Mississippi College Law Review

Volume 31
Issue 2 *Vol. 31 Iss. 2*

Article 2

2013

Friends, Gangbangers, Custody Disputants, Lend me your Passwords

Aviva Orestein

Custom Citation
31 Miss. C. L. Rev. 185 (2012-2013)

FRIENDS, GANGBANGERS, CUSTODY DISPUTANTS, LEND ME YOUR PASSWORDS

*Aviva Orenstein**

* Professor of Law, Indiana University School of Law Bloomington. I would like to thank Alexandra Block, Jason Howard, and Heather Shreve for outstanding research assistance. I dedicate this Article to my son, Michael M. Greenberg, who allows me to friend him on Facebook.

I. INTRODUCTION

Whenever parties seek to introduce out-of-court statements, evidentiary issues of hearsay and authentication will arise. As methods of communication expand, the Federal Rules of Evidence must necessarily keep pace. The Rules remain essentially the same, but their application varies with new modes of communication. Evidence law has been very adaptable in some ways and notoriously conservative, even stodgy, in others. Although statements on Facebook and other social media raise some interesting questions concerning the hearsay rule and its exceptions, there has been little concern about applying the hearsay doctrine to such forms of communication. By contrast, such new media have triggered what could be characterized as a judicial "freak-out" concerning how to authenticate statements made via social media.

Part II of this Article defines and explains the function of social media, and Part III discusses where evidence from social media currently appears in modern trials. (The short answer is: everywhere.)

Part IV discusses hearsay questions raised by statements on Facebook and Twitter, arguing that, with some small exceptions, the Rules are perfectly well-suited to deal with such new media and that courts face few problems in doing so.

Part V documents the divergent approaches courts have taken to authenticating evidence from social media. Although some argue that the capacity for false authorship and fraud is so great that new rules are necessary, the majority of scholars and practitioners believe that the current rules of authentication are adequate, though there is much disagreement about their application. After setting out the evidence standard for authentication and the various approaches of recent cases, Part V criticizes the overly cautious and restrictive approach of some courts.

Part VI advocates for the more open approach to authenticating social media adopted by some courts. It goes further, arguing for a rebuttable presumption of authenticity barring credible evidence of appropriation or hacking. As with other types of technology when first introduced—photographs, telephone calls, x-rays—an inevitable transition period exists as

courts gradually become familiar with the new mode of transmitting information and less fearful of undetectable fraud. In the meantime, it is satisfying to reflect how the Federal Rules of Evidence, properly applied, continue to be an excellent source for accommodating new and sometimes challenging forms of out-of-court communication.

II. WHAT IS SOCIAL MEDIA?

Hundreds of millions of people worldwide use social media. Wikipedia, which itself is a form of social media, describes social media as follows: "Social media includes web-based and mobile technologies used to turn communication into interactive dialogue."[1] Of particular interest in evidence law are social networking sites that provide online platforms for people to interact.[2] Users adopt a screen name and establish an online identity, forming links with friends they know in the real world or strangers who share similar interests.[3] Users can create and edit written content, post photographs, join groups, post on the pages of friends, and engage in one-on-one electronic conversations,[4] all in real-time with a timestamp. The content can be original or can be replicated from other sources.[5]

---

1. *Social Media*, WIKIPEDIA, http://en.wikipedia.org/wiki/Social_media (last visited June 24, 2012). *See* JOHN G. BROWNING, THE LAWYER'S GUIDE TO SOCIAL NETWORKING: UNDERSTANDING SOCIAL MEDIA'S IMPACT ON THE LAW 17 (2010) ("'Social media,' also known as 'social networking,' is the term used to describe any type of social interaction using technology (primarily the Internet, but also including modern smartphone and PDA innovations) with some combination of words, photos, video, and/or audio."). Such media has surpassed e-mail as the preferred formed of electronic communication. Breanne M. Democko, *Social Media and the Rules on Authentication*, 43 U. TOL. L. REV. 367, 367 (2012).

2. "[Social network sites are] web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system." James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1142 (2009) (quoting Danah M. Boyd & Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship*, 13(1) J. COMPUTER-MEDIATED COMM. art. 11 (2007)), *available at* http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html). *See* Megan Uncel, *"Facebook Is Now Friends with the Court": Current Federal Rules And Social Media Evidence*, 52 JURIMETRICS J. 43, 46–47 (2011) ("Social networking websites are defined by three main functions: first, users create their profile; second, users create and display a list of other users 'with whom they share a connection' and content; lastly, users browse 'their list of connections and those made by others.' ") (citations omitted).

3. Social online networking sites allow members to "use their online profiles to become part of an online community of people with common interests. Once a member has created a profile, she can extend 'friend invitations' to other members and communicate with her friends over the MySpace.com platform via e-mail, instant messaging, or blogs." Doe v. MySpace, Inc., 474 F. Supp. 2d 843, 846 (W.D. Tex. 2007).

4. It is possible to chat privately with individuals and to send private messages on Facebook. *See Facebook Features*, WIKIPEDIA, http://en.wikipedia.org/wiki/Facebook_features (last visited June 24, 2012); Grimmelmann, *supra* note 2, at 1145 (explaining some of Facebook's features, including "a private, email-like 'Message' system"); Uncel, *supra* note 2, at 48–49 (providing a detailed explanation of the many communication features of Facebook and Myspace); People v. Fielding, No. C062022, 2010 WL 2473344, at *1 (Cal. Ct. App. June 18, 2010) ("MySpace *comments* posted to an account can be read by anybody viewing that page, but MySpace *messages* are similar to e-mails and are exchanged privately between 'friends' through MySpace.") (emphasis in original).

5. Therefore, a posting to which Facebook friends have access can be reposted, and the original poster can lose control of who has access to the information.

Currently, Facebook has over 900 million active users,[6] more than half of whom check their pages daily.[7] Users register and create a personal profile using their actual names.[8] Designated "friends" receive feeds of the user's posts and status updates.[9] Such posts can be about politics, upcoming events, or simply the banality and minutiae of everyday life. Status updates can be boring,[10] wry,[11] poignant,[12] mildly amusing,[13] or incendiary.[14] Accumulation of "friends" and "likes" (where users share contents from pages they designate and share postings with their "friends")[15] can

6. *Facebook*, WIKIPEDIA, http://en.wikipedia.org/wiki/Facebook (last visited June 24, 2012). Facebook has been described recently by the Maryland Supreme Court as "the behemoth of the social networking world." Griffin v. State, 19 A.3d 415, 421 n.9 (Md. 2011).

7. *Facebook Statistics, Stats & Facts for 2011*, DIGITAL BUZZ BLOG (Jan. 18, 2011), http://www.digitalbuzzblog.com/facebook-statistics-stats-facts-2011/.

8. *See* Gresham v. City of Atlanta, No. 1:10-CV-1301-RWS-ECS, 2011 WL 4601022, at *2 n.3 (N.D. Ga. Aug. 29, 2011) ("Facebook is an internet based social networking site that allows individuals to maintain profiles of themselves, in which comments, photographs, and other postings may be made to certain other persons also subscribed to Facebook."); Ira P. Robbins, *Writings on the Wall: The Need for an Authorship-Centric Approach To The Authentication Of Social-Networking Evidence*, 13 MINN. J. L. SCI. & TECH. 1, 7 (2012) ("Facebook explicitly requires members to use their real names when creating profiles, but many other social-networking sites, such as MySpace, actually encourage the creation of pseudonymous accounts . . . ."); Andrew C. Payne, *Twitigation: Old Rules in a New World*, 49 WASHBURN L.J. 841, 846–47 (2010) ("Facebook members can share text with multiple people through a 'status update' or through information placed on the user's profile . . . . Users can also share text with another user individually through a direct message to the user or a wall post to the user's profile, or users can have a direct conversation with another user through Facebook's chat feature. Social-networking patrons can also share pictures and videos. A user's 'news feed' displays all the information that his or her friends create, change, or share.").

9. The average user on Facebook has 120 friends. *See* Sheryl Stanberg, *How Many Friends Can You Have?*, FACEBOOK BLOG (Apr. 8, 2009, 4:23 PM), http://blog.facebook.com/blog.php?post=72975227130. However, the limit is 5,000. *See* Aimee Lee Ball, *Are 5,001 Facebook Friends One Friend Too Many?*, N.Y. TIMES (May 30, 2010), http://www.nytimes.com/2010/05/30/fashion/30FACEBOOK.html?_r=1.

10. E.g., "I like carrots, but not cooked carrots." *Boring Status Updates*, FACEBOOK, http://www.facebook.com/pages/Boring-Status-Updates/100530216664201 (last visited June 24, 2012) (consciously attempting to be boring). Another boring Facebook trend is people posting about their breakfasts. *See Trollable*, FACEBOOK, http://www.facebook.com/photo.php?fbid=188083927976152&set=a.113181000879 9778.14420.&type=1&theater (last visited June 24, 2012).

11. E.g., "What good is it to have awesome pictures of burqas, pose with war junk, or wax ironic about pictures taken with celebs if Expat Aid Workers can't share those pictures with the world?" *#16 Facebook*, STUFF EXPAT AID WORKERS LIKE (Jan. 24, 2011), http://stuffexpataidworkerslike.com/2011/01/24/16-facebook/.

12. One can, with a special application, update Facebook friends about one's own death, sharing last words and video. Released once three approved trustees report the death, the status will be post-humously updated with the user's auto-epitaph. *See* Melanie Hick, *Who Will Update Your Facebook Status if You Die?*, HUFFINGTON POST U.K. (Jan. 9, 2012, 12:55 PM), http://www.huffingtonpost.co.uk/2012/01/09/i-die-facebook-app_n_1193443.html (mocking the application).

13. E.g., "Statistically, 6 out of 7 dwarfs aren't happy." *50 Funny Facebook Status Ideas*, RYAN KETT HUB PAGES, http://ryankett.hubpages.com/hub/50-Funny-Facebook-Status-Ideas (last visited Apr. 1, 2012); *Top 100 Status Updates*, FUNNY STATUS, http://www.funnystatus.com/status-updates/top-100-status-updates/ (last visited June 24, 2012) ("Artificial intelligence is no match for natural stupidity.").

14. E.g., "[I]f the fetus whose life you save turns out to be gay, will you still fight for its rights?" *Best Facebook Statuses*, TUMBLR, http://bestfbstatuses.tumblr.com/ (last visited June 24, 2012).

15. *See Like Button*, FACEBOOK DEVELOPERS, http://developers.facebook.com/docs/reference/plugins/like/ (last visited June 24, 2012).

affect social status and business advertising.[16] It is possible to "unfriend" a fellow Facebook user, a term that was recognized by the Oxford American Dictionary as the word of the year in 2009.[17] Unlike blogs or YouTube videos, where the creator of content has little control over who ultimately reads or watches it, social networking sites provide users with the option of controlling the initial dissemination of their posted information.[18] The user's homepage has privacy levels that he or she can adjust regarding who has access to the user's page,[19] though for evidentiary purposes, the privacy settings are meaningless—they have no influence on issues of admissibility.

Other prominent social networking providers include MySpace, which operates similarly to Facebook and focuses heavily on music and popular culture,[20] and LinkedIn, which is a more professional, less social version of networking.[21] In a variation of other social networking sites, another website, Twitter, is "a real-time information network" connecting followers to brief information bites.[22] Twitter communications are denominated "tweets," which are "small bursts of information" 140 characters long.[23]

16. There is a market for gathering "likes" by businesses to establish credibility and advertise their services. *See, e.g.*, SOCIAL FAN HUB, http://www.socialfanhub.com/ (last visited June 24, 2012) (offering businesses "likes" by individual Facebook users).

17. *"Unfriend" the Word of the Year*, CBS NEWS (Nov. 16, 2009, 8:08 PM), http://www.cbsnews.com/2100-201_162-5673974.html (quoting Oxford lexicographer Christine Lindberg as saying "unfriend" has 'real lex-appeal' " for reflecting the mood of the year). *But see* Rick Moriarity, *It's 'Defriend' not 'Unfriend' Says Facebook Co-founder Chris Hughes before Syracuse Lecture*, POST-STANDARD (Nov. 17, 2009, 8:30 PM), http://www.syracuse.com/news/index.ssf/2009/11/its_defriend_not_unfriend_says.html.

18. *See* Indep. Newspapers, Inc. v. Brodie, 966 A.2d 432, 438 n.3 (Md. 2009) (defining social networking sites as "sophisticated tools of communication where the user voluntarily provides information that the user wants to share with others" and distinguishing various privacy controls).

19. *Sharing and Finding You on Facebook*, FACEBOOK, http://www.facebook.com/about/privacy/your-info-on-fb (last visited June 24, 2012).

20. MySpace is a popular social networking website that "allows its members to create online 'profiles,' which are individual web pages on which members post photographs, videos, and information about their lives and interests." Doe v. MySpace, Inc., 474 F. Supp. 2d 843, 845 (W.D. Tex. 2007). United States v. Drew, 259 F.R.D. 449, 453 (C.D. Cal. 2009) ("MySpace is a 'social networking' website where members can create 'profiles' and interact with other members. Anyone with Internet access can go onto the MySpace website and view content which is open to the general public such as a music area, video section, and members' profiles, which are not set as 'private.' However, to create a profile, upload and display photographs, communicate with persons on the site, write 'blogs,' and/or utilize other services or applications on the MySpace website, one must be a 'member.' Anyone can become a member of MySpace at no charge so long as he or she meets a minimum age requirement and register.") (citations omitted).

21. *See About Us*, LINKEDIN, http://press.linkedin.com/about (last visited June 24, 2012) ("LinkedIn operates the world's largest professional network on the Internet with more than 161 million members in over 200 countries and territories.").

22. *See About*, TWITTER, http://twitter.com/about (last visited June 24, 2012) ("Twitter is a real-time information network that connects [its users] to the latest stories, ideas, opinions and news about what you find interesting."). In April 2009, Twitter, "the new kid on the social networking block," had over 14 million users. Sharon Nelson, John Simek & Jason Foltin, *The Legal Implications of Social Networking*, 22 REGENT U.L. REV. 1, 1 (2009-2010). In 2011, Twitter claimed 175 million registered users of whom about 119 million actually regularly follow at least one account. Nicholas Carlson, *How Many Users Does Twitter REALLY Have?* (March 31, 2011), http://articles.businessinsider.com/2011-03-31/tech/30049251_1_twitter-accounts-active-twitter-user-simple-answer.

23. *About*, *supra* note 22. *See also* Ascentive, L.L.C. v. Op. Corp., 842 F. Supp. 2d 450, 456 n.6 (E.D.N.Y. 2011) ("Twitter is a social networking service that allows its users to post messages using

All these media can be accessed not only on a regular computer, but also on tablets and cell phones.[24] Evidence is growing that social media, particularly Twitter, is addictive.[25]

Twitter and Facebook have been excoriated for derogating the quality of communication, increasing isolation,[26] and fostering cyberbullying. They have also been lauded for their roles in bringing people together, most notably in aiding the Arab Spring, allowing revolutionaries to broadcast stories and disseminate pictures as events unfolded.[27] Wherever one stands on the benefits of these new social media, their effects on American culture are marked.

Because caselaw necessarily lags behind technological advances, many of the cases involve MySpace, which is on the wane, and fewer involve Facebook, which is currently the social media leader and has grown exponentially.[28] The real next big thing, however, looks to be Twitter, which courts have barely considered.

---

short communications called 'tweets,' and to read the tweets of other users. Users can, among other things, monitor, or 'follow,' other users' tweets.").

24. *See Apps, SMS, and Mobile*, TWITTER, http://support.twitter.com/groups/34-apps-sms-and-mobile (last visited June 24, 2012).

25. *See* James Meikle, *Twitter is Harder to Resist than Cigarettes and Alcohol, Study Finds*, GUARDIAN (Feb. 3, 2012, 5:37 PM), http://www.guardian.co.uk/technology/2012/feb/03/twitter-resist-cigarettes-alcohol-study; Patrick Garratt, *My Life as a Twitter Addict and Why it is More Difficult to Quit than Drugs*, HUFFINGTON POST (Feb. 29, 2012), http://www.huffingtonpost.co.uk/patrick-garratt/twitter-addictions-more-difficult-to-quit-than-drugs_b_1305760.html ("[W]e've seen the internet revolutionise the way we interact with one another, with Facebook emerging as the global connectivity poster boy, but nothing else matches the pure buzz of Twitter."); Larry Carlat, *Confessions of a Tweeter*, N.Y. TIMES (Nov. 11, 2011), http://www.nytimes/2011/11/13/magazine/confessions-of-a-tweeter.html?_r=1 (detailing the author's loss of jobs and relationships due to his Twitter compulsion).

26. Stephen Marchie, *Is Facebook Making Us Lonely*, ATLANTIC MAGAZINE (May 2012), http://www.theatlantic.com/magazine/archive/2012/05/is-facebook-making-us-lonely/8930/ (our "web of connections ha[ve] grown broader but shallower").

27. *See* William Seltan, *Springtime for Twitter: Is the Internet Driving the Revolutions of the Arab Spring?*, SLATE (July 18, 2011, 8:34 AM), http://www.slate.com/articles/technology/future_tense/2011/07/springtime_for_twitter.html (noting that the "little" technologies such as cell phones are crucial in avoiding repression, though totalitarian regimes also used the Internet to foster repression). "[S]ocial media can be helpful in: a) mobilizing protesters rapidly; b) undermining a regime's legitimacy; or c) increasing national and international exposure to a regime's atrocities." *Twitter, Facebook and YouTube's Role in Arab Spring (Middle East Uprisings)*, SOC. CAP. BLOG (May 23, 2012), http://socialcapital.wordpress.com/2011/01/26/twitter-facebook-and-youtubes-role-in-tunisia-uprising/ (last visited June 24, 2012). *But see* Malcolm Gladwell, *Small Change: Why the Revolution will not be Tweeted*, NEW YORKER (Oct. 4, 2010), http://www.newyorker.com/reporting/2010/10/04/101004fa_fact_gladwell (arguing that the effect of social networking on true change was overstated and the nature of strong ties needed to foment revolution couldn't be accomplished via relatively anonymous social media).

28. *See* John S. Wilson, *MySpace, Your Space, or Our Space? New Frontiers in Electronic Evidence*, 86 OR. L. REV. 1201, 1221–24 (2007) (reviewing the history of social networking sites).

III. WHY DOES SOCIAL MEDIA MATTER FOR EVIDENCE LAW?

A. *Social Media's Relevance to Litigation Issues Other than Admission of Evidence*

The social media revolution affects many areas of litigation other than evidence law.[29] For instance, attorneys use social media to check out potential jurors during voir dire.[30] Similarly, attorneys may investigate potential witnesses on Facebook to learn about them, to anticipate problems with cross-examination, or to begin to craft ways to impeach them. An interesting question of ethics has arisen concerning whether attorneys may instruct private investigators to "friend" witnesses without disclosing their motives and association with the litigation.[31]

Social media is a major factor in juror misconduct during trial and deliberation.[32] Juror misbehavior on the Internet, either by gathering outside information in contravention of the judge's instructions or by posting confidential juror information or opinions mid-trial, occurs with increasing frequency.[33]

---

29. Beth C. Boggs & Misty L. Edwards, *Does What Happens on Facebook Stay on Facebook? Discovery, Admissibility, Ethics, and Social Media,* 98 ILL. B.J. 366, 367 ("As the popularity of social networking sites like Facebook, LinkedIn, Twitter, and MySpace grows, so does their importance in litigation. More and more attorneys use these rich archives of personal information to investigate the backgrounds of parties, witnesses, opposing counsel, jurors, and even judges.").

30. This is the subject of fantastical novels such as John Grisham's *The Runaway Juror. See Publishers Weekly*, AMAZON, http://www.amazon.com/The-Runaway-Jury-John-Grisham/dp/0440221471 (last visited Aug. 20, 2012) ("The details of jury selection are fascinating and the armies of lawyerly hangers-on and overpaid consultants that surround such potentially profitable (to either side) cases are horribly convincing.").

31. *See* PHILA. BAR ASS'N PROF'L GUIDANCE COMM., Op. 2009–02 (March 2009), *available at* http://www.philadelphiabar.org/WebObjects/PBAReadOnly.woa/Contents/WebServerResources/CMSResources/Opinion_2009-2.pdf (advising that directing an investigator to become a Facebook friend with a non-party witness would be unethical, even if the investigator used his real name); BROWNING, *supra* note 1, at 155–59.

32. *See, e.g.*, State v. Dellinger, 696 S.E.2d 38 (W. Va. 2010) (juror communicated with accused on MySpace); Dimas-Martinez v. State, No. CR 11-5, 2011 WL 6091330 (Ark. Dec. 8, 2011) (juror continued tweeting after court admonished him to desist). Colorado Civil Jury Instruction 1.5 provides, in relevant part, "Until I tell you that your jury service is completed, do not communicate with anyone, including family and friends, about the evidence or the issues in this case. This prohibition applies to all forms of communication . . . . For example, you must not communicate about this case by email, text messages, Twitter, blogging, or social media like Facebook." State v. Abdi, No. 2010-255, 2012 WL 231555, ¶ 25 n.3 (Vt. Jan. 26, 2012) (quoting the jury instruction). Nelson, Simek, & Foltin, *supra* note 22, at 7 (discussing an Oregon court instruction that includes the admonition, "[D]o not use any electronic device or media, such as the telephone, a cell or smart phone, Blackberry, PDA, computer, the Internet, any Internet service, any text or instant messaging service, any Internet chat room, blog, or website such as Facebook, My[ ]Space, YouTube or Twitter, to communicate to anyone any information about this case until I accept your verdict."). *See generally* John W. Clark, Andrea Wierzchowski, & Chelsea Luker, *Social Networking and the Contemporary Juror,* 47 CRIM. L. BULL. 83 (2011).

33. *See generally* Michelle Sherman, *The Anatomy of a Trial with Social Media and the Internet,* 14 J. INTERNET L. 1 (2011) (discussing jurors who blog about the case or otherwise fail to follow courts' limitations on social network use); David P. Goldstein, *The Appearance of Impropriety and Jurors on Social Networking Sites: Rebooting the Way Courts Deal with Juror Misconduct*, 24 GEO. J. LEGAL ETHICS 589 (recounting cases of jurors tweeting projected civil verdicts or polling friends by Facebook as to guilt).

In a very unusual Australian case—perhaps a sign of things to come—a defendant with a default judgment against him was served with notice of the default via his Facebook page, which he checked regularly.[34]

By far the most interesting and difficult questions pertaining to social media outside the area of evidence law arise in discovery. In civil cases, courts are struggling with how a party can obtain evidence of an opponent's social media output. In criminal cases, issues of search and seizure arise. These questions are beyond the scope of this Article, which examines the admissibility of such social media, not how it is obtained. Even when not admissible, however, social media can provide significant relevant information.[35]

B. Social Media's Relevance to Litigation Issues Involving the Admission of Evidence

Increasingly, evidentiary issues concerning the admission of social media arise in both civil and criminal cases. It is not hard to see why parties might value Facebook posts and tweets, which are often spontaneous, uncensored, newsy, and self-revelatory.[36] In fact, not consulting social media for investigative and evidence purposes has been deemed by some as legal malpractice.[37] Furthermore, social media users may not realize how accessible and public their information is.[38]

In one example that had less to do with the content of the speech than the fact of having made it, an accused offered as an alibi that he could not have committed the crime because at the time of the crime, he was logged into his Facebook account posting updates to his page.[39] The prosecution accepted his argument as sufficient to drop the charges.[40] More often, however, it is the prosecution that wishes to introduce evidence about the

34. *See* Pamela Pengelley, *Can Facebook Information Be Used in Court?*, TURNERS TIPS (Apr. 8, 2009), http://turnerstips.wikidot.com/can-facebook-in-court; BROWNING, *supra* note 1, at 29–36 (chapter entitled "Served Through Facebook" describing cases in Australia and the United Kingdom).

35. BROWNING, *supra* note 1, at 11 ("attorneys can find useful and sometimes startling information on other parties, key witnesses and even their own clients").

36. Deborah Jones Merritt, *Social Media, The Sixth Amendment, and Restyling: Recent Developments in the Federal Law of Evidence*, 28 TOURO L. REV. 27, 46 (2012) ("users of social media are surprisingly indiscrete"); Seth P. Berman et al., *Web 2.0: What's Evidence Between "Friends"?*, 53 B.B.J. 5, 6 (2009) (social networking sites "may record people's thought processes and impressions in unguarded moments, exactly the sort of evidence that can be invaluable during litigation.").

37. Nelson, Simek, & Foltin, *supra* note 22, at 14 ("It should now be a matter of professional competence for attorneys to take the time to investigate social networking sites."); *See generally*, BROWNING, *supra* note 1.

38. BROWNING, *supra* note 1, at 48–49. Nelson, Simek, & Foltin, *supra* note 22 ("Initially, very few people used the privacy settings that were available to them.").

39. *See* Joseph Goldstein, *In Social Media Postings, a Trove for Investigators,* N.Y TIMES (Mar. 2, 2011), http://www.nytimes.com/2011/03/03/nyregion/03facebook.html (discussing the case of Rodney Bradford, whose posting about breakfast made from his father's home in Manhattan exonerated him from a charge of bank robbery in Brooklyn at the same time); BROWNING, *supra* note 1, at 108–110.

40. Goldstein, *supra* note 39.

accused, including evidence where the accused boasts of her crime.[41] Alternatively, the prosecutor may wish to introduce a picture of the accused from her Facebook page, toting weapons in violation of her parole.[42] In another variation, a party may wish to demonstrate that a witness was threatened.[43] Social media may be one method of criminal stalking or bullying.[44] Finally, social media can be important at sentencing to refute allegations of remorse, such as the Facebook pictures of a drunk driver partying with alcohol and making flip comments about being drunk post-conviction.[45]

In civil cases, Facebook or other social media can provide evidence of a tort, such as harassment or defamation.[46] Social media postings can also support the defense in various tort areas, most notably personal injury, sick leave,[47] and workers' compensation. A plaintiff who claims she is immobilized or severely limited in her activities may provide substantive and impeachment evidence for the defense if she posts pictures of herself rock climbing, bowling, or line dancing.[48] The issues of admissibility are important not just for evidentiary rulings at trial, but also for pre-trial summary judgment motions, which must be supported by admissible evidence.[49]

---

41. *See, e.g.*, *In re* Welfare of D.L.W., No. A11-1238, 2012 WL 171412, at *1 (Minn. Ct. App. Jan. 23, 2012) (bragging about fight on Facebook undermines self-defense and unfair prejudice of boast did not outweigh probative value). *See also* BROWNING, *supra* note 1, at 49–50 (discussing poachers who posted about the endangered species they caught and ate before being imprisoned for the crime; bus thief documented his joy-ride on YouTube). One defense attorney lamented:

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.

Robbins, *supra* note 8, at 15 (quoting Laurie Mason, *Defense Attorneys Trolling the Net, Too*, BUCKS CNTY. COURIER TIMES (Aug. 23, 2008), http://www.highbeam.com/doc/1P3-1549445091.html).

42. State v. Cisz, No. 1 CA-CR 11-0244, 2011 WL 5964518, at *1 (Ariz. Ct. App. Nov. 29, 2011). *See also* State v. Felts, No. M2007-00945-CCA-R3-CD, 2008 WL 2521663, at *1 (Tenn. Crim. App. June 24, 2008) (admitting picture of "defendant holding an SKS assault rifle" on his MySpace page, linking him to the type of weapon used).

43. *See* State v. McWilliams, No. 2011-CA-00051, 2012 WL 554435, at *4 (Ohio Ct. App. Feb. 13, 2012) ("[A]t the dawn of the 21st century, there are a multitude of methods by which criminal threats may be conveyed: phone, pager, e-mail, blog, Twitter, Facebook, and so forth."); Griffin v. State, 995 A.2d 791, 795 (Md. Ct. Spec. App. 2010), *rev'd*, 19 A.3d 415 (Md. 2011).

44. *See, e.g.*, United States v. Cassidy, 814 F. Supp. 2d 574 (D. Md. 2011) (finding federal anti-stalking law unconstitutional as applied).

45. *See* Nelson, Simek, & Foltin, *supra* note 22, at 12 n.90 (citing Vesna Jaksic, *Litigation Clues Are Found on Facebook*, NAT'L L.J. (Oct. 15, 2007), http://vesnajaksic.com/?page_id=35).

46. *See, e.g.*, Gaston v. Facebook, Inc., No. 3:12-cv-00063-ST., 2012 WL 610005 (D. Or. Feb. 24, 2012); Boyd v. Int'l Ass'n of Machinist & Aerospace Workers, No. 11-2496, 2012 WL 78250 (D.N.J. Jan. 9, 2012); Tanner v. Ebbole, 88 So. 3d 856 (Ala. Civ. App. 2011).

47. Marianne White, *Quebec Woman Alleges Sick Leave Benefits Cut Off Because of Facebook*, GINGER TOES (Nov. 19, 2009, 6:02 PM), http://gingertoes.wordpress.com/2009/11/20/quebec-woman-alleges-sick-leave-benefits-cut-off-because-of-facebook/.

48. *Facebook Photos Fail to Undermine Victim's Claim Against ICBC*, VANCOUVER SUN (Sept. 30, 2009), http://www.canada.com/vancouversun/news/westcoastnews/story.html?id=5b189b7e-86d8-ab25-5eaa2b62fa6b (recounting the case of a Vancouver woman who claimed that her injuries diminished her enjoyment of dancing, hiking, and cycling, although photos from her Facebook profile showed her cycling and hiking after her injury and probably diminished the award).

49. FED. R. CIV. P. 56. *See* Impact Mktg. Int'l, L.L.C. v. Big O Tires, L.L.C., No. 2:10-CV-01809-RLH, 2012 WL 359914 (D. Nev. Feb. 2, 2012) (holding that trial court can only consider admissible

Outside of tort law, family law presents another area of civil litigation where evidence from social media is increasingly important. When parents engage in a heated custody battle, pictures and postings portraying drunken, drug-related, or sexually inappropriate behavior could prove significant.[50] Similarly, where infidelity is an issue, social media can provide evidence of cheating.[51]

IV. HEARSAY AND THE INTRODUCTION OF SOCIAL MEDIA

Because any statements made on social media are by definition out-of-court, they will at least raise traditional hearsay concerns and, in criminal cases, raise confrontation issues if the government wishes to use the out-of-court statement against the accused and the declarant does not testify. Any statement on social media made outside the courtroom will trigger questions about hearsay, authentication (which is discussed in the next section), and best evidence[52] (which is not addressed in this Article because no interesting or special questions arise from the context of social media).[53]

A. Statements Admitted Not for Their Truth but for Another Purpose

Not all out-of-court statements qualify as hearsay. The Federal Rules define hearsay as statements that are used to prove the truth of the matter asserted.[54] In other words, an out-of-court-statement is hearsay only if the trier of fact is being asked to believe that the statement is true. Where the statement is not being offered for its truth but is being offered just to show that it was uttered, the statement is not being offered for a hearsay purpose. When, for instance, the MySpace page of the accused was used to show his gang nickname and paraphernalia, but not the assertions in the

evidence in ruling on a motion for summary judgment and therefore may not consider unauthenticated documents); Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 538 (D. Md. 2007) (explaining the need for admissible evidence in determining a summary judgment motion).

50. *See* Lalonde v. Lalonde, No. 2009-CA-002279-MR, 2011 WL 832465, at *2 (Ky. Ct. App. Feb. 25, 2011) (factoring pictures on Facebook of the mother drinking in contravention of medical advice into granting custody to the father); Dexter v. Dexter, No. 2006-P-0051, 2007 WL 1532084, at *6 (Ohio Ct. App. May 25, 2007) (noting that in the mother's MySpace writings, she stated that while she was on a hiatus from using illicit drugs during the pendency of these proceedings, she planned on using drugs in the future and would use them in her home if her daughter were sleeping); BROWNING, *supra* note 1, at 39–41 (recounting dissolution and custody cases where Facebook pages were introduced).

51. *See* Stephanie Chen, *Divorce Attorneys Catching Cheaters on Facebook*, CNN (June 01, 2010), http://articles.cnn.com/2010-06-01/tech/facebook.divorce.lawyers_1_privacy-settings-social-media-facebook?_s=PM:TECH.

52. The best evidence rule requires that when a party wishes to prove the contents of a document, that party must present the document, when it is available, rather than merely solicit testimony about it. *See* FED. R. EVID. 1002. So, under the best evidence rule, a plaintiff wishing to offer evidence of a defamatory statement made by the defendant on a Facebook page would have to bring in a copy of the page itself. Unless issues arise concerning authentication or fairness, the best evidence rule accepts a duplicate as well as an original. *See* FED. R. EVID. 1003. Any printout of the page would be an original. *See* FED. R. EVID. 1001.

53. *See* Jonathan L. Moore, *Time for an Upgrade: Amending the Federal Rules of Evidence to Address the Challenges of Electronically Stored Information in Civil Litigation*, 50 JURIMETRICS J. 147, 148, 173–174 (2010) (noting that the majority of courts treat printouts of electronically stored material—even if modified—as originals that satisfy the best evidence rule).

54. FED. R. EVID. 801(a)–(c).

messages, the court explained that the accused's "hearsay challenge is without merit because the trial court did not admit the MySpace material for the truth of any assertion on the page."[55] The court explained further that the accused's hearsay objection failed

> because the nature of the evidence here did not consist of declarative assertions to be assessed as truthful or untruthful, but rather circumstantial evidence of [the accused]'s active gang involvement. For example, a reasonable jury would understand its purpose was not to determine whether [the accused] and his "Krew" were truly "Most Wanted" by the "Ladiez" in Orange County.[56]

Classic examples of statements that are not hearsay because they are being offered for a purpose other than their truth include circumstantial evidence of state of mind, effect on the listener, statements offered for impeachment, and legally operative facts. Some posts on social media will fall into these categories. On the issue of impeachment,[57] for instance, to show that a party was aware of an allegedly dangerous condition, warnings by posters on his Facebook page could be admissible not to prove the dangerous condition but to demonstrate effect on the listener—that the party was aware of them. Although I could find no example using social media, courts regularly allow evidence of notice on email to be introduced as outside the hearsay bar.[58] Statements of defamation, extortion, conspiracy, or threat would all be legally operative facts and hence not fit within the hearsay definition. Statements on social media could also be used to refresh the recollection of the declarant who is testifying. Jogging the memory of a witness with a document is not a hearsay use.[59]

B. Parties' Statements Offered by Party Opponents

Much of what might be offered at trial will, however, be introduced for its truth and hence fit the classical definition of hearsay. Even when a statement is technically hearsay according to the common law definition, some statements are deemed "not hearsay" under the Federal Rules because they fall within specified exemptions.[60] The most useful exemption for social media is statements by the parties themselves. Anything a party

55. People v. Valdez, 135 Cal. Rptr. 3d 628, 634 (Ct. App. 2011).

56. *Id.*

57. *In re* K.W., 666 S.E.2d 490, 494 (N.C. Ct. App. 2008) (holding that child victim's statements on her MySpace page were admissible for impeachment of her testimony, but that their exclusion was harmless error).

58. *See, e.g.*, X17, Inc. v. Lavanderia, No. CV06-7608-VBF(JCX), 2007 WL 790061 (C.D. Cal. March 8, 2007).

59. FED. R. EVID. 612 (providing the rules concerning writings used to refresh a witness's memory and requiring that the opposing party be able to view the refreshing document).

60. Here, I distinguish between exceptions that avowedly are hearsay but are nonetheless excepted from the hearsay ban, and exemptions that some rulemakers deem by fiat to be "not hearsay," but really are. *See* FED. R. EVID. 801(d).

says or does (other than a criminal defendant who has not been Mirandized but nevertheless makes statements to the police during a custodial interrogation)[61] is exempted from the hearsay rule.[62] Therefore, any relevant statement a party posts on her Facebook page or tweets on her Twitter account will be admissible notwithstanding the hearsay bar, if offered by her party opponent.[63] This huge exemption from hearsay affects much of the evidence parties will attempt to introduce at trial, particularly in civil cases. The exemption applies not only to direct personal statements but also to statements made by agents, employees, and co-conspirators. In *State v. Greer*,[64] the Ohio appellate court held that the trial court did not err in admitting the accused's own statements from his MySpace page that were offered by the government. In a South Carolina case, an alleged bank robber logged into his MySpace page to inform his followers: "On tha run for robbin a bank Love all of yall."[65] That message was admissible.

C. *Prior Consistent Statements of Witnesses*

Sometimes a party will wish to introduce his own statement. Just because the party testifies does not necessarily render his prior consistent statements admissible. When a party's statement is offered by the party himself and not the party opponent, a hearsay question arises. Such statements may fall within other exemptions or exceptions to the hearsay rule.

States vary significantly in their treatment of a witness's prior consistent statement (including that of a party). Under certain circumstances, the Federal Rules of Evidence allow such evidence both for common-law rehabilitation and for the truth of the matter asserted.[66] The Rules limit the substantive use of prior consistent statements of witnesses to situations where the proponent wishes to rebut a charge that the declarant recently fabricated his current testimony or acted from a recent improper motive or influence.[67] Under the Federal Rules of Evidence, to be admissible, the prior statement must have been made after the alleged motive to fabricate

61. Miranda v. Arizona, 384 U.S. 436 (1966) (statements made by an accused in police custody are admissible only if the accused received information about his right to counsel and right against self-incrimination).

62. FED. R. EVID. 801(d)(2).

63. *See, e.g.*, People v. Oyerinde, No. 298199, 2011 WL 5964613 (Mich. Ct. App. Nov. 29, 2011) (admitting relevant Facebook posts by the accused). This, of course, assumes that the statement presents no other evidentiary problems such as providing impermissible character evidence under Rule 404 or being so unfairly prejudicial so as to substantially outweigh the probative value of the statement under Rule 403.

64. 2009 WL 2574160 (Ohio Ct. App. Aug. 20, 2009). *See also* United States v. Sullivan, 2011 WL 4808118 (N.D. Ill. Oct. 11, 2011) (addressing statements made on an employee's MySpace page, as potential admissions by the accused).

65. *See* Goldstein, *supra* note 39.

66. I do not discuss prior inconsistent statements because such statements, when generated on social media, do not fit the requirements of Rule 801(d)(1)(A), under which the prior inconsistent statement has to be made under oath at a prior proceeding. *See* FED. R. EVID. 801(d)(1)(A).

67. FED. R. EVID. 801(d)(1)(B).

arose.[68] Essentially, for non-hearsay rehabilitation, the evidence is being used to say, "You see, the witness has been saying this all along."[69] For its substantive use, the theory is, "You see, the witness has said it all along, it's true, and you can use the witness's prior consistent statement as evidence."

D. State of Mind

One frequent use of statements on social media is to prove the state of mind of the speaker. Although hearsay, such statements are nevertheless admissible for their truth because they fall under a special exception for the declarant's "then existing mental, emotional or physical condition."[70] The exception covers statements relating to motive, intent, plan, and feelings, both physical and emotional.[71] The exception does not include statements of memory or belief, so the memory of a feeling or the then-belief of a fact is not covered by the exception.[72]

As the Court explained in the important and comprehensive analysis of *Lorraine v. Markel American Insurance Company*:

> [G]iven the ubiquity of communications in electronic media (e-mail, text messages, chat rooms, internet postings on servers like "myspace" or "youtube" or on blogs, voice mail, etc.), it is not surprising that many statements involving observations of events surrounding us, statements regarding how we feel, our plans and motives, and our feelings (emotional and physical) will be communicated in electronic medium.[73]

For instance, the accused assaulter of Representative Gabrielle Gifford posted a message on his MySpace page saying "Goodbye friends" hours before he went on his shooting rampage.[74] That post could help establish intent and could serve as evidence of premeditation.[75] In *People v. Oyerinde*, the trial court admitted Facebook page statements to demonstrate the victim's state of mind, but the appellate court indicated that the evidence, though ultimately harmless error, should have been excluded as facts remembered or believed.[76]

---

68. The Supreme Court held that 801(d)(1)(B) "permits the introduction of a declarant's consistent out-of-court statements to rebut a charge of recent fabrication or improper influence or motive only when those statements were made before the charged recent fabrication or improper influence or motive." Tome v. United States, 513 U.S. 150, 167 (1995).

69. *See, e.g.*, State v. Neese, No. M2005-00752-CCA-R3-CD2006, 2006 WL 3831387 (Tenn. Crim. App. Dec. 15, 2006) (allowing prior consistent statements of an abuse victim during a forensic interview to rehabilitate the witness after insinuations of fabrication and coaching.)

70. FED. R. EVID. 803(3).

71. *Id.*

72. *Id.* (excluding "statement[s] of memory or belief to prove the fact remembered or believed").

73. 241 F.R.D. 534, 568–69 (D. Md. 2007).

74. *See* Goldstein, *supra* note 33. The statement would also be admissible as a statement by a party-opponent under FED. R. EVID. 801(d)(2)(A).

75. *Id.*

76. People v. Oyerinde, No. 298199, 2011 WL 5964613 (Mich. Ct. App. Nov. 29, 2011).

E. Present Sense Impressions

The present sense impression creates a hearsay exception for statements "describing or explaining an event or condition, made while or immediately after the declarant perceived it."[77] A statement such as, "My, the sun is bright," qualifies as a present sense impression because it was made while the event was occurring, arguably before the declarant has the time or presence of mind to conjure something untrue.[78] Arguably, most postings on Facebook and MySpace will not qualify because of the timing requirement, since most posts are made sufficiently later than the time the declarant perceived the event.[79]

Professor Jeffery Bellin has raised interesting questions about the present sense impression with regard to Twitter.[80] Because tweets are sometimes composed while the event is occurring, they seem to fit this hearsay exception. Status updates on Facebook and Google+ might also have comparable immediacy. Bellin posits that the current exception was not designed with social media in mind and that one guarantee of trustworthiness—the presence of others who can testify not only to the statement but also to the underlying event or condition—is noticeably absent when present-sense statements are communicated via Twitter.[81]

A traditional present sense impression uttered to fellow passengers, such as, "That Ford pickup is weaving all over the road," would have corroborative witnesses—if not about the truck's behavior, then about what was happening with the declarant. A tweet concerning the same occurrence would not. Tweeting and other social media forms of concurrent updating are meant for public consumption and entertainment. As one compulsive tweeter explained: "When I wasn't on Twitter, I would compose faux aphorisms that I might use later."[82] The declarant expects to communicate with a far-flung audience that cannot verify the truth of the tweets. Bellin is persuasive in arguing for the return of some sort of corroboration requirement before tweets and analogous forms of immediate social media communication are admitted as present sense impressions.

---

77. FED. R. EVID. 803(1).

78. The reliability of present sense impressions stems from:

> (1) the report at the moment of the thing then seen, heard, etc., is safe from any error from defect of memory of the declarant; (2) there is little or no time for a calculated misstatement; and (3) the statement will usually be made to another (the witness who reports it) who would have the equal opportunity to observe and hence to check a misstatement.

Eisenman v. State, No. 13-05-705-CR, 2008 WL 2515877, at *14 (Tex. App. Jan. 10, 2008) (citations omitted).

79. *But see* United States v. Ferber, 966 F. Supp. 90 (D. Mass. 1997) (holding, in a mail/wire fraud case, that an e-mail from an employee to their boss regarding the substance of a telephone call with the defendant qualified as a present sense expression).

80. *See* Jeffrey Bellin, *Facebook, Twitter, and the Uncertain Future of Present Sense Impressions,* 160 U. PA. L. REV. 331 (2012).

81. *Id.* at 334–35.

82. Carlat, *supra* note 25.

F. Excited Utterances

Another exception to the hearsay rule is the excited utterance, which creates a hearsay exception for statements "relating to a startling event or condition, made while the declarant was under the stress of excitement" of the precipitating condition.[83] The theory of the exception is that under the stress of the excitement, the declarant will not have the opportunity to confabulate.[84] Although there is a built-in timing requirement (the length of time the declarant remains under stress), the time between the event and the declaration is not as short as with the present sense impression. Because the excited utterance requires a startling event that still holds the declarant in its thrall, it is a poor fit with social media. If a person is calm enough to tweet or to update her Facebook status, then the effect of the startling event has passed.

G. Recorded Recollections—But Not Business Records

Tweets and posts to Facebook do not qualify as business records. Statements made by individuals for non-business purposes on social media cannot qualify as business records. They simply lack the business purpose and routine practice of recording such business activity that the business record rule requires.[85] However, they may qualify as recorded recollections if (1) the declarant cannot fully remember the incident, (2) the writing was made when the event was fresh in the declarant's memory, and (3) the writing accurately reflects the declarant's knowledge.[86] If a tweet or a Facebook comment or update is admitted under the recorded recollection exception, it is generally read into the record and may be received as an exhibit only if offered by an adverse party.[87]

H. Dying Declarations

There is already sad evidence of suicide notes on Twitter and Facebook.[88] A post on social media could fit the requirements of a dying declaration. The declarant would have to be unavailable, the statement would have to be made while the declarant believed he was dying, and it

83. FED. R. EVID. 803(2).

84. *See* Aviva Orenstein, *"My God!": A Feminist Critique of the Excited Utterance Exception to the Hearsay Rule,* 85 CALIF. L. REV. 159 (1997).

85. *See* FED. R. EVID. 803(6).

86. FED. R. EVID. 803(5).

87. *Id.*

88. *See Woman Posted Suicide Note on Facebook,* THESMOKINGGUN.COM (January 24, 2012), http://www.thesmokinggun.com/documents/suicide-note-on-facebook-453129 (Suicide note, "i cant handle this shit anymore," barring her father from the funeral posted on Facebook immediately before mother of three shot herself); Jakob Rodgers, *Soldier Wrote Facebook Suicide Note Before Springs Crash,* COLORADO SPRINGS GAZETTE (Jan 7, 2012, 11:00 AM), http://www.gazette.com/articles/wrote-131361-facebook-springs.html; Catharine Smith, *Man Posts Suicide Note to Twitter,* HUFFINGTON POST (May 25, 2011 5:50 PM), http://www.huffingtonpost.com/2010/06/16/twitter-suicide-note-post_n_614956.html. *Cf.* Lisa Belkin, *Announcing a Child's Death on Twitter,* N.Y. TIMES (Dec. 17, 2009, 12:26 PM), http://parenting.blogs.nytimes.com/2009/12/17/tweeting-about-a-childs-death/.

would have to concern the cause of death.[89] Dying declarations have recently attracted more attention because the Supreme Court has indicated that they are a *sui generis* exception to the Confrontation Clause.[90]

I. Declarations Against Interest

A statement against interest is one that

> a reasonable person in the declarant's position would have made only if the person believed it to be true because, when made, it was so contrary to the declarant's proprietary or pecuniary interest or had so great a tendency to invalidate the declarant's claim against someone else or to expose the declarant to civil or criminal liability . . . .[91]

To be admissible, the declarant must be unavailable[92] and the statement tending to expose the declarant to criminal liability must be corroborated by circumstances clearly indicating its trustworthiness.[93] The Supreme Court has explained that "only those declarations . . . that are individually self-inculpatory" are admissible under Rule 804(b)(3).[94] Whether a statement meets the interest criteria can only be judged in context.[95] The declaration must be consciously against interest at the time it was made. As of this writing, I could find no case admitting a statement on social media via this exception. In one case, evidence of a person's salary posed on MySpace was not admissible because although detrimental to her custody case, it was not against interest at the time it was made.[96] Courts have admitted emails as statements against interest.[97]

J. Forfeiture of the Hearsay Right

Where a party intentionally renders a declarant unavailable, the declarant's statement may be admitted even if it is hearsay.[98] This hearsay

89. FED. R. EVID. 804(b)(2). Under the Federal Rules, dying declarations may be offered in civil and homicide cases. *See* Aviva Orenstein, *Her Last Words: Dying Declaration and Modern Confrontation Jurisprudence*, 2010 U. ILL. L. REV. 1141 (2010).

90. *See* Crawford v. Washington, 541 U.S. 36, 56 n.6 (2004) (noting in dicta that the dying declaration may be "deviation" from the general rule confrontation rule); Giles v. California, 554 U.S. 353, 358–59 (2008).

91. FED. R. EVID. 804(b)(3)(A).

92. Sources of unavailability include incapacity, death, refusal on pain of contempt to testify, and privilege. *See* FED. R. EVID. 804(a).

93. FED. R. EVID. 804(b)(3)(B). "A statement is admissible under this exception if: (1) the speaker is unavailable; (2) the statement is actually adverse to the speaker's penal interest; and (3) corroborating circumstances clearly indicate the trustworthiness of the statement." United States v. Smith, 383 F. App'x 355, 356 (4th Cir. 2010) (internal quotation marks omitted).

94. Williamson v. United States, 512 U.S. 594, 599 (1994).

95. *Id.* at 604.

96. Musgrove v. Helms, Nos. 08CA96, 09CA76, 2011 WL 1225672, at *6 (Ohio Ct. App. April 1, 2011). It is unclear to me why the statement on MySpace was not a statement by a party opponent under Rule 801(d)(2)(A).

97. *See, e.g.*, S.E.C. v. Sirianni, 334 F. App'x 386 (2d Cir. 2009).

98. FED. R. EVID. 804(b)(6).

exception is grounded in basic fairness. If a party wrongfully caused or acquiesced in making the declarant unavailable and intended to do so, then the party cannot be heard to complain that the statement is hearsay. As with declarations against interest, the exception applies only if the declarant is deemed unavailable.

K. The Residual Hearsay Exception

"To be admissible under Rule 807, the evidence must be (1) trustworthy, (2) material, (3) more probative than other available evidence, and must fulfill, (4) the interests of justice, and (5) notice."[99] Courts apply this residual or catch-all exception "very rarely, and only in exceptional circumstances."[100] Rule 807 is used as a back-up argument or part of a laundry list of exceptions when a court admits an out-of-court statement. For instance, one district court explained its ruling as follows: "The statements . . . are likely admissible because they will not be offered to prove the truth of the matter asserted and even if they are, they fall within one or more exceptions, specifically, the state of mind exception or the residual exception."[101] Federal district courts have admitted emails under this rule, but I have so far found no Facebook posts or other social-media material admitted under the residual hearsay exception.[102]

L. The Confrontation Clause

In criminal matters, where a "testimonial statement" is offered against the accused for its truth, the evidence will have to satisfy the Sixth Amendment Confrontation Clause as interpreted by *Crawford v. Washington.*[103] *Crawford* held that testimonial statements offered against the accused must be subject to cross examination.[104] If the declarant is proven unavailable, then the prosecutor may use the testimonial statement only if the declarant had a previous opportunity to confront the accused.[105] The only exceptions to the *Crawford* rule are dying declarations and forfeiture, where the accused has intentionally made the declarant unavailable.[106]

Hearsay exceptions that require unavailability (such as declarations against interest) trigger a *Crawford* inquiry in criminal cases. The complicated and unresolved question concerns the extent to which statements are "testimonial," intended as a substitute for in-court testimony or at the very

99. Lasnick v. Morgan, No. 3:10-cv-345 (JCH), 2011 WL 6300159, at *2 (D. Conn. 2011) (quoting Silverstein v. Chase, 260 F.3d 142, 149 (2d Cir. 2001)).

100. Parsons v. Honeywell, Inc., 929 F.2d 901, 907 (2d Cir.1991).

101. Fair Isaac Corp. v. Experian Info. Solutions Inc., No. 06-4112 ADM/JSM, 2009 WL 3526491, at *1 (D. Minn. 2009).

102. *See, e.g., Lasnick*, 2011 WL 6300159. *But see* Steven Shipping & Terminal Co. v. Japan Rainbow, 334 F.3d 439 (5th Cir. 2003) (holding that the district court did not err in admitting email correspondence under rule 807); Mercer v. Csiky, No. 08-11443-BC, 2010 WL 3565811 (E.D. Mich. Sept. 13, 2010) (rejecting application of Rule 807 to email statements).

103. 541 U.S. 36 (2004).

104. *Id.* at 68–69.

105. *See* PARK, LEONARD, ORENSTEIN & GOLDBERG, EVIDENCE LAW 414 (3d ed. 2011).

106. *See* Giles v. California, 554 U.S. 353, 357–61 (2008).

least made with awareness that the prosecution could use the statement. Statements seeking help—requesting others call 911 for instance—would not be testimonial. Statements intentionally inculpating the accused and made with full awareness that such statements would be helpful to the prosecution later might be testimonial, though they would have to be distinguishable from mere casual statements to friends.

V. AUTHENTICATION

A. Authentication Generally

Authentication questions are by far the most interesting issues raised by new social media. Whereas the traditional hearsay rules seem to fit nicely with new types of communication—which, after all, still remain out-of-court statements—the rules of authentication fit less well. There is little push to alter the rules,[107] but applying them to new media can be tricky.[108]

Essentially, the authentication question is a simple one: is the item what its proponent claims it is?[109] The authentication process requires two steps.[110] The first entails the gatekeeping role of the judge, who must determine whether a jury could find the item authentic; the second involves

107. *See, e.g.*, State v. Eleck 23 A.3d 818, 823 (Conn. App. Ct. 2011) ("[T]he emergence of social media such as e-mail, text messaging and networking sites like Facebook may not require the creation of new rules of authentication with respect to authorship."); Commonwealth v. Purdy, 945 N.E.2d 372, 378, 381 (Mass. App. Ct. 2011) ("While e-mails and other forms of electronic communication present their own opportunities for false claims of authorship, the basic principles of authentication are the same.") (citing United States v. Safavian, 435 F. Supp. 2d 36, 41 (D.D.C. 2006)); Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 539 n.5 (D. Md. 2007) (noting the capacity of the current rules to handle tricky questions of authenticity involving electronically stored information); *In re* F.P., 878 A.2d 91, 95 (Pa. Super. Ct. 2005) ("We believe that e-mail messages and similar forms of electronic communication can be properly authenticated within the existing framework of PA. R.E. 901 and Pennsylvania case law."). Steven Goode, *The Admissibility of Electronic Evidence*, 29 REV. LITIG. 1, 2 (2009) ("the current framework provided by the rules of evidence is adequate to the task"). *But see* Robbins, *supra* note 8, at 36. (advocating a shift in focus from account ownership and content to authorship of the evidence); Neil C. Magnuson & Bennett B. Borden, *The Admissibility of Digital Evidence*, 8 ABA SCITECH L. 4 (2011) (noting the "need for a more robust and reliable approach to authentication"); Moore, *supra* note 53, at 177–178, 181 (advocating for changes in the rules of authentication , hearsay, and best evidence to accommodate the "unique issues presented by ESI [electronically stored material] and that Rule 901(b) should also be amended to explicitly incorporate the use of technology as a method of authentication").

108. *See* Goode, *supra* note 107, at 6 ("While electronic evidence does not present any particularly difficult analytical problems in terms of the law of evidence, it does pose some very real practical problems.") (footnotes omitted); Jaksic, *supra* note 45 (quoting John Palfrey, executive director of The Berkman Center for Internet & Society at Harvard Law School: "There is a sense that this information would be admissible if it's verifiable, as with any other form of electronic discovery. The one issue is going to be authentication as far as what is said online and who said it."); Democko, *supra* note 1, at 371 ("[E]nacting new rules governing the authentication of electronic evidence, or specifically, evidence from social networking sites, is not only unnecessary, but counterproductive.").

109. FED. R. EVID. 901(a). This question is one of conditional relevance under FED. R. EVID. 104(b).

110. *See Lorraine*, 241 F.R.D. at 539 (discussing a "two-step process" for authentication).

the jury's revisiting of the authenticity question.[111] As the notes to the California Evidence Code explain:

> . . . the fact that the judge permits [a] writing to be admitted in evidence does not necessarily establish the authenticity of the writing; all that the judge has determined is that there has been a sufficient showing of the authenticity of the writing to permit the trier of fact to find that it is authentic.[112]

For example, in a case involving a contract on which the defendant claims his signature has been forged, the judge first considers the question of authentication. If no chance exists that it is the defendant's signature, then the document has no relevance, and the judge will keep it from the jury. Generally, however, if a legitimate question exists, the authenticity of the signature will next go to the jury, especially if it is an ultimate issue in the case. In construing and applying Rule 901, federal courts hold that "a document is properly authenticated if a reasonable juror could find in favor of authenticity."[113]

The authentication rules are by their structure not very rule-like. In the Federal Rules of Evidence, various illustrations, "examples only—not a complete list,"[114] follow the very general principle that the item must be what its proponent claims. Under the Rules, the relevant examples for methods of authentication include testimony of a witness with knowledge[115] and distinctive characteristics.[116] Unlike hearsay, which is very technical and categorical,[117] authentication is ultimately more flexible and practical, but less uniform and predictable.

Evidence law is conservative by nature and slow to adapt to new forms of technology.[118] Professor Jennifer Mnookin has written about the fascinating process by which courts slowly grew accustomed to the use of the

111. *Id.* at 539–40 (explaining that the court first determines whether the proponent has offered evidence from which the jury could reasonably find the evidence authentic and that the jury next decides authenticity as a matter of conditional relevance).

112. People v. Valdez, 135 Cal. Rptr. 3d 628, 633 (Ct. App. 2011) (citing CAL. EVID. CODE § 1400 (West 1995) (alteration in original)).

113. United States v. Gagliardi, 506 F.3d 140, 151 (2d Cir. 2007) (citing United States v. Tin Yat Chin, 371 F.3d 31, 38 (2d Cir. 2004)).

114. FED. R. EVID. 901(b). This loose structure of the authentication rules raises the odd question whether it is possible to "violate" an example.

115. FED. R. EVID. 901(b)(1) ("Testimony of a Witness with Knowledge: Testimony that an item is what it is claimed to be.")

116. FED. R. EVID. 901(b)(4) ("Distinctive characteristics and the Like: The appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances."). *See* People v. Fielding, No. C-062022, 2010 WL 2473344, at *4 (Cal. Ct. App. June 18, 2010) ("Documents may be authenticated in various ways. 'Circumstantial evidence, content and location are all valid means of authentication.' " (quoting People v. Gibson, 90 Cal. App. 4th 371, 383 (2001)).

117. Eleanor Swift, *A Foundation Fact Approach to Hearsay*, 75 CALIF. L. REV. 1339 (1987).

118. Goode, *supra* note 107, at 4 (2009) (discussing admissibility of photographs, audio recordings, and computer records, noting that "[o]ur jurisprudence is littered with examples of courts confronting the admissibility of evidence based on new technologies, and courts have reacted in a predictable pattern. At first, new technologies meet with judicial resistance.").

photograph as courtroom evidence.[119] In 1899, one court refused to admit photographs because " 'either through want of skill on the part of the artist, or inadequate instruments or materials, or through intentional and skillful manipulation, a photograph may be not only inaccurate, but dangerously misleading.' "[120] The now quaint-seeming opposition to photographs as evidence that parties cannot authenticate is eerily reminiscent of some of the current suspicions regarding the Internet and social media. In both cases, judges express concerns that through the "intentional and skillful manipulation"[121] of the proponent, jurors may be deceived by fakery and clever mock-ups.

B. Photographs

Ironically, social media raises few problems on the issue of photographs. The process of authenticating a photo from Twitter, MySpace, or Facebook is indistinguishable from authenticating a photo generally. A witness with knowledge must testify that the photograph is a fair and accurate representation of what it purports to be.[122] For instance, imagine someone were to snap a shot of a parent dancing naked on a bar with an alcoholic drink in hand and subsequently posted it on Facebook. In a custody dispute, if the dancer's ex-spouse wished to introduce the photo as evidence of alcoholism and bad judgment, anyone at the scene could authenticate the photo by testifying that it was a fair and accurate representation of the events of the evening in question.

Recently, commentators have raised questions about authenticating digital photographs because of the ease of altering or "photoshopping" them.[123] Such techniques for detecting alteration in digital photography

119. Jennifer L. Mnookin, *The Image of Truth: Photographic Evidence and the Power of Analogy*, 10 YALE J.L. & HUMAN. 1, 4 (1998) ("[P]hotography was recognized, almost from the time of its invention, as a potentially powerful juridical tool—perhaps even a dangerously powerful tool. The meaning and epistemological status of the photograph were intensely contested, both inside and outside the courtroom. Furthermore, the history of the legal use of photography is intimately intertwined with the history of photographic technologies.").

120. Goode, *supra* note 107, at 4 (quoting Cunningham v. Fair Haven & W. R. Co., 43 A. 1047, 1049 (Conn. 1899)).

121. *Id.*

122. EDWARD J. IMWINKELRIED, EVIDENTIARY FOUNDATIONS § 4.09(1) (7th ed. 2008) ("Modernly, the prevailing view is that any person familiar with the scene or object depicted may verify the photograph.").

123. *See* Zachariah B. Parry, Note, *Digital Manipulation and Photographic Evidence: Defrauding the Courts One Thousand Words at a Time,* 2009 U. ILL. J.L. TECH. & POL'Y 175 (noting the relative ease, low cost, and difficulty of detection where digital photographs are altered); Jill Witkowski, Note, *Can Juries Really Believe What They See?: New Foundational Requirements for the Authentication of Digital Images,* 10 WASH. U. J.L. & POL'Y 267 (2002) (explaining the dangers of altering digital photography and proposing changes to the authentication process). *See also* Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 561 (D. Md. 2007) (explaining that digital photographs present unique authentication problems because they are a form of electronically produced evidence that may be manipulated and altered).

are becoming increasingly sophisticated and inexpensive,[124] and valid concerns can be raised when digital images are enhanced.[125] To the extent that manipulation of digital photos is a problem, it is one not unique to social media, but rather represents a problem with digital photography generally. When faced with an authentication concern, one court noted: "Here, it was Jessica herself who acknowledged that indeed, she had been drinking alcohol and the pictures accurately reflected that activity. That testimony was sufficient to authentic the photographs and they were properly admitted into evidence."[126]

Nevertheless, one recurrent use of photographs from social networking has posed a conundrum for courts. Often, parties wish to demonstrate the gang affiliation of a witness or an opposing party.[127] The State of California, in a guide entitled *A Parent's Guide to Gangs*, explains that "[g]ang members often communicate, recruit, socialize and sell drugs using the Internet and publish their own web page to show off their gang affiliation (MySpace, Bebo, Facebook, etc.)."[128] Some gang members begin their taunting and fighting on social media, post the video of the fight online, and then brag about it.[129] This has obvious benefits for police investigations,[130] but the question here is: how can these postings on Facebook, Twitter, MySpace, etc., be used in court to demonstrate gang affiliation? Setting aside the question of character evidence[131] and unfair prejudice,[132]

---

124. *See* Chris Gaylord, *Digital Detectives Discern Photoshop Fakery: New Software Combs for Clues in al Qaeda Tapes, Harry Potter Pages, and Celebrity Waistlines*, CHRISTIAN SCI. MONITOR (Aug. 29, 2007), http://www.csmonitor.com/2007/0829/p13s02-stct.html (discussing techniques for spotting doctored photos); Mark L. Hoffman and Jesse Epstein, *Image Manipulation and the Rules of Evidence: The Admission of Digital Images and the Race to Detect Forgeries*, 2 ANN. 2008 AAJ-CLE 1881 (2008) (describing techniques for how to spot doctored photographs).

125. *Lorraine*, 241 F.R.D. at 561–62.

126. Lalonde v. Lalonde, No. 2009-CA-002279-MR, 2011 WL 832465, at *2 (Ky. Ct. App. Feb. 25, 2011) ("[A]lthough we acknowledge that modern digital photography techniques may allow for the alteration of a photograph, Jessica did not suggest such techniques were employed. She instead acknowledged the photographs were accurate which leads to the conclusion they were not altered.").

127. *See, e.g.*, BROWNING, *supra* note 1, at 57 (discussing introduction of MySpace page to show gang affiliation, thereby influencing bail determination).

128. CAL. ATTORNEY GEN. OFFICE, A Parent's Guide to Gangs 12, *available at* http://www.calgrip.ca.gov/documents/Parents_Gangs_Hdbk.pdf.

129. *See* Scott Gutierrez, *Street Gang Using Internet for Violent Bragging Rights; Masked Hoodlums Making Threats at MySpace, Other Sites*, SEATTLE PI (July 09, 2006, 10:00 PM, http://www.seattlepi.com/local/article/Street-gangs-using-Internet-for-violent-bragging-1208477.php (citing a MySpace page where a gang member points guns, flashes gang signs, and congratulates a fellow gang member for beating someone up, writing: "I hope your hands feel a little better. I will get the video to you of what you did to that guy. Keep it up babe boy.")

130. *See* Thomas Watkins, *Gangs Use of Twitter, Facebook on the Rise*, HUFFINGTON POST (Feb. 2, 2010, 2:24PM), http://www.huffingtonpost.com/2010/02/02/gangs-use-of-twitter-facebook_n_445551.html (noting increased use of social media for gang communication and that concomitant police monitoring has led to arrests).

131. The Federal Rules prohibit the use of character evidence to prove propensity. FED. R. EVID. 404(a). However, gang affiliation might be relevant to demonstrate motive or intent, which is a permissible use of such evidence. So it is permissible to use evidence of other acts to show motive or intent, and gang affiliation might be relevant for such other purposes. *See* FED. R. EVID. 404(b) (permitting evidence of other acts to show motive or intent).

how is a photograph of a person flashing a gang symbol to be authenticated on a networking site?

In *United States v. Cole*,[133] the accused claimed no knowledge of a drug conspiracy. To show that he was a member of the Latin King gang and knew the nature of the conspiracy, the government was allowed to present evidence concerning Cole's web page on MySpace.[134] His web page yielded evidence including photos depicting him wearing Latin King colors, Cole's listing of "drug wars" as a personal interest, and additional photos depicting Latin King members and Latin King symbols.[135] It is unclear whether the accused took the stand or whether any authentication questions were even raised about the MySpace page.

In *People v. Lenihan*,[136] the accused challenged his second-degree murder conviction by arguing that he was unfairly prohibited from cross-examining two state witnesses with photographs his mother had printed from MySpace that allegedly depicted the witnesses and the victim making hand gestures and wearing clothing suggesting affiliation with the Crips gang.[137] The New York appellate court approved the trial court's refusal to allow the defendant to admit the witness's MySpace photos as a basis for cross-examination.[138] The court reasoned that because the defendant had no idea who took the photos and under what circumstances they were taken, "[i]n light of the ability to 'photo shop', or edit photographs on the computer, the defendant could not authenticate the photographs."[139] Additionally, the Court was persuaded that the photos did not establish a good-faith basis for cross-examining the witnesses because the connection to the defendant was too remote and speculative, given that defendant denied being a member of a rival gang.[140] Similarly, in *People v. Beckley*,[141] the court held that the trial court erred in admitting the evidence of the defendant flashing a gang symbol on her MySpace page because "with the advent of computer software programs such as Adobe Photoshop it does not always take skill, experience, or even cognizance to alter a digital photo."[142] Apparently, the court required someone who was present at the time the photo was taken to testify that it accurately depicted what it purported to show.[143] The admission of the evidence, however, was deemed harmless error.[144]

132. Even if admissible under Rule 404, Rule 403 presents another hurdle, excluding the evidence of gang affiliation if the probative value of that evidence is significantly outweighed by its probative value. *See* FED R. EVID. 403.

133. 423 F. App'x 452 (5th Cir. 2011).

134. *Id.* at 456.

135. *Id.* at 457.

136. 911 N.Y.S.2d 588 (App. Div. 2010).

137. *Id.* at 591.

138. *Id.* at 592.

139. *Id.*

140. *Id.*

141. 110 Cal. Rptr. 3d 362 (Ct. App. 2010).

142. *Id.* at 367 (quoting Parry, *supra* note 123, at 183).

143. *Id.* (quoting People v. Bowley, 59 Cal. 2d 855, 859 (1963)).

144. *Id.*

In both *Cole* and *Lenihan*, the courts' emphasis on the technology and the photographer seems misplaced. The photos of individuals flashing gang signs should have been admissible if a person with knowledge had been at the event. Arguably, anyone who had seen the individual do so could testify that these photos were a fair and accurate representation of what the person looked like using gang signs. In the *Lenihan* case, which involved cross-examination of a prosecution witness, the witness himself could have served as a person with knowledge, and the accused should at least have been able to pose initial questions to see if the MySpace page could be authenticated.

C. Authenticating Posts, Updates, and Tweets

Even more difficult than the issues surrounding authenticating photographs are the authentication questions concerning written posts, messages, and tweets on social networks. The initial response from courts has been mixed. Back in 1999, in *St. Clair v. Johnny's Oyster & Shrimp, Inc.*,[145] a court opined: "There is no way Plaintiff can overcome the presumption that the information he discovered on the Internet is inherently untrustworthy. Anyone can put anything on the Internet . . . Hackers can adulterate the content on any website."[146] Thirteen years later, one can still find courts that are extremely wary of the new-fangled ways that young people communicate.[147] One can also find contrary examples, however, where the courts, though aware of potential problems with authentication, nevertheless allow the admission of remarks transmitted via social media.

Courts generally address four types of authentication concerns: (1) general lack of proper foundation; (2) the possibility that the entire social networking page is a fake;[148] (3) the possibility that a genuine existing page has been hacked; and (4) the possibility that someone has appropriated the site of another by obtaining the password through friendship, phishing,[149] or a computer left logged on and unattended in a place where third parties could post in the owner's name.[150]

Tweets, MySpace pages, and Facebook posts are not self-authenticating, as are, for instance, some certified public documents.[151] Certainly,

145. 76 F. Supp. 2d 773 (S.D. Tex. 1999).

146. *Id.* at 774–75.

147. *See* Uncel, *supra* note 2, at 44 ("Some courts, however, are making it difficult to admit social networking evidence because of their doubts that such evidence is authentic.").

148. *Cf.* Moore, *supra* note 53, at 148 (discussing the "unique authentication concerns" created by "the potential for the easier alteration or fabrication of ESI [electronically stored evidence] than traditional forms of physical evidence").

149. "Phishing is a way of attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication." *Phishing*, WIKIPEDIA, http://en.wikipedia.org/wiki/Phishing (last visited June 24, 2012).

150. Tienda v. State, 358 S.W.3d 633, 641–42 (Tex. Crim. App. 2012) (noting that "the provenance of such electronic writings can sometimes be open to question—computers can be hacked, protected passwords can be compromised, and cell phones can be purloined . . . .").

151. *See generally* FED. R. EVID. 902; State v. Eleck, 23 A.3d 818, 821 n.4 (Conn. App. Ct. 2011) (noting that the proponent of the evidence did not and could not argue that the Facebook messages were self-authenticating). *Cf.* Commonwealth v. Purdy, 945 N.E.2d 372 (Mass. 2011) (holding that

judges cannot just accept a piece of paper, printed out from a computer, and treat it as authentic without more (though I suspect this happens frequently in some courts, particularly with pro se litigants in domestic disputes). Authentication is easy where the party admits that the page is hers and she made the post, as this fairly comports with the example of authentication by a person with knowledge. But what if the alleged poster is not a party, or is a party who does not take the witness stand (such as where she exercises her right against self-incrimination) or simply denies the post as her own? Courts struggling with these questions have reached very different results.

1. The Stricter Approach

In *Griffin v. State*,[152] the Maryland Supreme Court, in a long opinion, reversed and remanded a conviction, holding that pages from MySpace admitted against the accused were not properly authenticated. The State sought to introduce the MySpace profile of the accused's girlfriend to demonstrate that she threatened another witness, who had significantly changed his testimony upon retrial.[153] The accused's girlfriend was not questioned about the pages.[154] Instead, the State attempted to authenticate the pages as belonging to her through the testimony of the lead investigator in the case.[155] The trial judge allowed the investigator to testify in support of authentication because the page (1) contained the photograph of a person who looked like the girlfriend, (2) used the nickname "Boozy" for her boyfriend, a known nickname of the accused, (3) included the girlfriend's date of birth, and (4) contained the post: "FREE BOOZY!!!! JUST REMEMBER SNITCHES GET STITCHES!! U KNOW WHO YOU ARE!!"[156] In authenticating the threat, the trial court reasoned that the posting contained identifying factors and information that only a few people would know and was posted from her regular social media address.[157]

The Maryland Supreme Court reversed, explaining that "[t]he identity of who generated the profile may be confounding, because 'a person observing the online profile of a user with whom the observer is unacquainted has no idea whether the profile is legitimate.'"[158] The court fretted that

evidence that electronic communication originates from e-mail or social networking website that bears purported author's name is not sufficient alone to authenticate it).

152. 19 A.3d 415, 418 (Md. 2011), *rev'g* 995 A.2d 791 (Md. Ct. Spec. App. 2010). The Maryland Supreme Court applied MD. EVID. R. 5–901, which is identical to the Federal Rule. *See supra* notes 96–102 and accompanying text.

153. *Griffin*, 19 A.3d at 418.

154. *Id.*

155. *Id.*

156. *Id.*

157. Griffin v. State, 995 A.2d 791 (Md. Ct. Spec. App. 2010).

158. Griffin v. State, 19 A.3d 415,421 (Md. 2011) (citing Nathan Petrashek, Comment, *The Fourth Amendment and the Brave New World of Online Social Networking*, 93 MARQ. L. REV. 1495, 1499 n.16 (2010)). This sounds suspiciously like the famous NEW YORKER cartoon, depicting a dog at the computer with the caption, "On the internet, nobody knows you're a dog." *See On the Internet, nobody knows you're a dog*, WIKIPEDIA, http://en.wikipedia.org/wiki/On_the_Internet,_nobody_knows_you're_

"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."[159] The Court therefore found that 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."[160]

The Maryland Supreme Court also stated that an inadequate foundation was laid for authenticating the MySpace page because the State failed to offer any extrinsic evidence describing MySpace, explain how the investigator obtained the MySpace pages at issue, or adequately authenticate the MySpace profile and the posting as belonging to the accused's girlfriend. The Court took seriously the prospect that "someone other than the alleged author may have accessed the account and posted the message in question" and "that another user could have created the profile in issue or authored the 'snitches get stitches' posting."[161] The girlfriend's picture, coupled with her birth date and location, were not deemed sufficiently "distinctive characteristics" to authenticate the printout from the MySpace account, given the possibility that the girlfriend might not have made the page in the first place.[162]

The *Griffin* majority suggested what would constitute adequate forms of authentication, noting that the "first, and perhaps most obvious method would be to ask the purported creator if she indeed created the profile and also if she added the posting in question."[163] Second, the court suggested searching the computer of the person who allegedly owns the page or made the posting "to determine whether that computer was used to originate the social networking profile and posting in question."[164] Third, the court suggested "obtain[ing] 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."[165]

Two judges dissented in *Griffin,* arguing that the MySpace page was adequately authenticated. The dissenters believed that a reasonable juror could conclude, based on the picture, birthday, and references to freeing

---

a_dog (last visited June 24, 2012). Since the year 2000, this is the magazine's most reproduced cartoon. *Id.*

159. *Id.* at 421.

160. *Id.* at 422.

161. *Id.* at 423 (citing Griffin v. State, 995 A.2d 791, 805 (Md. Ct. Spec. App. 2010)).

162. *Id.* at 424 ("[A] printout of an image from such a site requires a greater degree of authentication than merely identifying the date of birth of the creator and her visage in a photograph on the site in order to reflect that [the girlfriend] was its creator and the author of the 'snitches get stitches' language.").

163. *Id.* at 427.

164. *Id.*

165. *Id.* at 428 (citing People v. Clevenstine, 891 N.Y.S.2d 511, 514 (App. Div. 2009) (describing a case where an investigator from the computer crime unit of the State Police testified that "he had retrieved such conversations from the hard drive of the computer used by the victims")). The Court seems unaware that MySpace and Facebook will only certify ownership of a page and will not validate individual postings. Searching a hard drive is something different altogether.

"Boozy," that the redacted printed pages of the MySpace profile demonstrated sufficiently distinct characteristics to demonstrate that they were what the prosecution claimed them to be.[166] The dissent explained its view that "[t]he technological heebie jeebies discussed in the Majority Opinion go . . . not to the admissibility of the print-outs . . . but rather to the weight to be given the evidence by the trier of fact."[167] The dissent also noted that "[t]he potentialities that are of concern to the Majority Opinion are fit subjects for cross-examination or rebuttal testimony."[168]

Commonwealth v. Williams[169] provides another example of a strict approach to authentication of social media. In *Williams,* the Supreme Judicial Court of Massachusetts would not admit instant messages a witness had received through her account on MySpace.[170] The witness testified that the defendant's brother had contacted her "four times on her MySpace account . . . urging her not to testify . . . or to claim a lack of memory regarding the events of the night of the murder."[171] At trial, the witness testified that the accused's brother had a picture of himself on his MySpace page, she recognized his MySpace screen (from which she had previously received messages), and the document printed from her MySpace account indicated that the messages were in fact sent by a user with the brother's same screen name and picture.[172] The Supreme Judicial Court of Massachusetts held that the State had laid an inadequate foundation to authenticate the MySpace messages because it failed to offer any evidence regarding who had access to the MySpace page and whether another author could have posted the messages:

> Although it appears that the sender of the messages was using [the brother]'s MySpace Web "page," there is no testimony (from [the witness] or another) regarding how secure such a Web page is, who can access a MySpace Web page, whether codes are needed for such access, etc. . . . Here, while the foundational testimony established that the messages were sent by someone with access to Williams's MySpace Web page, it did not identify the person who actually sent the communication. Nor was there expert testimony that no one other than Williams could communicate from that Web page.[173]

166. *Id.* at 429–30 (Harrell, J., dissenting) ("As long as a reasonable juror could conclude that the proffered evidence is what its proponent purports it to be, the evidence should be admitted.").

167. *Id.* (footnotes defining "heebie jeebies" omitted).

168. *Id.*

169. 926 N.E.2d 1162 (Mass. 2010).

170. *Id.* at 1171.

171. *Id.* at 1172.

172. *Id.*

173. *Id.* at 1172–73 (citations omitted). Similarly, in *United States v. Jackson*, the accused was charged with mail and wire fraud and obstruction of justice after making false claims of racial harassment against the United Parcel Service. 208 F.3d 633 (7th Cir. 2000). At trial, the accused tried to admit postings from "the Euro-American Student Union and Storm Front," in which the white supremacist groups gloated about Jackson's case and took credit for the UPS mailings. *Jackson*, 208 F.3d at

A final example of some courts' hesitancy in authenticating written posts from social media comes from Connecticut. In *State v. Eleck*,[174] the trial court excluded evidence that the accused wished to introduce from his Facebook account documenting messages sent to him from a key witness for the State.[175] The witness acknowledged that the message was sent from her Facebook account but denied that she had done it. She testified that someone had hacked into her account and changed her Facebook password.[176] The court expressed skepticism about her account being hacked, noting that "this suggestion is dubious under the particular facts at hand, given that the messages were sent before the alleged hacking of the account took place."[177] Furthermore, immediately after being questioned about her post in court, the witness removed the accused from her list of Facebook friends.[178] Despite doubting the hacking event mentioned by the witness, the court nevertheless found the refusal to authenticate the witness's post within the trial court's discretion. The court in *Eleck* explained:

> The need for authentication arises in this context because an electronic communication, such as a Facebook message, an e-mail or a cell phone text message, could be generated by someone other than the named sender. This is true even with respect to accounts requiring a unique user name and password, given that account holders frequently remain logged in to their accounts while leaving their computers and cell phones unattended. Additionally, passwords and website security are subject to compromise by hackers. Consequently, proving only that a message came from a particular account, without further authenticating evidence, has been held to be inadequate proof of authorship.[179]

Given these authenticity concerns, "it was incumbent on the defendant, as the proponent, to advance other foundational proof to authenticate that the proffered messages did, in fact, come from [the witness] and not simply from her Facebook account."[180] The court found that mere proof of ownership was insufficient unless supplemented by authentication via identifying characteristics, which would have had to have been much

637. The court affirmed the trial court's refusal to admit the web page because it lacked an appropriate foundation; the accused did not demonstrate that the web postings "actually were posted by the groups, as opposed to being slipped onto the groups' websites by Jackson herself, who was a skilled computer user." *Id.* at 638.

174. 23 A.3d 818 (Conn. App. Ct. 2011).

175. *Id.* at 820. The witness testified that the accused stated before the fight that "if anyone messes with me tonight, I am going to stab them." *Id.*

176. *Id.*

177. *Id.* at 824.

178. *Id.* at 821.

179. *Id.*at 822.

180. *Id.* at 824.

more distinctive than the general conversation regarding past friction between the two.[181]

2. A More Liberal Approach

In *State v. Yates*,[182] the State introduced postings from a MySpace account named "Murdaman Flocka" that the State demonstrated was created and used by Yates. A representative from MySpace.com testified as to the creation of the account, giving the date it was established with the email of the accused.[183] The State also presented testimony from a witness whose photograph was included on the MySpace page, supporting the contention that it was Yates's MySpace account. The profile information, the picture of Yates as the account holder, and the use of the accused's email were also indicative of its being Yates's account. According to the appellate court, the MySpace postings "connected Yates to the shootings and disclosed his feelings of betrayal and being 'pissed off' by people talking to the police."[184] The court rejected the accused's argument that the State failed to properly authenticate the MySpace posting and establish that the postings belonged to him. The court noted that the authentication standard of evidence sufficient to support a finding "is not rigorous, and the threshold of admissibility articulated in it is low."[185] The court concluded that "Yates's contention that anyone could have created the postings goes to the weight of the evidence that the jury should consider."[186]

In *People v. Valdez*,[187] the California Appellate Court affirmed the authentication of the accused's MySpace page without verification from the provider.[188] The page displayed a picture of the accused's face and included greetings from friends and family members by name. The page contained a list of interests, which included gangs.[189] The court explained, with an ironic, dismissive tone, that "[t]his suggested the page belonged to Valdez, rather than someone else by the same name, who happened to look just like him."[190] The court acknowledged that the accused was free to argue otherwise to the jury but concluded that "a reasonable trier of fact could conclude from the posting of personal photographs, communications, and other details that the MySpace page belonged to him."[191]

In *Tienda v. State*,[192] the Texas Court of Criminal Appeals affirmed the trial court's authentication of the MySpace pages of an alleged murderer,

181. The court provided this example: when the accused sent the message asking, "why would you wanna talk to me," the other party (allegedly the witness) replied, "The past is the past." *Id.* at 820 n.2.

182. No. 96774, 2012 WL 759201 (Ohio Ct. App. March 8, 2012).

183. *Id.* at *6.

184. *Id.* at *1.

185. *Id.* at *6 (citations omitted).

186. *Id.* (citations omitted).

187. 135 Cal. Rptr. 3d 628 (Ct. App. 2011).

188. *Id.* at 633.

189. *Id.*

190. *Id.*

191. *Id.*

192. 358 S.W.3d 633 (Tex. Crim. App. 2012).

Ronnie Tienda. The pages were originally brought to the prosecution's attention by the victim's sister.[193] The State admitted the pages through the testimony of the victim's sister.[194] The prosecutor also offered affidavits and subscriber reports associated with each profile account that it subpoenaed from MySpace.[195] The subscriber reports indicated that the MySpace accounts were created by a "Ron Mr. T" or "Smiley Face" (the appellant's nickname).[196] The account holder wrote that he lived in "D TOWN" or "dallas" (as did the accused) and registered the accounts with a "ronnietiendajr@" or "smileys_shit @" email address.[197] The page included a mention of the deceased with the comment "RIP David Valadez" linked to a song that was played at the victim's funeral.[198]

Instant message comments exchanged between the MySpace page holder and other MySpace users included specific references to the shooting and subsequent investigation.[199] The messages made specific reference to snitches, and the MySpace page owner complained about his electronic monitor, which was a condition of his house arrest pre-trial.[200] Tienda denied that the pages were his. In cross-examining the deceased's sister, "defense counsel elicited testimony regarding the ease with which a person could create a MySpace page in someone else's name and then send messages, purportedly written by the person reflected in the profile picture, without their approval."[201] The defense emphasized the prosecution's failure to prove through any technological or expert evidence that the appellant created the account.[202]

In affirming the admissibility of the MySpace pages, *Tienda* began by reviewing the generally low standard for authentication:

> In performing its Rule 104 gate-keeping function, the trial court itself need not be persuaded that the proffered evidence is authentic. The preliminary question for the trial court to decide is simply whether the proponent of the evidence has supplied facts that are sufficient to support a reasonable jury determination that the evidence he has proffered is authentic.[203]

The court held that "the internal content of the MySpace postings—photographs, comments, and music—was sufficient circumstantial evidence

193. *Id.* at 635.
194. *Id.*
195. *Id.*
196. *Id.*
197. *Id.*
198. *Id.*
199. *Id.*
200. *Id.* at 636.
201. *Id.*
202. *Id.* There was no attempt, for instance, to trace the IP address listed in the subscriber report to the appellant's personal computer. *Id.*
203. *Id.* at 638.

to establish a prima facie case such that a reasonable juror could have found that they were created and maintained by the appellant."[204] In what can only be read as a sarcastic critique of the accused's objections and the timidity of courts[205] that have been more grudging in their willingness to authenticate such pages, the court observed:

> It is, of course, within the realm of possibility that the appellant was the victim of some elaborate and ongoing conspiracy. Conceivably some unknown malefactors somehow stole the appellant's numerous self-portrait photographs, concocted boastful messages about [the victim's] murder and the circumstances of that shooting, was aware of the music played at [the victim's] funeral, knew when the appellant was released on pretrial bond with electronic monitoring and referred to that year-long event along with stealing the photograph of the grinning appellant lounging in his chair while wearing his ankle monitor. But that is an alternate scenario whose likelihood and weight the jury was entitled to assess once the State had produced a prima facie showing that it was the appellant, not some unidentified conspirators or fraud artists, who created and maintained these MySpace pages.[206]

Finally, in *People v. Fielding*,[207] a twenty-one year-old woman who was being prosecuted for having sex with a fourteen-year-old boy objected to the admission of their message exchanges on MySpace. The victim's father testified that he had printed all the communications between his son and the defendant from his son's MySpace account and did not alter them.[208] The accused argued that the messages were not sent by her and questioned the accuracy of the printouts that the boy's father had printed from the boy's computer, arguing it was possible to edit the conversations. This claim was bolstered by the fact that some conversations were not fully reproduced, and that the victim's MySpace page had once been hacked.[209] The court noted "the fact that a document was or may have been altered does not preclude a preliminary finding of authenticity, where the claimed alterations are immaterial."[210] The court also credited the testimony of the

204. *Id.* at 642.

205. The court in *Tienda* addressed and specifically disagreed with the State of Maryland's approach in *Griffin*. *See supra* notes 188–201 and accompanying text.

206. *Id.* at 645–46.

207. No. C-062022, 2010 WL 2473344 (Cal. Ct. App. June 18, 2010).

208. *Id.* at *2.

209. *Id.* at *3 (accused argued that "the packet of exchanges prepared by the victim's father was incomplete and inaccurate. For example, in the exchange which shows that she said she wanted to have sex, the victim erased her message, wrote a new message, and then replied to it. Other exchanges were not reproduced fully."). On cross-examination, the victim conceded that someone had "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.' " *Id.* at *4.

210. *Id.* at *5 (citations omitted).

victim, who recognized the conversations on MySpace; the victim claimed he knew it was the accused because he was often "talking on the phone to her at the same time."[211] Ultimately, the court concluded that "the possibility that the incriminating messages purportedly coming from defendant were in fact sent or posted by someone else went to the weight of the evidence, not its admissibility."[212] In answer to a concern about ownership of the page, the trial court noted the defense could subpoena records from MySpace.[213]

3. Potential Analogues to Authenticating Social Media—Authenticating Other Types of Evidence

In *Lorraine*, a long opinion full of dicta setting out the requirements of various forms of authentication, Judge Grimm rightly observed that "any serious consideration of the requirement to authenticate electronic evidence needs to acknowledge that, given the wide diversity of such evidence, there is no single approach to authentication that will work in all instances."[214] Although each form of electronic communication presents its own authentication conundrums, it is useful to try to draw analogies among various forms of evidence, particularly electronic evidence.[215]

Courts have considerably more experience with authenticating phone call and emails (and, to a lesser extent, instant messages) than they do with social media.[216] Each type of communication presents possible templates for the authentication of Facebook pages and other social networking cites.

Like social media, phone calls and emails involve a level of anonymity and the potential for impersonation.[217] The example for authenticating a telephone call in the Federal Rules of Evidence requires an assigned number and either self-identification of the person or a call to a business for business-related transactions.[218] In *Williams*,[219] the court analogized a message on MySpace to a telephone call, and noted that:

---

211. *Id.* at *4. (At a pretrial hearing, the victim "testified he had had a MySpace account since he was 12 years old, and defendant was a 'friend' on his page between September and December 2007" and "identified pages of copied messages dated between September and December 2007, exchanged between himself and defendant, via their MySpace accounts.").

212. *Id.* at *5.

213. *Id.* at *3.

214. Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 553–54 (D. Md. 2007).

215. The history of photograph authentication reveals courts' tendencies to engage in analogic reasoning, searching for what social media is most similar to among the types of evidence that we already know how to authenticate. *See* Mnookin, *supra* note 119. Professor Mnookin makes a persuasive case that the analogies have transformative effects in both directions, changing understanding not only of the novel entity, but also the types of evidence it was compared to that formed the basis for the analogy. *Id.* at 74. In this moment of great flux, where courts are divided on the questions of authenticating social media, it will be interesting to see how phone calls and emails are used as analogies and how, in turn, authentication of social media may alter how these relatively accepted forms of evidence are authenticated.

216. *See* Democko, *supra* note 1 (drawing the analogy to email and instant messaging).

217. *See* Uncel, *supra* note 2, at 60–61 (drawing analogies regarding authenticating social media to authenticating phone conversations and emails).

218. FED. R. EVID. 901(b)(6).

219. 926 N.E.2d 1162 (Mass. 2010).

> a witness's testimony that he or she has received an incoming call from a person claiming to be 'A,' without more, is insufficient evidence to admit the call as a conversation with 'A.' Here, while the foundational testimony established that the messages were sent by someone with access to Williams's MySpace Web page, it did not identify the person who actually sent the communication.[220]

The *Williams* analysis is faulty. If we know someone is calling from his own phone (something easily accomplished with caller ID) and self-identifies when he calls (e.g., "Hi, this is Bob."), that would be sufficient under Rule 901(b)(6) to authenticate the phone call. A posting on Bob's Facebook page actually provides more points of identification such as photos, birth date, geographic information, and time stamp.

Another potential analogy is to email, a form of electrically stored information with which judges are probably more familiar. Emails tend to be authenticated by their distinctive characteristics, such as content displaying familiarity with people and events that its purported authors know. Also, the timeline of email exchanges may correlate with other established events.[221] Metadata[222] embedded in the email also can trace its provenance. Finally, when the email involves a reply, it is reasonable to assume that the replying writer is authentically the sender, since the original writer will recognize the original email content and be able to explain where he

220. *Id.* at 1172–73.

221. *See* Massimo v. State, 144 S.W.3d 210 (Tex. App. 2004) (authenticating email because, among other reasons, it was sent to the email address of the victim claiming harassment shortly after a physical fight, and it referenced the physical fight); Fenje v. Feld, 301 F. Supp. 2d 781, 809 (N.D. Ill. 2003) ("E-mail communications may be authenticated as being from the purported author based on an affidavit of the recipient; the e-mail address from which it originated; comparison of the content to other evidence; and/or statements or other communications from the purported author acknowledging the e-mail communication that is being authenticated.").

222. Metadata is defined as "data providing information about one or more aspects of the data, such as:

- Means of creation of the data;
- Purpose of the data;
- Time and date of creation;
- Creator or author of data;
- Location on a computer network where the data was created; and
- Standards used.

For example, a digital image may include metadata that describes how large the picture is, the color depth, the image resolution, when the image was created, and other data. A text document's metadata may contain information about how long the document is, who the author is, when the document was written, and a short summary of the document." *Metadata*, WIKIPEDIA, http://en.wikipedia.org/wiki/Metadata (last visited June 24, 2012).

sent it.[223] The mere "from" on an email without more is probably insufficient to authenticate the email,[224] but additional information from "confirming circumstances,"[225] such as use of the proper password, attachments that help identify the sender, special language, non-public information, and metadata about the trail of the email can assist in authentication.[226] According to one Massachusetts court, claims of hacking email go to the weight and not the admissibility of email messages."[227] Social media, while sharing some attributes with phone calls and emails, have their own distinctive characteristics.[228] In some ways, social media seems more amenable to easy identification because they often contain date stamps and photos.

4. Which Approach is Better?

Judge Grimm, author of *Lorraine*'s long exegesis regarding admissibility of electronically stored information, argues that "the inability to get evidence admitted because of a failure to authenticate it almost always is a self-inflicted injury which can be avoided by thoughtful advance preparation."[229] Given some courts' strict approach to authenticating social media, I beg to differ. Although it is true much of the time that failure to prepare adequately can leave an attorney flat-footed when trying to authenticate a piece of evidence, in this time of transition when courts are only slowly accommodating to the new social media and new means of communication, some courts are unnecessarily grudging in authenticating information emanating from social networking sites.[230]

223. *See* Lorraine v. Markel American Ins. Co., 241 F.R.D. 534, 554–555 (D. Md. 2007). *See Massimo*, 144 S.W.3d at 216 (authentication of email because, among other reasons, victim had corresponded with accused at the same email address in the past). *Cf.* United States v. Macaluso, 460 F. App'x 862, 865 (11th Cir. 2012) (authenticating instant messenger chats between the accused and his victims "because the victims were able to testify to the contents.").

224. *See* Commonwealth v. Purdy, 945 N.E.2d 372, 378, 381 (Mass. App. Ct. 2011) ("Evidence that the defendant's name is written as the author of an e-mail or that the electronic communication originates from an e-mail or a social networking Web site such as Facebook or MySpace that bears the defendant's name is not sufficient alone to authenticate the electronic communication as having been authored or sent by the defendant.") (citations omitted). *Goode, supra* note 107, at 12 ("E-mail accounts can be used without the owner's permission. Therefore, the mere fact that an e-mail bears a particular e-mail address will often prove inadequate to authenticate the identity of the author; typically courts demand at least a little more evidence.").

225. *Purdy*, 945 N.E.2d at 381.

226. Goode, *supra* note 107, at 29 n.115 (citing IMWINKELRIED, *supra* note 122, at §4.03[4][b]). Professor Imwinkelried also provides detailed instruction on how to authenticate email messages using cryptography that require evidence that the user owns the key to unlock the cryptography and provides a sample foundation for proving the chain of custody for the handling of email by an email service). *Id.*

227. *Purdy*, 945 N.E.2d at 381–82. In *Purdy,* the email messages were actually found on the hard drive of the computer. *Id.*

228. *Cf.* Payne, *supra* note 8, at 842 (distinguishing information on social media from other electronically stored information for discovery purposes because evidence from social media is (1) more difficult to access, (2) personal, (3) inherently intimate and carries with it privacy implications, and (4) allows users to choose who can view their information).

229. 241 F.R.D. 534, 542 (D. Md. 2007).

230. Merritt, *supra* note 36, at 51–52 ("[J]udges approach social media evidence with trepidation. The anonymity of the internet, combined with the ephemeral nature of some communications, makes some judges wary of accepting social media statements at face value.").

Two procedural matters necessarily focus the debate. The first concerns the evidentiary standard for authentication. As the court in *Lorraine* observed: "A party seeking to admit an exhibit need only make a *prima facie* showing that it is what he or she claims it to be. This is not a particularly high barrier to overcome."[231] Unsurprisingly, the courts that are liberal in allowing authentication of social media emphasize this standard, which sets a very low bar for admission.[232]

Second, in understanding appellate court decisions, it is important to acknowledge that the standard of review is abuse of discretion. As the *Tienda* court explained: "If the trial court's ruling that a jury could reasonably find proffered evidence authentic is at least 'within the zone of reasonable disagreement,' a reviewing court should not interfere."[233] Technically, a reviewing court should only decide whether the trial court abused its discretion in making the authentication ruling. However, many courts seem to be taking the opportunity to explain their views of authentication, while leaving the status quo in place by resorting to the harmless error doctrine when they disagree with the trial court's ruling.

To analyze how courts may be making the authentication task more challenging than it should be, it is worth separating concerns about page ownership from concerns about hijacking of the page.

a. Page Ownership

Certainly, it makes sense that the proponent of the social network evidence somehow proves ownership of the page or profile in question. That can be done easily if the page owner is a witness. If the owner of the page is present, it is worth authenticating the page, at least so far as that the page exists and the witness created it.[234]

How should a party authenticate the ownership of the site when such ownership is denied by its purported creator or when the purported creator is not a witness who can be questioned? When the page owner does not testify from personal knowledge, other means of authentication include: (1) verification by the provider regarding who set up the page, (2) testimony of

231. Lorraine v. Markel American Ins. Co., 241 F.R.D. 534, 542 (D. Md. 2007); Dickens v. State, 927 A.2d 32, 37 (2007) (quoting United States v. Safavian, 435 F. Supp. 2d 36, 38 (D.D.C. 2006)) ("[T]he burden of proof for authentication is slight, and the court 'need not find that the evidence is necessarily what the proponent claims, but only that there is sufficient evidence that the *jury* ultimately might do so.' ") (emphasis in original).

232. *See, e.g.*, Ohio v. Bell, 882 N.E.2d 502, 512 (Ohio Ct. Com. Pl. 2008) (observing that that threshold for admissibility "is quite low—even lower than the preponderance of the evidence," and that "[o]ther jurisdictions characterize documentary evidence as properly authenticated if 'a reasonable juror could find in favor of authenticity.' ").

233. Tienda v. State, 358 S.W.3d 633, 638 (Tex. Crim. App. 2012) (quoting Montgomery v. State, 810 S.W.3d 372, 391 (Tex. Crim. App. 1991)). *See In re* F.P., 878 A.2d 91, 93 (Pa. Super. Ct. 2005) ("Admission of evidence is within the sound discretion of the trial court and will be reversed only upon a showing that the trial court clearly abused its discretion.").

234. Perhaps one reason for the strict standard of authentication in *Williams* was that the prosecution did not ask the witness herself about the MySpace page in question. *See supra* notes 169–73 and accompanying text.

an expert who found traces of the page on the purported owner's computer,[235] (3) statement of another witness with knowledge of the page or account's ownership, and (4) circumstantial evidence that the page belongs to its purported owner.

Parties can obtain provider verification with a warrant or a valid subpoena. The providers do not, however, verify the content of the site—they just verify who created the page.[236]

Verification from the provider and expert analysis of the owner's computer to establish ownership can be expensive and time-consuming. Because no other person may have first-hand knowledge of the page or account ownership, courts must decide whether social network pages can be authenticated via the circumstantial evidence of distinctive characteristics, as anticipated by Rule 901(b)(4). In *United States v. Grant*,[237] the court relied on Mil. R. Evid. 901(b)(4) to authenticate evidence via "[a]ppearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with the circumstances . . . ."[238] Each Facebook message contained the name of the accused and included a picture of him in uniform.[239] The witness testified that she had chatted about events known to her and the accused on the Facebook page in question and texted the accused using a number transmitted to her on that same Facebook account.[240]

Another form of circumstantial evidence is the behavior of the purported page-owner. Courts can consider the fact that the page or posting was taken down immediately after a party inquired about it in the litigation process.[241]

b. Concerns About Creating a Fake Page

Least convincing is the concern that the page was just a made-up farce or an attempt to frame an innocent person. Certainly, there are examples of people making fake pages on behalf of others. To create a free page on a social network does not require much—just a full name, email address, password, gender, and date of birth.[242] Even when the person does exist,

235. Commonwealth v. Purdy, 945 N.E.2d 372, 378 (Mass. App. Ct. 2011) (police "made an exact copy of the hard drive of the defendant's computer and, in searching it, located numerous e-mails, of which ten e-mail exchanges were admitted in evidence.").

236. The content can sometimes be validated by various "wayback" services that assemble and save postings on the web. *See Wayback Machine*, INTERNET ARCHIVE, http://archive.org/web/web.php (last visited June 24, 2012); Specht v. Google Inc., 758 F. Supp. 2d 570 (N.D. Ill. 2010) (describing the Internet Archive as providing users screen shots of websites that allegedly depict how the website appeared at a particular time.).

237. ACM S31768, 2011 WL 6015856 (Air Force Ct. Crim. App. 2011).

238. *Id.* at *1 (quoting MIL. R. EVID. 901(b)(4)).

239. *Id.* at *2.

240. *Id.*

241. In *State v. Eleck*, 23 A.3d 818 (Conn App. Ct. 2011), the witness who denied the authenticity of the posting immediately unfriended the accused after she was questioned about their communication.

242. Uncel, *supra* note 2, at 47.

however, fake pages are usually easy to spot for what they are.[243] For instance, it is not hard to find pranks where students make fake, unflattering social networking pages about their school principals,[244] or someone creates a MySpace page purportedly in the name of a church pastor describing homosexual conduct and drug use.[245] Such pages are self-evident parodies easy to unmask as non-genuine. Where a genuine question arises about who owns the page, the service providers can be subpoenaed to provide that information. As I argue below, that should not be standard procedure in every case.

c. *Concerns About Hacking or Opportunistic Signing on to Someone Else's Page*

It is also possible for someone to hack into or temporarily appropriate an existing page.[246] This can be accomplished by installing malicious software to record keystrokes, stealing or cracking someone's password, or gaining the trust of someone who is duped into voluntarily sharing access information.[247] The court in *State v. Eleck* deemed the potential for hacking a crucial factor that "highlights the general lack of security of the medium . . . ."[248] In *Commonwealth v. Purdy*,[249] the accused in a prostitution case objected to the authenticity of emails, claiming that his computer was located "near the massage room" and that "it was always on and that other people in the salon, particularly the masseuses, knew the passwords to his computer and used the computer frequently. He testified that they used his e-mail account to play pranks on him and that they answered e-mails in his name."[250]

Some commentators believe that this risk is so substantial that authentication of the owner's account is insufficient and that courts must insist on heightened authentication proving actual authorship.[251] I disagree and find myself supporting the logic of the court in *Tienda*[252]—that such elaborate hoaxes are unlikely and should not drive the authentication process.

---

243. United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009).

244. Layshock v. Hermitage School Dist., 650 F.3d 205, 207–10 (2011) (chronicling a fake MySpace profile of a principal, including parodic reference to his girth, drunkenness, and drug use); Draker v. Schreiber, 271 S.W.3d 318 (Tex. 2008) (describing a case where a MySpace page created by students purported to be the page of their vice principal; the page contained explicit sexual references, in addition to the vice principal's name, photo, and place of employment).

245. Clear v. Superior Court, No. E050414, 2010 WL 2029016 (Cal. Ct. App. May 24, 2010).

246. Uncel, *supra* note 2, at 68 ("[A]lthough the metadata and IP address can identify the *computer* that created the data, it cannot necessarily identify the actual *person* who created the data.").

247. *See* Robbins, *supra* note 8, at 10–13.

248. 23 A.3d 818, 824 (Conn. App. Ct. 2011).

249. 945 N.E.2d 372, 378 (Mass. App. Ct. 2011).

250. *Id.*

251. *See* Robbins, *supra* note 8, at 34–35 (arguing that authorship factors should be conditions of admissibility and should not go to weight); Magnuson & Borden, *supra* note 108 ("Authentication under Rule 901(b)(4) is potentially as problematic, as the indicia of reliability considered under this subsection, if susceptible to fabrication, are ultimately unreliable.").

252. *See supra* notes 192–206 and accompanying text (discussing *Tienda*).

Certainly, it is possible that others will post maliciously on a page to which they gain unfair access. Where others regularly have access, such as a joint email account or a Facebook page to which the owner has shared the password, it is certainly credible that someone could have maliciously posted to damage another's reputation or chances in litigation. For instance, a married couple might share a social networking page. If they divorce, one could easily believe that one spouse could make damaging posts facially attributable to the soon-to-be ex-spouse.[253] Even that situation, however, should not automatically bar authentication. Instead, the court should weigh various factors and, in general, leave it to the finder of fact to assess the likelihood that the postings are fraudulent.

Some fact patterns do indeed demand a finding by the court that the posting is inauthentic. When a page owner can demonstrate that she was locked out of her Facebook account on the relevant dates postings were made and that she complained to the provider that her access was cut off, that constitutes grounds for rejecting the authenticity of the post. Similarly, if a post is taken down, the password is changed, and the person immediately disavows the posting as soon as she regains use of the site, the judge should probably reject the post as inauthentic. Remarkably, many of those denying that they made a post on their social network pages never bothered to take it down until after it presented legal trouble.

VI. RECOMMENDATIONS AND CONCLUSION

So much modern communication already transpires over new media such as Facebook that lawyers and judges must find reliable and inexpensive ways to accommodate the huge volumes of information and potential courtroom evidence these sites generate. On the hearsay front, there has been little problem adapting to the forms of communication. With some added limits to the present sense impression exception[254] (an exception that, along with excited utterance, tends to be overused anyway), the byzantine hearsay structure works well, and no courts struggle with it.

Issues of authentication, however, have caused much more confusion—perhaps because one must have a basic understanding of the technology to grapple with authenticity issues.[255] The hyper-wariness of authenticating social media pages displayed by some courts is bad policy that will appear quaint one day but is impeding litigation now. Because social networking has become ubiquitous and may soon be the primary means of communication for many, the stingy approach to authentication

253. Ilana Gershon, an anthropologist who studies breakups via new social media and the author of BREAKUP 2.0, recounted to me that she came across a case where a wife, on an jointly held email account, posted mean-spirited remarks about her herself and threats to her new boyfriend to make her soon-to-be-ex-husband look vengeful and imbalanced.

254. *See supra* notes 80–82 and accompanying text (discussing Professor Bellin's suggestions regarding present sense impressions and Twitter).

255. Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 538 (D. Md. 2007) (recognizing that authenticating electronically stored information presents a myriad of concerns because "technology changes so rapidly" and is "often new to many judges.").

will lead to the unnecessary loss of valuable evidence.[256] Fear of the technology has led some courts to demand unreasonable levels of assurance of genuineness, ignoring that judges' initial screens for authenticity should not present a high hurdle to admissibility. True, Facebook pages can be faked. So can written documents.

Some scholars believe that the complexity and novelty of the new social media "requires greater scrutiny of 'the foundational requirements' than letters or other paper records, to bolster reliability."[257] I, however, agree with the court in *In re F.P.*,[258] which rejected the notion that electronic communication is "inherently unreliable."[259] The court did not support challenges to authentication, stating that "[e]ssentially, appellant would have us create a whole new body of law just to deal with e-mails or instant messages."[260] The court acknowledged the possibility that the difficulty of tracing electronic communication to a specific author can create some uncertainty and that "anybody with the right password can gain access to another's e-mail account and send a message ostensibly from that person."[261] It continued to observe, however, that "the same uncertainties exist with traditional written documents. A signature can be forged; a letter can be typed on another's typewriter; distinct letterhead stationary can be copied or stolen."[262] Historically, those sorts of questions are for the finder-of-fact to sort out.[263]

Attorneys can make their own lives and courts' determinations easier if they follow some basic principles. Attorneys wishing to authenticate a Facebook page or some other form of social networking should:

1. Lay a foundation for the provenance of the printout of the social media page in question.

a. The witness must describe where on the Internet the page was located and how the witness downloaded it.[264]

b. The relevant page should be printed out with its URL visible.[265]

c. The witness should also be prepared to testify that the printout reflects accurately what the witness saw on the webpage.[266]

---

256. *See* Uncel, *supra* note 2, at 45–46 (criticizing courts' "mistrust of social networking content even in the midst of ample evidence that exists to support its authenticity.").

257. *Lorraine*, 241 F.R.D. at 543–44 (quoting JACK B. WEINSTEIN & MARGARET A. BERGER, WEINSTEIN'S FEDERAL EVIDENCE § 900.06[3] (2d ed.1997)).

258. 878 A.2d 91 (Pa. Super. Ct. 2005).

259. *Id.* at 95.

260. *Id.*

261. *Id.*

262. *Id.*

263. *See* Uncel, *supra* note 2, at 66–69 (advocating a "presumption of authenticity"). *But see* Robbins, *supra* note 8 (arguing for stricter standards).

264. If the page is still up (which is doubtful at the time of the testimony) the finder-of-fact could access the page in the courtroom.

265. BROWNING, *supra* note 1, at 113.

266. *Id.*

d. Some evidence should be offered as to who has access to the page and how.[267]

2. Establish ownership of the page. This can be accomplished by stipulation, testimony of a person with knowledge (ideally, but not necessarily, the page owner), an affidavit from the service provider about to whom the page is registered, or circumstantial evidence. In appropriate circumstances, particularly where the name, birth date, geographic location, photo, and other identifying characteristics of the page owner are visible on the page, ownership can be established by such distinctive criteria, along with content-based evidence. Allowing authentication based on the page information alone is particularly appropriate when evidence is abundant from the style and content of the page that the page owner regularly used it. It would be an expensive and unnecessary impediment to litigation if courts routinely required affidavits from service providers.[268]

3. Demonstrate that the page owner actually wrote the post in question. This can best be accomplished by stipulation or questioning the page owner or post writer.[269] It can also sometimes be established by examining the hard drive of the page owner's computer, but that is expensive and incomplete because Facebook pages and their ilk can be accessed from many different devices anywhere there is an Internet connection.[270] Even if the owner of the page denies having written the post, circumstantial evidence, such as the content of the post, can provide sufficient distinctive characteristics for authentication and identification of the author.[271] Where the page owner acknowledges ownership of the page but claims hacking or other usurpation, evidence that the posting remained up while the page was in the owner's control would persuasively rebut claims of hacking, etc.

Essentially, I recommend a rebuttable presumption of authenticity of social media accounts whereby the offering party goes through the three

267. Commonwealth v. Purdy, 945 N.E.2d 372, 382 n.7 (Mass. 2011) (requiring some "testimony regarding how secure a MySpace Web page is, who can access it, or whether codes are needed for such access.").

268. *See* Democko, *supra* note 1, at 403 (rejecting a suggestion to obtain information directly from the social network provider as too expensive); *Purdy*, 945 N.E.2d at 382 n.7 (noting "that we do not suggest that expert testimony or exclusive access is necessary to authenticate the authorship of an e-mail. Nor do we suggest that password protection is necessary to authenticate the authorship of an e-mail, even though there was such protection here.").

269. BROWNING, *supra* note 1, at 113 ("To make the process of proving authorship as simple and direct as possible, consider asking the witness about his or her online social networking during a deposition.").

270. *See* Democko, *supra* note 1, at 403 (rejecting a proposal to examine the hard drive to determine the provenance of a Facebook past noting: "This option may be viable in theory, but impractical in practice. Internet-communication devices and social networking sites can be accessed from any computer, in any location, at any time, as long as the user's username and password are supplied.").

271. *Cf.* Dickens v. State, 927 A.2d 32 (Md. Ct. Spec. App. 2007) (authenticating telephonic text messages as having been sent by the defendant based on the content and the circumstances of those messages, including evidence of the timeline, references to other messages, and mention of the couple's wedding vows).

steps above.[272] I disagree both normatively and descriptively with Judge Grimm, who states that "it is critical for courts to start demanding that counsel give more in terms of authentication—and counsel who fail to meet courts' expectations will do so at their own peril."[273]

Many courts have taken an appropriately liberal approach to authentication.[274] The standard for authentication by the judge as a gatekeeper should remain low. The technology should not drive a demand for more than the minimal showing that the evidence rules wisely require.

On the issue of page ownership, normally, subpoenaing the service provider or examining the computer in question should not be necessary to prove page ownership.[275] In civil cases, questions of authenticity and admissibility of documents should be hashed out in advance of trial. If a party refuses to stipulate as to page ownership, then resorting to a subpoena is appropriate, with the objecting party paying for the cost of discovery if ownership is found.

In criminal cases, many prosecutors already use subpoenas and computer experts, particularly in cases where the computer evidence is key (such as cases involving solicitation of minors for sex on social media).[276] In such cases, using subpoenas and experts makes the most sense strategically but should not be an absolute requirement.

In many cases, the accused objects that the prosecutor has not authenticated a page but never actually denies that the social media is his own. Such disingenuous and opportunistic objections undermine the function of the evidence rules when there is enough other evidence to prove that the item in question is what the prosecutor purports it to be. Particularly troubling is when the accused in a criminal case attempts to admit evidence from a social network site and is met with a high bar for authentication.

---

272. Many courts employ such a rebuttable presumption in admitting emails. *Cf.* Midwest Retailers Ass'n v. City of Toledo, 582 F. Supp. 2d 931, 934–35 (N.D. Ohio 2008); Mortgage Mkt. Guide, L.L.C. v. Freedman Report, L.L.C., No. 06-CV-140, 2008 WL 2991570, at *12 n.3 (D.N.J. July 28, 2008); Telewizja Polska USA, Inc. v. Echostar Satellite Corp., No. 02C3293, 2004 WL 2367740, at *6 (N.D. Ill. Oct. 15, 2004).

273. 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, 366 (2009).

274. *See, e.g.*, State v. Bell, 882 N.E.2d 502, 511–12 (Ohio Ct. Com. Pl. Jan. 29, 2008), *aff'd,* No. CA2008–05–044, 2009-Ohio-2335, 2009 WL 1395857 (Ohio Ct. App. May 18, 2009) (denying authentication challenge despite the fact "that MySpace chats can be readily edited after the fact from a user's homepage. . . . [and] that while his name may appear on e-mails to T.W., the possibility that someone else used his account to send the messages cannot be foreclosed.").

275. *See, e.g.*, Dockery v. Dockery, No. E2009-01059-COA-R3-CV, 2009 WL 3486662, at *6 (Tenn. Ct. App. Oct. 29, 2009) (rejecting arguments that "the computer printouts of the conversations between Husband and [ex-wife] could be authenticated only by a representative of MySpace").

276. *See, e.g.*, People v. Clevenstine, 891 N.Y.S.2d 511, 514 (App. Div. 2009) ("investigator from the computer crime unit of the State Police related that he had retrieved such conversations from the hard drive of the computer used by the victims, a legal compliance officer for MySpace explained that the messages on the computer disk had been exchanged by users of accounts created by defendant and the victims, and defendant's wife recalled the sexually explicit conversations she viewed in defendant's MySpace account while on their computer. Such testimony provided ample authentication for admission of this evidence.").

Where there is a genuine objection that the page does not belong to the putative owner, each side has equal access to subpoena power, and the burden should not necessarily be on the proffering party to subpoena the records.

On the issue of whether an impermissible post was made on a site that the owner acknowledges as his, questions of authenticity should almost always be left for the finder-of-fact. Unless the evidence of hacking or capture is irrefutable, questions as to who made an individual post should not be solely determined by the trial court in its gatekeeping role.