the purported creator if she indeed created the profile and also if she added the posting in question"; (2) "search the computer of the person who allegedly created the profile and posting and examine the computer's [I]nternet history and hard drive to determine whether that computer was used to originate the social networking profile and posting in question"; and (3) "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."[157] While the Maryland Court of Appeals recognized that "[p]ossible 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,"[158] the court could have provided considerably more direction for the trial court to follow on the remand.

V. AN AUTHORSHIP-CENTRIC APPROACH TO AUTHENTICATION

The existing approaches to authentication of social-networking evidence are inadequate, whether in kind or in degree. Courts generally have failed to compel litigants to elicit clearly relevant testimony about the processes by which social-networking evidence was obtained and have routinely dismissed concerns about the authorship of postings to social-networking websites. Specifically, they have failed to require proponents of social-networking evidence to demonstrate a nexus between the accounts on which the postings were found and their purported authors. While the *Williams* decision from the Massachusetts Supreme Judicial Court marked a step in the right direction and the *Griffin* decision from the Maryland Court of Appeals went further than any other court to date toward establishing an authorship-centric approach to authentication of social-networking evidence, there is still a great deal of room for courts to develop better law and practices in this ever-increasing area of concern in both civil and criminal litigation.

---

[154] *Id.* at 424. The dissent argued that the evidence in the case was sufficient to authenticate the printout and that, in any event, the issues concerning authentication went only to the weight of the evidence: "The technological heebie jeebies discussed in the Majority Opinion go, in my opinion, . . . not to the admissibility of the print-outs . . . , but rather to the weight to be given the evidence by the trier of fact." *Id.* at 430 (Harrell, J., dissenting) (footnote and citations omitted).

[156] *Id.* at 427.

[157] *Id.* at 428.

[158] *Id.* at 427.

This Part emphasizes what the courts have largely ignored—specific, adequate proof of who authored the posting in question. It draws upon the Federal Rules of Evidence and several states' approaches to authentication in the social-networking context and proposes authentication factors that focus on *authorship* of the evidence at issue. The proposed method is no more onerous than current authentication approaches and fits neatly within the circumstantial-evidence approach to authentication under Rule 901(b)(4).[159]

A. The Need for an Authorship-Centric Approach

Addressing authorship is critical when authenticating evidence gathered from social-networking sites.[160] Indeed, the reliability of evidence obtained from these sites turns on whether the author of the posting is, in fact, the person reflected in the evidence.[161] Establishing the *owner* of a social-networking account does not serve to establish the *author* of the posting at issue for the purpose of authentication.[162] In the social-networking context, then, proving "that the matter

---

[159] FED. R. EVID. 901(b)(4). Courts have discretion to conduct a more stringent authentication inquiry without exceeding the bounds of evidentiary rules. *See* Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 542–43 (D. Md. 2007) ("Although courts have recognized that authentication of ESI [electronically stored information] may require greater scrutiny than that required for the authentication of 'hard copy' documents, they have been quick to reject calls to abandon the existing rules of evidence when doing so.") (footnote omitted).

[160] *See Lorraine*, 241 F.R.D. at 543 ("[C]ourts increasingly are demanding that proponents of evidence obtained from electronically stored information pay more attention to the foundational requirements than has been customary for introducing evidence not produced from electronic sources."). Also, the court in *Lorraine* provided this analysis of chat-room messages, which can be analogized to postings on social-networking sites: "[T]he fact that chat room messages are posted by third parties, often using 'screen names[,]' means that it cannot be assumed that the content found in chat rooms was posted with the knowledge or authority of the website host." *Id.* at 556.

[161] *See* Petitioner's Brief, *supra* note 142, at 16–18 (discussing how the court in *Commonwealth v. Williams* found that, even though the messages in question were established to have been posted by someone with access to Williams's MySpace profile, there was not sufficient evidence to identify the person who actually posted the messages). Thus, petitioner argued that under the precedent set in *Williams*, the message in question in this case must be authenticated as coming from Barber, which was not done. *Id.* at 16–17.

[162] *Id.* at 17 (noting that a message sent from a particular person's social-networking account does not mean that the account owner actually authored that message). In a different context, a "producer of adult entertainment content" sued 1017 defendants—"identified only by Internet Protocol ('IP') address"—for violation of the plaintiff's copyrights. VPR Internationale v. Does 1-1017, No. 2:11-cv-02068-HAB-DGB, 2011 U.S. Dist. LEXIS 64656, at *1 (C.D. Ill. Apr. 29, 2011) (denying a motion to certify for interlocutory review the court's denial of a motion for expedited discovery). The court stated: "The list of IP addresses attached to VPR's complaint suggests, in at least some instances, a . . . disconnect between IP subscriber and copyright infringer. . . . The infringer might be the subscriber, someone in the subscriber's household, a visitor with her laptop, a neighbor, or someone parked on the street at any given moment." *Id.* at *4. While it is premature to make sweeping generalizations about this case, as it is still in the pretrial stages, one writer has called this ruling a potential "landmark" because the judge decided "that an IP address is not adequate evidence to pin a crime on someone." Matthew DeCarlo, *U.S. Judge: An IP address is not a person*, TECHSPOT (May 5, 2011, 3:31 PM), http://www.techspot.com/news/43664-us-judge-an-ip-address-is-not-a-person.html.

in question is what its proponent claims"[163] translates into proving that "the person to whom any words are attributable is actually that person and not another person."[164]

Consider the situation of a social-networking profile allegedly belonging to a criminal defendant. Any person who knows the circumstances surrounding the defendant's case can easily create a profile or posting allegedly belonging to the defendant that suggests the defendant's guilt. This problem arises even if the account actually belongs to the defendant. If the defendant's account is accessible to others—due to faulty password protection, carelessness by leaving the account logged on at a public computer, or allowing others to access the account[165]—the account is thus "authentic" in the sense that it belongs to the defendant. But given the lack of account security, it would be unclear whether the defendant actually authored any incriminating posting.[166] This point cuts both ways: a falsified third-party profile or posting originating from the defendant's account could also exculpate the defendant. If the evidence is ruled admissible over a hearsay objection, for example, the profile or postings would be authenticated if the reviewing court focuses only on content; this could be crucial evidence if there is no other corroboration in the case. This would also be the outcome if the court centers its inquiry on account ownership, where someone other than the defendant authored a posting from the defendant's account. However, if the court properly emphasizes authorship in its authentication analysis, these false profiles and postings would be excluded before reaching the jury.[167]

B. Essential Factors for Courts to Consider When Authenticating Social-Networking Evidence

Given the importance of keeping from the jury evidence that is likely falsified or authored by someone else, what is the best approach for courts to follow when

---

[163] FED. R. EVID. 901(a).
[164] Warnken, *supra* note 84.
[165] *See OAuth FAQ*, *supra* note 47 and accompanying text (noting that users of some applications may unwittingly grant access to post to or send messages from their account).
[166] The court in *Williams* considered this very real possibility, ultimately ruling that the evidence gathered from MySpace should have been excluded. Commonwealth v. Williams, 926 N.E.2d 1162, 1173 (Mass. 2010) ("An additional reason for excluding these messages is that they could have been viewed by the jury as evidence . . . of guilt. There was no basis for the jury to conclude that the statements were generated, adopted, or ratified by the defendant or, indeed, that they had any connection to him. Thus, the messages are irrelevant to consciousness of guilt and their admission was prejudicial to the defendant.").
[167] *See* Petitioner's Brief, *supra* note 142, at 14 ("[E]vidence of authorship is vital since anyone can create a MySpace page and put any content on it that they choose, and people frequently gain unauthorized access to other people's profiles and make postings purporting to be from the profile's creator.").

authenticating evidence from a social-networking site? The answer lies in the rules themselves. When applying Federal Rule of Evidence 901(b)(4), or an equivalent state rule, courts should adopt an authorship-centric approach that instructs courts to ask the appropriate questions when considering evidence from social-networking websites. This approach concentrates the courts' attention on the unique issues presented by this type of evidence, aligning the judicial process with the novel legal issues presented by modern technology.

Refocusing the authentication inquiry on authorship will not require the courts to engage in a more exhaustive inquiry than is already required for other types of evidence. But the factors outlined below—which fit within the 901(b)(4) circumstantial-evidence authentication framework—get to the heart of the proper authentication questions in the social-networking context and build a solid foundation upon which the court can decide whether to authenticate the evidence at issue. The factors fall into three categories: account security, account ownership, and the posting in question. Although no one factor in these categories is dispositive, addressing each will help to ensure that admitted evidence possesses more than a tenuous link to its purported author.

1. Account Security

This category focuses on the security of the social-networking account in question, integrating the Massachusetts approach discussed above.[168] Because security levels of social-networking websites and specific personal profile settings vary, courts should evaluate the security of the particular account from which a posting was made. The inquiry should include at least the following questions:

- Does the social-networking site allow users to restrict access to their profiles or certain portions of their profiles?[169]
- Is the account that was used to post the proffered evidence password-protected?[170]

[168] *See* discussion *supra* Part IV.C.

[169] This factor is similar to—but less demanding than—the petitioner's argument in *Griffin* that the court needs foundational testimony regarding the operation of the social-networking site in question. *See* Petitioner's Brief, *supra* note 142, at 20 ("This lack of any evidence regarding MySpace privacy, security, operation, or use in general or specifically with regard to the profile in question renders the posting *worthless* as evidence and demonstrates that the State failed to meet its burden to prove that the exhibit was what the State claimed it was.") (emphasis added). The factors in this section by no means require the proponent to prove that the evidence is what it purports to be; rather, the factors seek to obtain foundational testimony from different questions to allow the court to decide whether to admit the evidence under the same authentication standard.

- Does anyone other than the account owner have access to the account?[171]
- Has the account been hacked into in the past?
- Is the account generally accessed from a personal or a public computer?
- How was the account accessed at the time the posting was made?

2. Account Ownership

Questions that elicit information about the alleged account owner may be helpful to the court at the authentication stage in various ways. Not only do these questions assist the court in determining who owns the account in question, but they also help to assess the likelihood that the posting at issue was actually authored by the account owner. These questions integrate the approach taken by the Maryland Court of Appeals in *Griffin v. State*.[172] Unlike the *Griffin* approach, however, these questions alone are not sufficient to authenticate a posting from a particular account. A court should address, at a minimum, the following key questions:

- Who is the person attached to the account that was used to post the proffered evidence?[173]
- Is the e-mail address attached to the account one that is normally used by the person?
- Is the alleged author a frequent user of the social-networking site in question?

Answering these questions should not tax the resources of the court. If account ownership is in dispute or is unknown from testimony, the proponent of the posting can subpoena the social-networking site to obtain the name and e-mail address used to create the account, offer expert testimony from a qualified individual with knowledge of the way the particular website functions, or seize the computer on which the postings were allegedly made to examine the hard drive to determine whether the postings actually originated from that computer.[174]

---

[170] The petitioner in *Griffin* argued that the "limited" testimony of the investigator used to authenticate the posting and profile failed to meet the authentication bar, in large part because the investigator was not asked about the security of the account—namely, whether the account requires a password to access the profile. *Id.* at 37–38.
[171] *See* discussion *supra* note 47.
[172] *See* discussion *supra* Part IV.D.
[173] According to the petitioner in *Griffin*, this does not necessarily require expert testimony. Petitioner's Brief, *supra* note 142, at 35–36.
[174] *Id.* at 35–36, 38.

3. Posting in Question

The following questions seek foundational testimony about the particular type of evidence obtained from a social-networking website. As the petitioner in *Griffin* argued, "[s]ome evidence regarding the way in which material is placed on the profile at issue is necessary since sites differ considerably with respect to how information is posted, how it can be accessed and altered, and whether any privacy settings protect the members' content."[175] Here, the court should ask at least these questions:

- How was the evidence at issue placed on the social-networking site?
- Did the posting at issue come from a public or a private area of the social-networking website?[176]
- How was the evidence at issue obtained from the website?

The questions in these categories, weighed together, will allow the court to make an authentication decision based on the authorship concerns inherent in social-networking evidence. Courts that apply this authorship-centric approach will fulfill their gate-keeping function and ensure that finders of fact will not have to wrestle with the foundational reliability concerns that should normally be addressed at the authentication stage.

C. Authorship Factors Are a Condition of Admissibility and Should Not Go to Weight

For any document that is ultimately admitted into evidence, it is the fact-finder's role to determine the weight and credibility to assign to that evidence. Some argue that the issues of authorship of social-networking evidence—the "technological heebie jeebies"[177]—should be considered only at this stage of the proceedings rather than in the authentication inquiry. This argument is misguided.

---

[175] *Id.* at 33–34.

[176] The petitioner in *Griffin* argued for a distinction between postings or photographs on profiles and private messages between specified individuals, noting that the "content of the profile at issue [in that case] . . . was not a communication between specified individuals, but rather was posted on the Internet for anyone to see as evidenced by the fact that [the lead investigator] was able to access it." *Id.* at 21.

[177] *See* Griffin v. State, 19 A.3d 415, 424, 430 (Md. 2011) (Harrell, J., dissenting); *see also* discussion *supra* note 154.

Although the question of authentication is indeed "a narrow legal one,"[178] this threshold burden must still be met before a judge can allow the evidence to reach the jury.[179] Addressing these concerns using the factors presented above does not require a higher burden for authentication.[180] Weighing the factors merely requires different foundational testimony to meet the same well-established authentication bar—that a reasonable fact-finder could find the evidence to be what the proponent claims.[181]

The court must address critical authorship concerns at the authentication stage, because there are two significant possible consequences of a wrongly focused authentication inquiry. First, if the court does not consider these issues during the authentication stage, the court will be unable to give the fact-finder a proper foundation upon which to evaluate the reliability and credibility of the evidence. Weighing the authorship factors under Rule 901(b)(4) remedies this problem. If the document is authenticated after weighing the foregoing factors, the court can direct the finder of fact to focus on any authorship disputes or other issues that were insufficient to bar the evidence from admissibility. These issues will *then* go to the weight of the evidence.[182]

Second, if the document is admitted under one of the current approaches and is so inherently unreliable that it would have been excluded under an authorship-centric authentication process, the fact-finder will then consider evidence that may seriously prejudice the party against whom the evidence is offered. The fact that the authentication bar is a low one is of no consequence; the bar must still be met as a matter of law.

CONCLUSION

Courts should not view the authentication of evidence obtained from social-networking websites in a one-size-fits-all framework,[183] especially in light of the

---

[178] Brief of Respondent/Cross-Petitioner, *supra* note 144, at 4.

[179] Petitioner's Brief, *supra* note 142, at 12 (citing MD. CODE ANN., Evid. § 5-901(a) (West 2011)).

[180] *See* Petitioner/Cross-Respondent's Reply Brief at 2, Griffin v. State, 19 A.3d 415 (Md. 2011) (No. 74), 2010 WL 5146302 at *2 ("While the State claims that this standard would require 'definitive proof of authorship,' it does not pose an onerous burden and may easily be met with circumstantial evidence.").

[181] Brief of Respondent/Cross-Petitioner, *supra* note 144, at 5–6.

[182] *See* Petitioner/Cross-Respondent's Reply Brief, *supra* note 180, at 2 ("Because of the unique authentication concerns implicated by the anonymous nature of the Internet, the proponent of evidence obtained from a social networking website must provide some evidence that links the posting to the purported author separate and apart from the posting itself."); *see also* GOODE ET AL., *supra* note 94.

[183] *See* Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 553–54 (D. Md. 2007) (recognizing 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," but arguing that "[i]t is possible . . . to identify certain authentication issues that have been noted by courts and commentators

flexible approach to authentication inherent in the Federal Rules of Evidence and its state counterparts. The issues of anonymity and authorship presented by social-networking websites differ from the authentication issues raised by more traditional evidence. Authentication must be more finely tailored to resolve the ultimate issues at stake in the social-networking context.

As courts grapple with the novel evidentiary questions presented by social-networking websites, new technologies are being developed and unique legal issues are certain to accompany them. The authentication factors outlined in this Article, however, constitute a good starting point. The authorship-centric approach properly shifts a court's attention from content and account ownership to authorship, keeping pace with the most serious problems presented by technologies that make communicating across the globe just as easy as concealing one's identity on the Internet. The goal of this approach is not to protect people from their own stupidity in posting embarrassing or incriminating information online. Rather, it is to underscore the importance of fairness and accuracy in the outcome of judicial proceedings that involve social-networking evidence.

---

with particular types of electronic evidence and to be forearmed with this knowledge to develop authenticating facts that address these concerns").