Litigation and Social Media: Using Social Media to Your Advantage at Every Step of the Trial†

Marisa A. Trasatti
Anna C. Horevay

I. Introduction

"There's a whole generation of people for whom tw[eeting] is as natural as breathing,"[1] *for whom the word "friend" has become a verb, and for whom Web 2.0 is the only media platform they know.*

Social networking has exploded in recent years. Today, Facebook has more than one billion users—over one-seventh of the world's population.[2] Facebook and YouTube rank as the two most visited sites on the Internet.[3] Indeed, social networking pervades the Internet: According to the Pew Research Center, as of late 2012, 71% of all Internet users use Facebook, 22% use LinkedIn, 21% use Pinterest, 18% use Twitter, and 17% use Instagram.[4] For Internet users under age fifty, social networking use increases to 83% of all Internet users.[5]

---

† Submitted by the authors on behalf of the FDCC Drug, Device and Biotechnology Section.

[1] Nora Lockwood Tooher, *Tackling Juror Internet Use*, Lawyers USA, (Mar. 24, 2009), http://lawyersusaonline.com/blog/2009/03/24/tackling-juror-Internet-use/.

[2] Ashley Vance, *Facebook: The Making of 1 Billion Users*, Bloomberg Businessweek (Oct. 4, 2012), http://www.businessweek.com/articles/2012-10-04/facebook-the-making-of-1-billion-users.

[3] Graeme McMillan, *Facebook Tops One Trillion Hits Per Month, Wins Internet*, Time (Aug. 25, 2011), http://techland.time.com/2011/08/25/facebook-tops-one-trillion-hits-per-month-wins-Internet/.

[4] Maeve Duggan & Aaron Smith, Social Media Update 2013 (Dec. 30, 2013), *available at* http://pewinternet.org/Reports/2013/Social-Media-Update/Main-Findings.aspx.

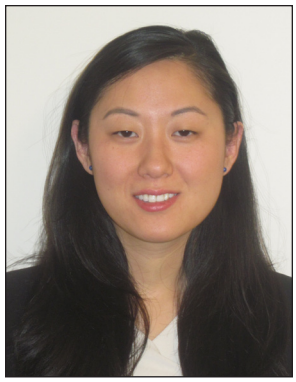
[5] Maeve Duggan & Joanna Brenner, The Demographics of Social Media Users — 2012 (Feb. 14, 2013), *available at* http://pewInternet.org/Reports/2013/Social-media-users.aspx.

Marisa A. Trasatti is a principal at Semmes, Bowen, and Semmes in the Baltimore, Maryland office. Her practice focuses primarily on civil litigation, with an emphasis on products liability litigation including cases involving drugs and medical devices. Ms. Trasatti has significant trial experience in medical malpractice, insurance defense, and products liability cases. She has also defended locally and nationally several large corporations in connection with toxic tort litigation. Ms. Trasatti serves on the Board of the Maryland Defense Counsel as the Co-Chair of the Judicial Nominations Committee and the organization's Treasurer. Ms. Trasatti is a member of the Maryland bar, and is also admitted to practice before the Superior Court of the District of Columbia, the U.S. District Court for the District of Maryland, the U.S. Court of Appeals for the Fourth Circuit, and the United States Supreme Court. She is a member of DRI and of its products liability and drug and medical defense committees, and is the immediate past Program Chair of the 2013 Women's Committee Seminar, "The Seminar for Legal and Business Innovators." She is an active member of the Federation of Defense & Corporate Counsel, currently serving as a Vice-Chair of the Drug, Device, and Biotechnology and Publications Committees and as a member of the Admissions Committee. She is a frequent speaker at FDCC meetings and regularly blogs about recent cases for the organization.

This brave new world of social media poses a host of challenges, both substantive and procedural, for judges, attorneys, and litigants. Though some have refused to recognize the reality of social media,[6] most jurists and attorneys are now dealing head-on with issues raised by its use. And while some trends appear to be developing—e.g., California and New York are the most permissive jurisdictions with respect to the use of social media; Florida and Maryland the most restrictive—the law is rapidly evolving, and there is not yet a consistent body of law with respect to most of the critical issues. One thing is certain, however: Social networking is here to stay, and judges and attorneys must learn how it can be used—and abused—throughout the litigation process.

---

[6] *See* E.C. v. C.B.T., Sr., No. FV-03-282-13, 2013 WL 1858859, at *3 (N.J. Super. Ct. App. Div. May 6, 2013) (where a lower court judge stated, "I don't give a lot of credence to e-mails and Facebook and all that nonsense because that's not a face to face exchange").



Anna Horevay was a 2013 summer associate with Semmes, Bowen & Semmes in Baltimore, Maryland. A 2014 J.D. Candidate at the University of Maryland Francis King Carey School of Law, Ms. Horevay is a Leadership Scholar, an articles editor for the Journal of Health Care Law and Policy, and a research assistant to Distinguished Visiting Professor Sheldon Krantz. Ms. Horevay was an Asper Fellow to the Honorable Lawrence Fletcher-Hill of the Circuit Court for Baltimore City and a legislative extern for the Maryland Developmental Disabilities Council. Ms. Horevay will serve as a judicial law clerk to the Honorable Alexander Wright, Jr. of the Court of Special Appeals of Maryland for the 2014-15 term.

This article addresses some of the challenges related to the use of social media in the course of litigation and provides guidance for how judges and attorneys can respond to them. Part II discusses issues arising at the outset of litigation, including personal jurisdiction in cases arising out of the use of social media and the use of social media to effect service. Part III examines 47 U.S.C. § 230 as a bar to suing Internet service providers for torts related to the misuse of social media. Part IV focuses on discovery of private social media pages as "electronically stored information" and on the use of subpoenas to unmask anonymous social media users. Part V addresses the implications of social media at the trial stage, including issues related to voir dire, evidence authentication, and juror misconduct. Finally, Part VI discusses ethical considerations for both judges and attorneys in using social media.

II.
Bringing a Lawsuit

A. *Personal Jurisdiction*

Asserting personal jurisdiction over a defendant for claims arising out of social media interactions can be difficult, especially when the defendant could be located hundreds or thousands of miles from where the alleged injury is suffered—assuming he or she can be located at all. Due process requires that a nonresident defendant have certain minimum contacts with the forum state such that the maintenance of the suit does not offend "traditional notices of fair play and substantial justice."[7] Courts have grappled with how to protect defendants' due process rights while still giving plaintiffs a forum to redress their injuries.

---

[7] Int'l Shoe Co. v. Washington, 326 U.S. 310, 316 (1945).

As these cases show, courts continue to have difficulty molding old jurisdictional principles to fit the new social networking paradigm.

In analyzing the propriety of exercising personal jurisdiction over a third-party user of a website, the threshold question is whether the user has "purposefully availed" himself or herself of conducting activities in the forum state.[8] In *Wilkerson v. RSL Funding, LLC*,[9] for example, the Texas Court of Appeals analyzed the purposeful availment standard with respect to a person who posted negative comments about a Texas-based company on Yahoo and Yelp.[10] In addition to its Houston headquarters, the company advertised that it had locations in New York, Chicago, Philadelphia, Washington, D.C., Los Angeles, West Palm Beach, and Atlanta.[11] The defendant's negative comments contained only one reference to the company's presence in Texas.[12] The court noted that without evidence the defendant "deliberately used a website oriented towards, aiming at, or otherwise specifically targeting Texas," asserting personal jurisdiction over him would violate due process.[13] Courts in other jurisdictions have similarly found that without some indication that a third-party user of a social networking site intended to specifically target the forum state, purposeful availment, and thus personal jurisdiction, cannot be found.[14]

By contrast, when a defendant has engaged in specific targeting, personal jurisdiction can be exerted. In *Rios v. Fergusan*,[15] a resident of North Carolina threatened an individual in Connecticut via a YouTube video.[16] In a case of first impression, the Superior Court of Connecticut considered whether it could extend jurisdiction over the North Carolina resident based on the threatening video.[17] Although courts in other jurisdictions had stated that the

---

[8] To satisfy minimum due process standards, there must be "some act by which the defendant purposefully avails itself of the privilege of conducting activities within the forum State, thus invoking the benefits and protections of its laws." Hanson v. Denckla, 357 U.S. 235, 253–54 (1958).

[9] 388 S.W.3d 668 (Tex. Ct. App. 2011).

[10] *Id.* at 677–82.

[11] *Id.* at 671.

[12] *Id.* at 680.

[13] *Id.* at 678–79.

[14] *See* Woodhurst v. Manny's Inc., No. 12-0317, 2013 WL 1452929, at *2–3 (Iowa Ct. App. Apr. 10, 2013) (holding that mere advertisements on Facebook and MySpace pages that were for a separate location outside the forum state did not show purposeful direction of activities toward the forum state). *See also* Lyons v. Rienzi & Sons, Inc., No. 09-CV-4253, 2012 WL 1393020, at *1 (E.D.N.Y. Apr. 23, 2012) (holding that an Italian company's operation of a Facebook page accessible to U.S. users did not suffice for personal jurisdiction over the company); M & M Techs., Inc. v. Gurtler Chems., Inc., No. Civ. A. 03-994 GMS, 2005 WL 293509 (D. Del. Feb. 8, 2005) ("while [defendant] does maintain an Internet website that it can use to solicit business from Delaware, the mere existence of its website does not rise to the level of regularly soliciting business in Delaware") (citations omitted).

[15] 978 A.2d 592 (Conn. Super. Ct. 2008).

[16] *Id.* at 593–94.

[17] *Id.* at 594.

mere posting of a message on a social networking site accessible in the forum state was not enough to confer jurisdiction upon an out-of-state defendant,[18] the specific targeting of a Connecticut resident through online threats created grounds for personal jurisdiction in Connecticut over the North Carolina resident.[19]

B. *Service via Social Media*

Plaintiffs struggling to serve process on defendants have begun to turn to the Internet as a way to effect service. In *Fortunato v. Chase Bank USA, N.A.*,[20] Chase Bank wanted to implead a third party into the case, but was unable to serve her at the address they had.[21] An investigator for the bank located what he believed to be the third party's Facebook profile, which included her location.[22] Chase then sought leave of court to serve the third party via a Facebook message, among other methods of service.[23]

The United States District Court for the Southern District of New York denied the motion, noting that service by Facebook was unorthodox and had not been authorized by any known court.[24] Analogizing to service by email, the court further noted that such service had been approved only when there was a degree of certainty that the email would likely reach the defendant.[25] Because Chase had not adduced any evidence that such would be the case—or even that the purported Facebook account actually belonged to the party sought to be impleaded—there was no basis to authorize service via Facebook.[26]

Less than one year later, in *FTC v. PCCare247 Inc.*,[27] the same jurisdiction approved service through Facebook as a supplement to other methods of service. The court observed that service by Facebook raised due process concerns when there was no way to confirm that the Facebook profile was actually created by the person to be served.[28] In contrast to

---

[18] *See, e.g.*, Goldhaber v. Kohlenberg, 928 A.2d 948, 952 (N.J. Super. Ct. App. Div. 2007). However, in *Goldhaber*, the court did find personal jurisdiction over the defendant based on evidence that the postboard messages targeted New Jersey, as the author knew the plaintiff lived in New Jersey and made references to the town where the plaintiff lived. *Id.* at 953. Additionally, the defendant referred to the plaintiff's neighbors and even posted the plaintiff's address. *Id.*

[19] *Rios*, 978 A.2d at 600.

[20] No. 11 Civ. 6608(JFK), 2012 WL 2086950 (S.D.N.Y. June 7, 2012).

[21] *Id.* at *2

[22] *Id.*

[23] *Id.* at *1.

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] No. 12 Civ. 7189(PAE), 2013 WL 841037 (S.D.N.Y. Mar. 7, 2013).

[28] *Id.* at *5. Determining the identity of the owner of a social media profile is a recurring issue in cases involving social media.

Fortunato, however, plaintiffs in *PCCare247* established the likelihood that the Facebook accounts were operated by the defendants based on the accounts' registration email addresses and the fact that the defendants' profiles listed their jobs at the defendant companies as their professional activities.[29] Even with these protections, the court observed that there was a "substantial question" whether service by Facebook alone would comport with due process;[30] thus, the court authorized the Facebook service only as a supplement to service by email.[31]

As the court noted in *PCCare247*, technological advances require that courts be open to "considering requests to authorize service via technological means of then-recent vintage rather than dismissing them out of hand as novel."[32] In doing so, the court followed the lead of the Ninth Circuit, which had stated that the "due process reasonableness inquiry unshackles the federal courts from anachronistic methods of service and permits them entry into the technological renaissance."[33] Since *Fortunato*, service via social media has been approved in foreign jurisdictions, such as Canada.[34]

At present, it appears that service by social media is likely to be allowed only when coupled with service by another method, such as email.[35] Further, plaintiffs must establish that service by social media will likely reach the defendant.[36] This can be shown through facts, e.g., that the social media account is registered to the defendant's email address; that the account lists the defendant's last known address as the address of record; and that the job information listed on the account is the same as the defendant's.[37]

---

[29] *Id.*

[30] *Id.*

[31] *Id.*

[32] *Id.*

[33] *Id.* (citing Rio Props., Inc. v. Rio Int'l Interlink, 284 F.3d 1007, 1017 (9th Cir. 2002) (addressing service by email)) (internal quotation marks omitted).

[34] *See Brian Burke can serve legal notices online in defamation lawsuit*, CTV News (May 29, 2013, 4:21 PM EDT), http://www.ctvnews.ca/canada/brian-burke-can-serve-legal-notices-online-in-defamation-lawsuit-1.1302491 (noting that service via email or private message on social media has been approved in a defamation case about online message board comments). Since *Fortunato*, one jurisdiction has stated that service via electronic service is permitted only when serving *foreign* defendants, as the Rules of Federal Procedure do not permit electronic service on *domestic* defendants. *See* Joe Hand Promotions, Inc. v. Shepard, 4:12CV1728 SNLJ, 2013 WL 4058745, at *2 (E.D. Mo. Aug. 12, 2013).

[35] *See PCCARE247*, 2013 WL 841037, at *6.

[36] *Fortunato*, 2012 WL 2086950, at *2.

[37] *See PCCARE247*, 2013 WL 841037, at *5 (listing facts that establish that defendant is likely person who owns social media account in question).

III.
Foreclosing a Suit — Section 230 Immunity

Everyone has heard the social networking horror stories: a mother charged with cyberbullying a teenage girl over MySpace;[38] a man convicted of conspiracy for discussing cannibalism in an online message forum;[39] a vengeful boyfriend posting an explicit tape of his ex-girlfriend online;[40] a debt agency using Facebook to harass a woman regarding an unpaid loan;[41] and a well-known, but unsuspecting, football player duped into falling in love

---

[38] Jennifer Steinhauer, *Woman Indicted in MySpace Suicide Case*, N.Y. Times (May 16, 2008), http://www.nytimes.com/2008/05/16/us/16myspace.html?ref=meganmeier. While this article does not endeavor to provide comprehensive information on cyberbullying, it is difficult to ignore in the context of Section 230 immunity, as plaintiffs often have nowhere to turn for redress if a court grants immunity. Instead, injured parties often must rely on federal misuse statutes, like 18 U.S.C. §§ 875 and 2261A(2), which criminalize threatening interstate communication and interstate stalking through an interactive computer service, respectively. Applications of these statutes have been largely unsuccessful. *See* United States v. Baker, 890 F. Supp. 1375, 1388–90 (E.D. Mich. 1995) (holding that emails detailing plans to harm a woman fell short of the constitutional standard of a true threat and denying prosecution of defendant under 18 U.S.C. § 875 when analyzed under the lens of the First Amendment), *aff'd sub nom.* United States v. Alkhabaz, 104 F.3d 1492 (6th Cir. 1997); United States v. Cassidy, 814 F. Supp. 2d 574, 587 (D. Md. 2011) (holding 18 U.S.C. § 2261A(2)(A) invalid as applied to blog and Twitter posts, which are constitutionally protected expressions of speech). Notably, no court analyzing section 2261(A)(2)(A) has upheld its constitutionality. *Cassidy*, 814 F. Supp. 2d at 586 n.13. Recently, Congress reenacted the Violence Against Women Act ("VAWA"), 18 U.S.C. § 2261, which may provide women with a recourse against cyberstalking. Under the VAWA, it is a federal crime to use an interactive computer service to cause substantial emotional distress or place a person in reasonable fear of death or serious bodily injury in certain categories of people. 18 U.S.C. § 2261A (2013). This new law has yet to undergo any constitutional challenge.

Scholars have noted that Section 230 immunity actually affords social networking sites the unique opportunity to foster online citizenship given that no matter what action the site takes (to leave a post alone or delete it), the provider will be immune from suit. *See, e.g.,* Danielle Keats Citron & Helen Norton, *Intermediaries and Hate Speech: Fostering Digital Citizenship for Our Information Age*, 91 B.U. L. Rev. 1435 (2011). Despite this chance to shape the Internet community, some sites (while adopting terms that prohibit abusive speech) have adopted terms where users are largely responsible for policing the posts on their websites. *See, e.g., Facebook Community Standards*, Facebook, https://www.facebook.com/communitystandards (last visited June 26, 2013).

[39] Benjamin Weiser, *'Ugly Thoughts' Defense Fails as Officer Is Convicted in Cannibal Plot*, N.Y. Times, Mar. 12, 2013, at A1, *available at* http://www.nytimes.com/2013/03/13/nyregion/gilberto-valle-is-found-guilty-in-cannibal-case.html?pagewanted=all.

[40] Todd Quinones, *'Heart Broken' Boyfriend Charged After Posting Sex Tape Online*, CBS Philly (Nov. 16, 2011, 10:43 PM), *available at* http://philadelphia.cbslocal.com/2011/11/16/heart-broken-boyfriend-charged-after-posting-sex-tape-online/.

[41] Tamara Lush, *Court Rules Debt Agency Can't Contact Woman on Facebook*, Law Technology News (Mar. 3, 2011), http://www.law.com/jsp/lawtechnologynews/PubArticleFriendlyLTN.jsp?id=1202485594771.

with a fake Internet persona.[42] In such cases, the injured party may seek to sue the interactive computer service provider where the offensive posts appeared. Such an attempt will almost certainly be faced with a claim that suit is barred by Section 230 of the Communications Decency Act.[43]

Under Section 230, no "interactive computer service"[44] shall be subject to liability for:

> (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
>
> (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).[45]

In essence, Section 230 bars suits against intermediary interactive computer service providers—e.g. Facebook, MySpace, and Twitter—for third-party content that appears on their websites.[46]

---

[42] This phenomenon, known as "catfishing," occurs when a person falls in love with a fake Internet persona—i.e., someone who is not whom they claim to be online. Steve Eder, *Hoax Is Revealed as Irish Star Says He Was Duped*, N.Y. Times, Jan. 16, 2013, at B15, *available at* http://www.nytimes.com/2013/01/17/sports/ncaafootball/story-of-manti-teos-girlfriend-is-said-to-be-a-hoax.html. *See also* Rachel Dodes, *Nev Schulman on Texting, 'Catfishing' and Manti Te'o*, Wall St. Journal (Apr. 5, 2013, 11:07 AM), http://blogs.wsj.com/speakeasy/2013/04/05/nev-schulman-on-texting-catfishing-and-manti-teo/ (for discussion of the term "catfishing" and the Manti Te'o hoax).

[43] 47 U.S.C. § 230.

[44] "The term 'interactive computer service' means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions." 47 U.S.C. § 230 (f)(1)(2) (1998). "Information content provider" means "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service." *Id.* at § 230(f)(1)(3).

[45] *Id.* at § 230(c)(2).

[46] Other suits outside of this context could still arise (*see infra* text accompanying notes 68 -79), and Congress may still attempt to shape ways to find intermediary liability. For example, the Stop Online Piracy Act ("SOPA") and the Protect IP Act ("PIPA"), as introduced in U.S. Congress, attempted to make it difficult for sites to sell or distribute pirated copyrighted material. Larry Magrid, *What Are SOPA and PIPA And Why All the Fuss?*, Forbes (Jan. 18, 2012 10:14 AM), http://www.forbes.com/sites/larrymagid/2012/01/18/what-are-sopa-and-pipa-and-why-all-the-fuss/. Under SOPA, the U.S. Attorney General would be able to seek a court order to require a "service provider [to] take technically feasible and reasonable measures designed to prevent access by its subscribers . . . to the foreign infringing site." *Id.* Websites would thus have to worry that they could be violating the law by linking to a "banned site." *Id.* But SOPA and PIPA went without a vote after many online and offline protests against the bills. Julianne Pepitone, *SOPA and PIPA postponed indefinitely after protests*, CNN Money (Jan. 20, 2012 7:54 PM ET), http://money.cnn.com/2012/01/20/technology/SOPA_PIPA_postponed/index.htm. Still, these acts target the content of the website for copyright infringement as opposed to censoring of free speech (though some claim that the acts would in effect censor speech on websites). *See* Magrid, *supra*.

The Fourth Circuit discussed the application of Section 230 in *Zeran v. America Online, Inc*.[47] In that case, Kenneth Zeran sued America Online ("AOL") after posts were made on an AOL bulletin board purporting to advertise t-shirts with offensive slogans related to the Oklahoma City bombings and listing Zeran's name and phone number as the contact to purchase the shirts.[48] Following the first post, Zeran contacted AOL and requested that the post be removed.[49] AOL agreed to do so. Over the next five days, several more messages advertising the sale of additional t-shirts and other items were posted, again with Zeran's contact information.[50] As a result, Zeran received angry and abusive telephone calls, including death threats.[51] Eventually, Zeran received an abusive phone call about every two minutes.[52] Zeran repeatedly contacted AOL during this period and was told by company executives that AOL would close the account where the posts originated.[53]

In his suit, Zeran sought to hold AOL liable for defamatory speech under a theory of distributor liability.[54] The Fourth Circuit held that Section 230 applied to the case regardless of whether Zeran attempted to rebrand AOL a distributor instead of an interactive computer service.[55] According to the court, Congress enacted Section 230 to "maintain the robust nature of Internet communication and, accordingly, to keep government interference in the medium to a minimum."[56] Interactive computer service providers have so many users that imposing tort liability upon them would have a chilling effect on free speech becayse they would have to screen each post for problems.[57] *Zeran* has since been heavily relied upon in other courts for establishing the basic principles behind Section 230.[58]

Cases since *Zeran* have attempted to test the limits of immunity for social networking sites. In *Doe v. MySpace, Inc.*,[59] the mother of a teenage girl sued MySpace after her thirteen-year-old daughter was sexually assaulted by someone she met on the social networking

---

47 129 F.3d 327 (4th Cir. 1997).

48 *Id.* at 329.

49 *Id.*

50 *Id.*

51 *Id.*

52 *Id.*

53 *Id.*

54 *Id.* at 331.

55 *Id.* at 330.

56 *Id.* For now, social media sites rely on their terms of use to help avoid problematic users by making users agree to policies that prohibit using social media services for unsavory purposes, like harassment and bullying. *See, e.g. Statement of Rights and Responsibilities,* Facebook, https://www.facebook.com/legal/terms (last visited Oct. 18, 2013).

57 *Id.* at 331. The court also rejected a theory of notice-based liability and held that such a harsh standard would defeat the purpose of Section 230. *Id*. at 333.

58 On January 15, 2014, a search on Westlaw for citing references to *Zeran* revealed over 150 cases.

59 474 F. Supp. 2d 843 (W.D. Tex. 2007), *aff'd*, 528 F.3d 413 (5th Cir. 2008).

site.[60] The daughter had set up a MySpace account by untruthfully representing she was eighteen and was subsequently contacted by a nineteen-year-old boy.[61] After communicating for several weeks, the two arranged to meet for a date.[62] According to the complaint, the nineteen year old sexually assaulted the daughter during the date.[63] The mother's suit against MySpace alleged negligence against MySpace based on its ineffective security measures for age verification.[64] Noting that Section 230 immunity is not limited to the publication of third-party content,[65] the United States District Court for the Western District of Texas granted the defendants' motion to dismiss based on the statute.[66]

Although cases such as *Zeran* and *Doe* suggested that Section 230 bars any claim alleging *tort* liability against an intermediary, these cases did not consider potential liability under a *contract* theory. Such claims were subsequently addressed in *Barnes v. Yahoo!, Inc.*[67] In that case, plaintiff Barnes broke up with her boyfriend, who then created a number of profiles on Yahoo using Ms. Barnes's contact information.[68] The profiles included nude photographs of Ms. Barnes and implied she was open to solicitations for sex.[69] As a result, Ms. Barnes received a number of calls, emails, and visits from men with the expectation of sex.[70]

Over the next two months, Ms. Barnes requested Yahoo remove the fraudulent profiles four different times, but to no avail.[71] A day before a local news show was scheduled to broadcast a report about Ms. Barnes's situation, Yahoo's Director of Communications contacted Ms. Barnes and told her she would "personally walk the statements over to the division responsible for stopping unauthorized profiles and they would take care of it."[72] Relying on this statement, Ms. Barnes took no further action.[73] After two more months without action by Yahoo, Ms. Barnes filed her lawsuit.[74]

---

60 *Id.* at 846.

61 *Id.*

62 *Id.*

63 *Id.*

64 *Id.*

65 *Id.* at 848-49.

66 *Id.* at 850.

67 570 F.3d 1096 (9th Cir. 2009).

68 *Id.* at 1098.

69 *Id.*

70 *Id.*

71 *Id.*

72 *Id.* at 1098–99.

73 *Id.* at 1099.

74 *Id.*

In her lawsuit, Ms. Barnes made a claim for promissory estoppel based on her reliance on Yahoo's promise to remove the profiles.[75] The district court dismissed the suit based on Section 230, but the Ninth Circuit reversed, noting that liability under a contract theory would have a different analysis than claims alleging tort liability.[76] The statements by Yahoo's representative that they would remove the profiles could have been an enforceable promise that would provide the basis for suit.[77] Though the court focused only on the reach of Section 230 and did not decide whether the plaintiff actually stated a viable contract claim,[78] the court at least opened the door for potential liability on the basis of promissory estoppel.

The issue of whether Section 230 actually grants total immunity to social media websites remains open. Because there is a split of authority among the circuits,[79] the scope of immunity may remain unresolved until the Supreme Court decides the issue.

IV.
Pretrial Issues

A. *Discovery of Social Media Postings*

The Federal Rules of Civil Procedure allow parties to obtain discovery of any matter so long as it "appears reasonably calculated to lead to the discovery of admissible evidence."[80] Since 2006, this has included "electronically stored information" ("ESI"), and issues surrounding ESI and e-discovery have erupted.[81] Under the current rules, litigants and attorneys have a duty to preserve potentially relevant ESI,[82] including information on social networking accounts.[83] Courts, attorneys, and litigants continue to struggle with the meaning of the discovery rules as they relate to ESI,[84] and failure to produce such information is now the most common basis for court-ordered sanctions.[85]

---

[75] *Id.* at 1106.

[76] *Id.* at 1107–08.

[77] *Id.* at 1108–09.

[78] *Id.* at 1009.

[79] *See* Hare v. Richie, No. ELH-11-3488, 2012 WL 3773116, at *14 (D. Md. Aug. 29, 2012) (noting a circuit split as to whether Section 230 is an immunity defense, citing the Eighth and Eleventh Circuits as recognizing immunity to suits under Section 230, and the Seventh and Ninth Circuits as not recognizing immunity under Section 230).

[80] Fed. R. Civ. P. 26(b)(1).

[81] Brent R. Austin, ESI, E-Discovery, and Ethics: Managing Pre-Trial Litigation in the Age of Electronically Stored Information, 2012 WL 3058127, at *1 (Aspatore ed., 2012).

[82] *Id.* at *3.

[83] *Id.* at *8.

[84] *Id.* at *2.

[85] Dan H. Willoughby, Jr. et al., *Sanctions for E-Discovery Violations: By the Numbers,* 60 Duke L.J. 789, 789 (2010).

Applying the federal discovery standard to private social media pages,[86] courts have consistently ruled that production of such pages will not be compelled unless there is some indication from the publicly viewable pages that such production will lead to the discovery of admissible evidence.[87] In *Romano v. Steelcase, Inc.*,[88] the defendant viewed the public portions of plaintiff's MySpace and Facebook pages after plaintiff claimed she sustained permanent injuries that affected her enjoyment of life.[89] The public portions of the plaintiff's pages revealed her smiling happily outside of her home, despite her allegations that she was largely confined to her bed as a result of her injuries.[90] The Supreme Court for Suffolk County, New York held that it was reasonable to infer from these public pages that plaintiff's private pages might contain information relevant to her claims or that could lead to the discovery of admissible evidence.[91]

Without the type of publicly accessible information present in *Romano*, courts have typically deemed requests for access to private social networking a "fishing expedition." In *Davids v. Novartis Pharmaceuticals Corp.*,[92] for example, the United States District Court for the Eastern District of New York found that more than a smiling profile photograph on plaintiff's public Facebook page was required to gain access to her private Facebook information, even though the plaintiff was claiming ongoing suffering.[93] In contrast to *Romano*, where the defendant could point to multiple photos and statements on the plaintiff's social networking page to contradict her claims, the defendant in *Davids* had only the plaintiff's

---

[86] Private social media pages are pages that are not visible to the public (or to the Internet at-large). However, different levels of "private" exist, depending on a user's chosen privacy settings, from open to the Internet at-large to visible only to the author. *See Choose Who You Share With*, Facebook, http://www.facebook.com/help/459934584025324/ (click "What does 'Public' mean?") (last visited June 24, 2013).

[87] *See, e.g.*, *Tompkins v. Detroit Metro. Airport*, 278 F.R.D. 387 (E.D. Mich. 2012) (requiring a "threshold showing that the requested information is reasonably calculated to lead to the discovery of admissible evidence"). Most courts opt for the standard adopted in *Tompkins*, but one court has recently noted that this approach can improperly shield discovery of information that is held privately on Facebook. *Compare* Jewell v. Aaron's, 21 Wage & Hour Case.2d (BNA) 292, 2013 WL 3770837, at *5 (N.D. Ga. July 19, 2013) *and* Davenport v. State Farm Mut. Auto. Ins. Co., No. 3:11–cv–632–J–JBT, 2012 WL 555759, at *1 (M.D. Fla. Feb. 21, 2012) (both applying *Tompkins* standard for electronic discovery) *with* Giacchetto v. Patchogue-Medford Union Free Sch. Dist., 293 F.R.D. 112, 114 (E.D.N.Y. 2013) (stating that *Tompkins* standard can improperly shield "from discovery the information of Facebook users who do not share any information publicly").

[88] 30 Misc. 3d 426 (N.Y. Sup. Ct. 2010).

[89] *Id.* at 429.

[90] *Id.* at 430.

[91] *Id.* at 432. This conclusion was buttressed by the general principle that plaintiffs who place their physical condition in dispute cannot shield disclosure of material that is necessary to the defense of their action. *Id.* at 428.

[92] CV06-0432 (ADS) (WDW), slip op. (E.D.N.Y. Feb. 24, 2012).

[93] *Id.* at 2–3.

profile picture for evidence.[94] Because there was thus no factual predicate from which to infer there was relevant information on the plaintiff's private page, the court would not allow access to the private information.[95]

Based on these cases, it is clear there must be some evidence on the person's public pages that will allow an inference that further information would be located on the individual's private pages.[96] Attorneys could present such evidence to the court in a number of ways, including dated screenshots capturing the information and real-time accessing of the accounts in court.[97] Given the susceptibility of social media to rapid change (and possible deletion) of information, preservation of information through screenshots that can be authenticated may be the best way to present evidence to a judge or jury.[98]

B. *Privacy*

Courts have made clear that it is unreasonable to expect that disclosures made over social media will remain private.[99] Information conveyed through social media is public information that is not subject to any privileges.[100] As the California Court of Appeal stated in *Moreno v. Hanford Sentinel, Inc.,*[101] once an affirmative action is taken to publish information, that information is no longer a private fact and is now within the public domain.[102]

Similarly, in *McMillen v. Hummingbird Speedway*,[103] the Pennsylvania Court of Common Pleas noted that "it would be unrealistic to expect that such disclosures would be considered confidential."[104] The court in *McMillen* even took it a step further: The terms of use of both Facebook and MySpace clearly put users on notice that the information shared will not be kept private; thus, users cannot claim that the information is private or privileged after the fact.[105] In sum, it appears that while individuals may have a reasonable expectation of privacy

---

[94] *Id.*

[95] *Id.* at 3.

[96] *See, e.g.,* Sterling v. May, No. 106493-2009, slip op. at 1–2 (N.Y. Sup. Ct. Nov. 18, 2011) (holding that mere testimony that someone has a social networking account without any further facts does not establish an inference that a private page would lead to the disclosure of admissible evidence).

[97] Timothy Flynn, *Authenticating Social Media Evidence for Trial*, Laywernomics (Dec. 17, 2012), lawyernomics.avvo.com/social-media/authenticating-social-media-evidence-for-trial.html.

[98] *Social Media: From Chat Room to Courtroom*, Kroll Ontrack, www.krollontrack.com/resource-library/legal-articles/imi/social-media-from-chat-room-to-courtroom/ (last visited June 24, 2013).

[99] McMillen v. Hummingbird Speedway, Inc., No. 113-2010 CD, 2010 WL 4403285, at *3 (Pa. C.P. Civ. Div. Sept. 9, 2010).

[100] *Id.* at 2–3.

[101] 91 Cal. Rptr. 3d 858 (Ct. App. 2009).

[102] *Id.* at 862.

[103] No. 113-2010 CD, 2010 WL 4403285 (Pa. C.P. Civ. Div. Sept. 9, 2010).

[104] *Id.* at *3.

[105] *Id.* at *4–5.

in general, that expectation does not extend to situations where they share information, even if they keep it confined to a non-public page.

C. *Subpoenas to Identify Anonymous Posters*

In many instances, plaintiffs do not know the identity of the defendants they seek to sue, as persons posting harmful or defamatory content often do so anonymously. In an attempt to solve this problem, plaintiffs may file suit and then serve a subpoena upon an Internet service provider to obtain the identity of the person using a particular IP address.[106] Courts facing challenges to such subpoenas must balance the defendant's right to anonymous Internet speech against the plaintiff's need for discovery to redress harm caused by actionable speech.[107]

In *Doe I v. Individuals*,[108] two female students at Yale Law School brought suit against unknown individuals using thirty-nine different usernames on a website discussion board called AutoAdmit.com.[109] Some of the messages about the two girls included: "hope[ ] she gets raped and dies" and "Rate this HUGE breasted cheerful big tit girl from YLS."[110] After filing suit, the plaintiffs issued a subpoena duces tecum to AT&T seeking information about the person assigned to the IP address from which an individual using the name AK47 had posted certain of the comments.[111] AT&T sent a letter to the person whose IP address corresponded with the AK47 account, notifying him that it had been ordered to produce information relating to that account.[112]

AK47, or Doe 21, filed a motion to quash, claiming that disclosure of his identity would violate his First Amendment right to anonymous speech.[113] In denying this motion, the United States District Court for the District of Connecticut examined a number of factors relevant

---

[106] An IP address is the "numeric address of a computer on the Internet." It uniquely identifies each computer that is linked to the Internet. *IP address*, Merriam-Webster, http://www.merriam-webster.com/dictionary/ip%20address (last visited June 24, 2013). Internet service providers, like Verizon and AT&T, can either permanently assign an IP address to a computer or supply an IP address each time a computer connects to the Internet. *Id.*

[107] SaleHoo Grp., Ltd. v. ABC Co., 722 F. Supp. 2d 1210, 1214 (W.D. Wash. 2010).

[108] 561 F. Supp. 2d 249 (D. Conn. 2008).

[109] *Id.* at 251.

[110] *Id.*

[111] *Id.* at 252.

[112] *Id.* The Stored Communications Act ("SCA") requires this notice. Mark S. Sidoti et al., *How Private Is Facebook Under the SCA?*, Law Technology News (Oct. 5, 2010), http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202472886599&How_Private_Is_Facebook_Under_the_SCA. The SCA attempts to protect private communications from disclosure by Internet-based providers, including social media providers. *Id.* Critics have complained that the SCA is outdated and that courts struggle to apply the statute to modern forms of electronic communications. *Id.*

[113] *Doe I*, 561 F. Supp. 2d at 253.

to the balancing of the plaintiffs' and defendant's competing interests, including whether the plaintiffs had made an adequate evidentiary showing against the defendant. As to this factor, the court found that the "most appropriate balance" between the right to anonymous speech and the right to redress wrongs is struck when a plaintiff can make a "concrete showing" as to each element of a prima facie case against the defendant—i.e., that there is "a factual and legal basis for believing [actionable speech] has occurred . . . ."[114] Accordingly, because the plaintiff was able to adduce sufficient evidence to support a prima facie case for libel, her interest in pursuing discovery outweighed Doe 21's First Amendment right to speak anonymously.[115]

In *Solers, Inc. v. Doe*,[116] the court adopted a more stringent test. There, Doe reported Solers to the Software & Information Industry Association ("SIIA") for copyright infringement.[117] Solers then filed suit and served a subpoena on the SIIA to determine Doe's identity. Analyzing the standard necessary to force a third party to reveal the identity of a defendant charged with defamation, the District of Columbia Court of Appeals held that a plaintiff cannot gain the identity of an anonymous defendant unless he or she can plead facts sufficient to defeat a motion for summary judgment by "proffer[ing] evidence creating a genuine issue of material fact on each element of the claim that is within its control."[118]

At least four jurisdictions have adopted a standard similar to *Solers*,[119] and at least four have adopted a standard similar to *Doe I*.[120] And while there is presently no consensus on the appropriate standard for testing the validity of a subpoena seeking the identity of an

---

[114] *Id.* at 255–56 (addressing different courts' interpretations of what constitutes adequate showing).

[115] *Id.* at 257. While this case focused on libel, all states have since enacted statutes aimed at cyberstalking and cyberharassing, targeting people who harass, threaten, or bully others online. For a complete list of state statutes, *see State Cyberstalking and Cyberharassment Laws,* NCSL (Nov. 16, 2012), http://www.ncsl.org/issues-research/telecom/cyberstalking-and-cyberharassment-laws.aspx.

[116] 977 A.2d 941 (D.C. 2009).

[117] *Id.* at 945.

[118] *Id.* at 954 (emphasis in original omitted). *See also* Doe v. Cahill, 884 A.2d 451, 460 (Del. 2005); Dendrite Int'l, Inc. v. Doe No. 3, 775 A.2d 756, 760–61 (N.J. Super. Ct. App. Div. 2001). In *Solers*, the court adopted a five-prong test for ruling on a motion to quash a subpoena seeking the identity of an anonymous defendant: "(1) ensure that the plaintiff has adequately pleaded the elements of the defamation claim, (2) require reasonable efforts to notify the anonymous defendant that the complaint has been filed and the subpoena has been served, (3) delay further action for a reasonable time to allow the defendant an opportunity to file a motion to quash, (4) require the plaintiff to proffer evidence creating a genuine issue of material fact on each element of the claim that is *within its control,* and (5) determine that the information sought is important to enable the plaintiff to proceed with his lawsuit." *Id.* (emphasis in original).

[119] *Id.* at 952–54 (noting that New Jersey, Maryland, and Delaware have adopted a summary judgment standard similar to that in *Solers*). This test is sometimes referred to as the *Dendrite* or *Cahill* test. *See supra* note 118.

[120] *See Doe I*, 561 F. Supp. 2d at 256 (noting that Wisconsin, California, New York, and Connecticut have adopted similar motion to dismiss standards).

anonymous Internet user, at least one court has stated that courts have begun to "coalesce around" the summary judgment test adopted in *Solers*.[121]

V.
Issues at Trial

A. *"Voir Google"*

Voir dire is a crucial step for attorneys in evaluating a panel of potential jurors. Social networking now allows attorneys to search for information to impeach or challenge a juror simply by searching for the juror's name on the Internet. Attorneys have also turned to social networking sites to find a basis for rehearing based on lack of candor by members of the venire.[122]

Such was the case in *State v. Dellinger*.[123] There, approximately one week before trial, a juror sent a message to the defendant through MySpace.[124] The juror and the defendant then became MySpace friends.[125] When the panel was asked whether any of them had a relationship with the defendant, the juror remained silent.[126] The defendant eventually realized he was MySpace friends with the juror after the verdict was announced.[127]

In the ensuing investigation, the juror stated she "knew" the defendant, even though she never indicated that she knew him at the trial.[128] At a subsequent hearing on the juror misconduct issue, the juror testified that although she had a MySpace connection with the defendant, she did not respond because "I just didn't feel like I really knew him. I didn't know him personally."[129] She stated that being connected on MySpace "isn't that important."[130]

According to the West Virginia Supreme Court of Appeals, the juror's lack of candor "undermined the purpose of *voir dire* and, as a result, deprived the Appellant of the ability to

---

[121] SaleHoo Grp., Ltd. v. ABC Co., 722 F. Supp. 2d 1210, 1214 (W.D. Wash. 2010).

[122] *See infra* Part IV.C.

[123] 696 S.E.2d 38 (W. Va. 2010).

[124] *Id.* at 40. In the message, the juror told the defendant "Hey, I dont [sic] know you very well But I think you could use some advice! I havent [sic] been in your shoes for a long time but I can tell ya [sic] that God has a plan for you and your life . . . ." *Id.*

[125] *Id.*

[126] *Id.* The defendant claimed that at that time he did not recognize the juror as being the same person that sent him the message. *Id.* According to him, the juror looked much different from her MySpace photograph. *Id.*

[127] *Id.*

[128] *Id.* at 41.

[129] *Id.*

[130] *Id.*

determine whether she harbored any prejudices or biases against him."[131] Citing inconsistencies in the juror's statements and her repeated silence during voir dire, the court concluded that bias must be presumed, entitling the defendant to a new trial.[132]

As to friendships with a party's relatives, the question of candor becomes more complex. In *Sluss v. Commonwealth*,[133] a defendant convicted of murder sought a new trial based on juror misconduct after he learned that two jurors were Facebook friends with the mother of his alleged victim.[134] During voir dire, neither juror indicated they knew the victim's family.[135] According to the Supreme Court of Kentucky, a Facebook "friendship" does not carry the weight of a true friendship or relationship in the community because people can be Facebook "friends" with people with whom they have no actual connection.[136] Thus, such a "friendship" is not enough, by itself, to warrant a presumption of juror bias.[137] Rather, when a juror knows someone acquainted with a case, the question becomes "the extent of the interaction and the scope of the relationship."[138] In this case, though, the jurors' misstatements about their Facebook use prevented further exploration during voir dire of the possible relationship between the jurors and the victim's mother.[139] As a result, defendant was entitled to a new trial so he could explore whether the jurors were in fact fair and impartial.[140]

As *Dellinger* and *Sluss* make plain, conducting thorough research of jurors before trial is critical.[141] In fact, one court has stated that because of the advances in technology, litigants can no longer "lie in wait" until after a verdict has been rendered before bringing to the court's attention matters relating to the impeachment of jurors.[142]

Many attorneys already use the Internet to vet potential jurors, but are hesitant to discuss their methods without a definitive ethics statement condoning the practice.[143] The practice has, however, been deemed acceptable by New York County, which noted that it is both

---

[131] *Id.* at 43.

[132] *Id.* at 44–45.

[133] 381 S.W.3d 215 (Ky. 2012)

[134] *Id.* at 220–21.

[135] *Id.* at 221.

[136] *Id.* at 222.

[137] *Id.*

[138] *Id.* at 223.

[139] *Id.* at 223–24.

[140] *Id.* at 229. The court provided guidance that it must be determined when the jurors became Facebook "friends" with the victim's mother, whether the jurors' alleged Facebook accounts are in fact owned by the jurors, and the nature and extent of the jurors' relationships with the victim's mother. *Id.*

[141] *Id.* at 227.

[142] *See* Johnson v. McCullough, 306 S.W.3d 551, 558–59 (Mo. 2010).

[143] *Sluss*, 381 S.W.3d at 227 (citing Brian Grow, *Internet v. Courts: Googling for the Perfect Juror,* Reuters (Feb. 17, 2011), http://us.mobile.reuters.com/article/technology News/id USTRE 71 G 4 VW 20110217).

proper and ethical for lawyers to undertake a pretrial search of prospective juror's social networking sites, as long as they do not contact the prospective juror, "friend" the juror, or subscribe to the juror's accounts.[144]

As these authorities teach, lawyers can and should investigate whether prospective jurors have social media pages. If they do, the lawyer should be allowed to explore whether a prospective juror has a connection through these sites with any party (or relative of a party).[145] If such a connection is found, the attorney should be allowed to inquire into the nature and extent of the relationship to determine whether the juror is biased.[146] To avoid any challenge for timeliness, the attorney should attempt to conduct these inquiries at the earliest possible stage of trial.[147]

B. *Evidence Authentication*

Increasingly, attorneys turn to social media to prove facts at trial. While statements made in social networking settings may be potentially relevant, such evidence cannot be admitted at trial without proper authentication. At a minimum, this requires the proponent to "produce evidence sufficient to support a finding that the item is what the proponent claims it is."[148] In the context of social media, it can be difficult to authenticate statements made on social networks, especially when anyone can create a profile and claim to be whomever they want.[149]

Griffin v. State[150] highlights the many problems associated with authentication and social networking accounts. In *Griffin*, the Court of Appeals of Maryland was tasked with determining the proper way to authenticate information printed from a MySpace page.[151] There, Griffin was charged with the shooting death of an individual in Maryland.[152] At trial, the State wanted to introduce into evidence statements allegedly made by Griffin's girlfriend on her MySpace account to show she had allegedly threatened a witness called

---

[144] NYCLA Comm. on Prof'l Ethics, Formal Op. 742 (Apr. 16, 2010), *available at* http://www.nycla.org/siteFiles/Publications/Publications1348_0.pdf. This same procedure was subsequently adopted in Kentucky in *Sluss*, 381 S.W.3d at 228.

[145] *See Sluss*, 381 S.W.3d at 229 (suggesting that attorneys should be allowed to question potential jurors as to their Facebook "friends").

[146] *See id.* (noting that once a Facebook "friend" with a key party is revealed, attorneys should be able to ask follow-up questions about the connection).

[147] *See Johnson*, 306 S.W.3d at 559 (noting that litigants should not be allowed to lie in wait and must endeavor to prevent retrials by making early investigations into jurors).

[148] Fed. R. Evid. 901.

[149] *See* U.S. v. Drew, 259 F.R.D. 449, 452 (C.D. Cal. 2009) (where Lori Drew posed as a teenage boy named Josh Evans on MySpace to contact a teenage girl through MySpace).

[150] 19 A.3d 415 (Md. 2011).

[151] *Id.* at 416–17.

[152] *Id.* at 418.

by the State.[153] The profile in question was under the name of "Sistasouljah"; described a 23-year-old female from Port Deposit, Maryland with a birth date of "10/02/1983"; and contained a photo of the defendant and the girlfriend in an embrace.[154] The blurb on the pages read: "JUST REMEMBER SNITCHES GET STITCHES!! U KNOW WHO YOU ARE!!"[155] Instead of calling the girlfriend to authenticate her own MySpace page, the State attempted to authenticate the page through the testimony of a police sergeant.[156]

The court noted the problems with authenticating evidence from a MySpace page.[157] As the court explained, anyone can create a MySpace profile, and an outsider would not know whether the profile, or statements posted by the purported account owner, is legitimate.[158] Thus, the potential for promulgating fabricated or tampered information on a social media site was significant.[159] Given the potential for manipulation, ESI requires "greater scrutiny of 'the foundational requirements' than letters or other paper records, to bolster reliability."[160] Noting that the picture of the girlfriend, along with her birth date and location, were "not sufficient 'distinctive characteristics'" to authenticate the profile as belonging to the girlfriend, the court held the evidence should not have been admitted at trial.[161]

The court identified three methods of authenticating printouts from social networking sites. First, attorneys could ask the purported creator if he or she in fact created the profile and the post in question.[162] Second, attorneys could search the computer of the person who may have created the profile and post, and examine the computer's Internet history and hard drive to determine if the computer was used to originate the social media profile and post.[163] Last, attorneys could attempt to obtain information directly from the social media website where the profile was created.[164] The dissent rejected the majority's concerns as going to

---

[153] *Id.*

[154] *Id.*

[155] *Id.*

[156] *Id.*

[157] *Id.* at 419–22.

[158] *Id.* at 420–21.

[159] *Id.* at 422.

[160] *Id.* at 423. The court also noted three other jurisdictions (Massachusetts, New York, and the Seventh Circuit) that have suggested the same requirement of heightened scrutiny for electronic evidence on social networking sites because of the potential for manipulation and lack of transparency. *Id.* at 425–26.

[161] *Id.* at 423–24.

[162] *Id.* at 427.

[163] *Id.*

[164] *Id.* at 428. The court noted that this particular method was successfully used in *People v. Clevenstine*, where a legal compliance officer from MySpace explained that the "messages on the computer disk had been exchanged by users of accounts created by [the defendant] and the victims." *Id.* (quoting People v. Clevenstine, 68 A.D.3d 1448, 1450 (N.Y. App. Div. 2011)).

the weight of the evidence, not its admissibility, and argued that the evidence should be admitted "[a]s long as a reasonable juror could conclude that the proffered evidence is what its proponent purports it to be . . . ."[165]

Whether the *Griffin* standard is too high to be practical remains to be seen. Some courts have gone a different route, relying instead on circumstantial evidence to authenticate information on social networking pages.[166] Others have suggested that expert testimony as to the security of web pages and the workings of social networking accounts might be enough to authenticate statements on social networking sites.[167]

C. *Juror Misconduct and Due Process Rights*

Social media has impacted jurors by affording them greater opportunities to conduct research about cases and communicate with other jurors and non-jurors.[168] The resulting potential for juror misconduct pervades courts worldwide: In England, a juror conducted an informal poll on Facebook to decide whether a defendant was guilty.[169] In Australia, the government amended its Juries Act to raise the potential fine for jurors who improperly use the Internet during trial.[170] In New Zealand, a judge prevented the media from printing the names or images of two defendants on trial for fear that jurors would conduct online research.[171] Indeed, the Internet has changed the landscape of juror misconduct: From 1999 to 2010 in the United States, at least ninety verdicts were challenged because of a juror's alleged Internet misconduct.[172]

---

[165] *Id*. at 429–30 (Harrell, J., dissenting).

[166] *See* In re Interest of F.P., 878 A.2d 91, 95 (Pa. Super. Ct. 2005) (where the court used circumstantial evidence, such as defendant referring to himself and statements that mirrored real life testimony, to establish that an instant messaging account under the name "Icp4Life30" belonged to appellant). *See also* Tienda v. State, 358 S.W.3d 633, 645 (Tex. Crim. App. 2012) (where a MySpace page was authenticated based on circumstantial evidence, including numerous photographs of appellant that featured unique body tattoos; references to a gang, a shooting and the victim of the shooting; and an email address listing that matched appellant's).

[167] *See* Commonwealth v. Williams, 926 N.E.2d 1162, 1172–73 (Mass. 2010) (suggesting that an expert witness with knowledge about MySpace could authenticate information on a MySpace page).

[168] Thaddeus Hoffmeister, *Google, Gadgets, and Guilt: Juror Misconduct in the Digital Age*, 83 U. Colo. L. Rev. 409, 409 (2012).

[169] *Id.* at 413 (citing Urmee Khan, *Juror Dismissed from a Trial After Using Facebook to Help Make a Decision*, Telegraph (Nov. 24, 2008, 10:01 AM), http://www.telegraph.co.uk/news/newstopics/lawreports/3510926/Juror-dismissed-from-a-trail-after-using-Facebook-to-help-make-a-decision.html).

[170] *Id.* (citing Ellen Whinnett, *DIY Jury Probe*, Herald Sun (May 9, 2010, 12:00 AM), http://www.heraldsun.com.au/news/diy-jury-probe/story-e6frf7jo-1225864033798).

[171] *Id.* (citing Edward Gay, *Judge Restricts Online Reporting of Case*, N.Z. Herald (Aug. 25, 2008, 5:06 PM), http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10528866).

[172] Brian Grow, *As jurors go online, U.S. trials go off track*, Reuters (Dec. 8, 2010, 1:48 PM EST), http://www.reuters.com/article/2010/12/08/internet-jurors-idUSN0816547120101208.

Unfortunately, improper use of social media is difficult to detect. In 2011, 79% of judges said "they had no way of knowing whether jurors had violated a social-media ban."[173] When judges have discovered such violations, however, they have taken stiff measures, with some going as far as holding the offending juror in contempt.[174]

Jurors, though, seem oblivious to the problem of using social media during a trial. During the corruption trial of former Baltimore Mayor Sheila Dixon, five jurors became Facebook "friends."[175] When the judge learned of the "friendships," he held a hearing on the matter.[176] Following the hearing, one juror wrote on his Facebook page "F--- the Judge."[177] When asked about the comment, the juror told the judge, "[T]hat's just Facebook stuff."[178]

What jurors fail to realize is that their posts on social networks can be construed as bias against one of the parties.[179] A prejudiced juror or a juror that has been influenced by extraneous information is especially problematic in criminal cases where the Sixth Amendment grants defendants the due process right to an impartial jury.[180] Personal biases as expressed through social media were discussed at length in *State v. Goupil.*[181] There, a juror wrote on

---

[173] Steve Eder, *Jurors' Tweets Upend Trials*, Wall Street Journal (Mar. 5, 2012, 8:10 PM), http://online.wsj.com/article/SB10001424052970204571404577255532262181656.html.

[174] *See id.* (where a Florida juror was held in contempt and sentenced to three (3) days in jail for attempting to friend a defendant in a case); Martha Neil, *Juror Held in Contempt, Gets Community Service for Effort to Friend Defendant on Facebook*, ABA Journal (Aug. 29, 2011, 2:55 PM CDT), http://www.abajournal.com/news/article/juror_held_in_contempt_gets_community_service_for_contacting_defendant/ (where a Texas juror was held in contempt and sentenced to two days of community service after attempting to friend the defendant in his case); *Facebook juror sentenced to eight months for contempt*, BBC News (June 16, 2011, 9:53 ET), http://www.bbc.co.uk/news/uk-13792080 (where a British juror was held in contempt and sentenced to a suspended two month jail term for contacting the defendant via Facebook); *Oregon Juror Jailed For Texting During Trial*, CBS Seattle (Apr. 18, 2013, 7:12 PM), http://seattle.cbslocal.com/2013/04/18/oregon-juror-jailed-for-texting-during-trial/ (where a juror was caught texting and held in contempt).

[175] Grow, *supra* note 172.

[176] *Id.*

[177] *Id.*

[178] *Id.*

[179] *See* Eder, *supra* note 173 (noting that judges instruct jurors against communicating with anyone about the case because they are concerned that such communications could be construed as bias about the case).

[180] U.S. Const. amend. VI ("In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed, which district shall have been previously ascertained by law, and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to have the Assistance of Counsel for his defence."). The Sixth Amendment is incorporated upon the states through the Fourteenth Amendment. U.S. Const. amend. XIV.

[181] State v. Goupil, 908 A.2d 1256 (N.H. 2006).

his blog prior to jury selection, "Lucky me, I have Jury Duty! Like my life doesn't already have enough civic participation in it, now I get to listen to the local riff-raff try and convince me of their innocence."[182] After he was impaneled, but before trial, the juror continued blogging: "After sitting through 2 days of jury questioning, I was surprised to find that I was not booted due to any strong beliefs I had about police, God, etc."[183] Based on these blog entries, the defendant sought to vacate his conviction based on alleged juror misconduct.[184] The Supreme Court of New Hampshire disagreed, finding nothing in the record indicated personal bias of the juror.[185]

Use of social media also potentially exposes jurors to prejudicial extraneous information. In *Commonwealth v. Guisti*,[186] the Supreme Judicial Court of Massachusetts considered whether a defendant was deprived of a fair trial when, during trial, a juror posted the following message to a listserv: "stuck in a 7 day-long Jury Duty rape/assault case … missing important time from the gym, working more hours and getting less pay because of it! Just say he's guilty and lets [sic] get on with our lives!"[187] The court found that, though the statement itself did not involve extraneous matter, it was unclear whether the juror received any responses to her posting.[188] The possibility of such responses left the juror vulnerable to receiving information about the case that could have exposed her to external influences.[189] As a result, the trial court should have granted the defendant's postverdict motion for voir dire of the juror, and its failure to do so required that the case be remanded for a hearing to determine whether: (1) the juror was the person who posted the message; (2) if so, whether the juror received any responses to her messages; (3) the content of any such messages; and (4) whether the juror communicated the substance of any responses to any of her fellow jury members during the course of deliberations.[190]

As one court has observed: "No matter what the instructions may be, they are only as effective as the integrity of the juror who hears them."[191] The same judge has even wondered whether sequestration may be the ultimate end point to ensure that jurors do not use the

---

[182] *Id.* at 214.

[183] *Id.*

[184] *Id.* 217–18.

[185] *Id.* at 219.

[186] 747 N.E.2d 673 (Mass. 2001).

[187] *Id.* at 678–79.

[188] *Id.* at 679–80.

[189] *Id.* at 680.

[190] *Id.*

[191] People v. Jamison, 24 Misc. 3d 1238(A), 2009 WL 2568740, at *6 (N.Y. Sup. Ct. Aug. 18, 2009), *aff'd*, 95A.D.3d 1236 (N.Y. App. Div. 2012).

Internet to obtain outside information.[192] For now, strict admonitions will have to suffice, even though some jurors will be unable to resist the temptation to ignore them.[193]

VII.
Ethical Considerations

The American Bar Association (ABA) Commission on Ethics 20/20 (the "20/20 Commission") conducted a three-year study of how technology has transformed the practice of law.[194] Despite finding that technology has fundamentally changed the practice,[195] the study concluded that a complete overhaul of the rules was not necessary, instead suggesting only minor changes.[196]

At the 20/20 Commission's suggestion,[197] the Model Rules of Professional Conduct now include a provision that competent attorneys must "keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology."[198] Though not binding, this rule is a strong indication that basic professional responsibility requires that judges and attorneys stay up-to-date with changes in technology.

A. *Judges and Social Media*

Not only are judges creating social media profiles, some use social media to research the attorneys and parties before them.[199] According to the ABA, judges may participate in social networking, but they must comply with all relevant provisions of the Code of Judicial

---

[192] *Id.*

[193] *Id.*

[194] *Commission on Ethics 20/20, Introduction and Overview,* ABA (2012), http://www.americanbar.org/content/dam/ABA/administrative/ethics_2020/20120508_ethics_20_20_final_hod_introdution_and_overview_report.authcheckdam.pdf.

[195] *Id.* at 3.

[196] *Id.* at 2.

[197] *Id.* at 8.

[198] Model Rules of Prof'l Conduct, R. 1.1 cmt. 8 (2013).

[199] *See* Molly McDonough, *Facebooking Judge Catches Lawyer in Lie, Sees Ethical Breaches #ABAChicago*, ABA J. (July 31, 2009, 3:16 PM), http://www.abajournal.com/news/article/facebooking_judge_catches_lawyers_in_lies_crossing_ethical_lines_abachicago/ (where one judge recounted using Facebook to find out that an attorney had lied when giving the reason for requesting a continuance); Purvis v. Comm'r of Soc. Sec., Civ. No. 09-5318(SDW)(MCA), 2011 WL 741234, at *7 n.4 (D.N.J. Feb. 23, 2011) (where judge noted that during her own research, she looked at profile picture on plaintiff's Facebook page); *Defendant's post-plea rant on Craigslist costs him sentence reduction for accepting responsibility*, Sentencing Law and Policy, Nov. 29, 2010, http://sentencing.typepad.com/sentencing_law_and_policy/2010/11/defendants-post-plea-rant-on-craigslist-costs-him-sentence-reduction-for-accepting-responsibility.html (where a judge used a defendant's statement on Craigslist as evidence that the defendant had not accepted responsibility for his crimes).

Conduct and "avoid any conduct that would undermine the judge's independence integrity, or impartiality, or create an appearance of impropriety."[200]

As to a judge's "friends" on social networking sites, the context of the relationships matter.[201] In the *Public Reprimand of B. Carlton Terry, Jr.*,[202] a presiding judge "friended" one of the attorneys before him.[203] The judge and the attorney had a Facebook exchange about the case on two separate occasions.[204] The Judicial Standards Commission for North Carolina found that these exchanges constituted ex parte communications with counsel in a matter before the judge, which was a violation of the rules of judicial conduct.[205] As a result, the judge was reprimanded.[206]

In a contrasting case, a judge had a previous Facebook relationship with the father of the girlfriend of a defendant before him.[207] Approximately one week before the defendant entered a plea, the father sent the judge a Facebook message requesting leniency for the defendant.[208] In response, the judge advised the father that the message violated the rules against ex parte communications; that the judge stopped reading the message when he realized it was improper; and that any further communications about any pending legal matter would result in "de-friending."[209] At the hearing on the defendant's motion for a new trial based in part on the ex parte communication, the judge testified he knew the father because both ran for office during the same election cycle, but that was "the extent of [their] relationship."[210] Noting that "[m]erely designating someone as a 'friend' on Facebook 'does not show the

---

[200] ABA Standing Comm. on Ethics and Prof'l Responsibility, Formal Op. 462 (2013).

[201] *See* Youkers v. Texas, No. 05-11-01407-CR, slip op. at 7 (Tex. Ct. App. May 15, 2013) (noting that context is necessary to understand whether judges "friending" someone is prejudicial).

[202] Inquiry No. 08-234 (N.C. Jud. Stds. Comm'n 2008), *available at* http://www.aoc.state.nc.us/www/public/coa/jsc/publicreprimands/jsc08-234.pdf .

[203] *Id.* at 2.

[204] *Id.* The conversations included a post on Facebook by the attorney asking: "[H]ow do I prove a negative. [sic]" The judge responded that he had "two good parents to choose from" and that he "feels he will be back in court." The attorney then responded that he "ha[s] a wise judge." In the second conversation, the judge wrote on Facebook that "he was in his last day of trial." The attorney responded, "I hope I'm in my last day of trial." The judge replied, "[Y]ou are in your last day of trial." *Id.* The judge also visited one of the parties' websites about four times. *Id.* at 3.

[205] *Id.* at 3–4.

[206] *Id.* at 4–5.

[207] *Youkers*, No. 05-11-01407-CR, at 3.

[208] *Id.*

[209] *Id.* at 4. The judge also advised the father that he would place a copy of the message in the court's file, tell the lawyers about the message, and contact the judicial conduct commission to determine if anything further was required. *Id.*

[210] *Id.* at 3.

degree or intensity of a judge's relationship with a person'"[211] and given the judge's quick disclosure of the communication, the Court of Appeals for the Fifth District of Texas found no implication of bias.[212] Thus, judges may use social media, but they should be aware of the context of their relationships before they "friend" an individual.[213]

B. *Attorneys and Social Media*

As potential clients turn to the Internet to contact attorneys, it can be unclear when an attorney-client relationship is formed. The 20/20 Commission proposed changes to the Model Rules to clarify when communications over blogs or social networking sites create an attorney-client relationship.[214] Now, "a person who *consults* with a lawyer about the possibility of forming a client-lawyer relationship with respect to a matter is a prospective client."[215]

The 20/20 Commission, though, did not attempt to define just what use an attorney can make of a social networking site.[216] Instead, state bar associations have sought to fill the gap through their current ethics rules. New York, for example, has stated that attorneys may ethically access the public pages of another party's social networking site to gather information in pending litigation; however, they may not "friend" the other party or direct a third party to do so.[217] The Philadelphia Bar Association has similarly stated that it would be unethical for an attorney to have a third-party "friend" an unrepresented, adverse witness.[218]

---

[211] *Id.* at 7 (quoting ABA Op. 462).

[212] *Id.* at 9.

[213] Kentucky, New York, Ohio, and South Carolina seem to agree with this assessment. Supreme Court of Ohio Board of Commissioners on Grievances and Discipline, Op. 2010-7 at 5–8 (2010). Florida has stated that judges may not add lawyers who appear before them as "friends" on social networking sites. *Id.* at 6.

[214] ABA Commission on Ethics 20/20, *supra* note 194, at 10.

[215] Model Rules of Prof'l Conduct R. 1.18(a) (2013). The word "consults" replaced the former language of "discussion," which implied a two-way verbal exchange between attorney and client. ABA Commission on Ethics 20/20, *supra* note 194, at 10.

[216] Instead, the ABA has only issued a formal opinion regarding lawyer websites. ABA Standing Comm. on Ethics and Prof'l Responsibility, Formal Op. 10-457 (2010), *available at* http://www.americanbar.org/content/dam/ABA./migrated/2011_build/professional_responsibility/ethics_opinion_10_457.authcheckdam.pdf. There, the ABA indicated that when it comes to website content, "no website communication may be false or misleading, or may omit facts such that the resulting statement is material misleading." *Id.* at 1. The opinion stated an email is analogous to a phone or face-to-face conversation, but did not comment on whether this would apply to a Facebook or Twitter or other similar exchange. *Id.* at 4.

[217] N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Op. 843 (2010), *available at* http://www.nysba.org/Content/ContentFolders/EthicsOpinions/Opinions826900/EO_843.pdf.

[218] Phila. Bar Ass'n Prof'l Guidance Comm., Op. 2009-02 (2009), http://www.philadelphiabar.org/WebObjects/PBAReadOnly.woa/Contents/WebServerResources/CMSResources/Opinion_2009-2.pdf.

The State Bar of Arizona has commented that lawyers probably should not answer specific legal questions that are posted online because of the inability to screen for conflicts.[219]

Attorneys that decide to actively participate in social media must be cautious about what they share online. In *In re Peshek*,[220] an attorney published a blog with information about her work.[221] The blog contained confidential information about clients and derogatory comments about judges.[222] Because of the attorney's violation of client confidences, the Supreme Court of Illinois suspended her license to practice law for sixty days.[223] The Supreme Court of Wisconsin subsequently imposed an identical sixty-day suspension based on the same betrayal of client confidences.[224] In sum, attorneys may use social media, but they should be careful about what information they reveal on social networking sites.

VIII.
Conclusion

Social networking is now a part of the fabric of Internet use worldwide. Some jurisdictions like California, including the Court of Appeals for the Ninth Circuit, have embraced technology wholeheartedly. Others, like Maryland, have been more restrictive in the use of technology in the courtroom. Regardless of a given jurisdiction's position, attorneys and judges must be aware not only of how the technology works, but also how best to use it. Going forward, social media users should:

1. Pay attention to how they use social media to avoid playing the personal jurisdiction game;[225]
2. Be aware that 47 U.S.C. § 230 will likely bar any suit against an intermediary interactive computer service provider;[226]

---

[219] State Bar of Ariz. Ethics Op. 97-04 (1997), http://www.azbar.org/Ethics/EthicsOpinions/ViewEthicsOpinion?id=480.

[220] No. M.R. 23794, slip op. (Ill. May 18, 2010).

[221] *Id.* at 1.

[222] *Id.* In different entries, Peshek revealed a client's information by giving his jail identification number, by using a client's first name, and by using a derivative of a client's first name. *Id.* at 3. One entry revealed that a client had been under the influence of cocaine when he appeared before a judge, and another revealed that Peshek allowed a client to misinform the court about her drug use. *Id.* As to statements about judges, in one entry she called a judge "a total asshole," and in another called a judge "Judge Clueless." *Id.* at 4.

[223] *Id.* at 8.

[224] *In re Disciplinary Proceedings Against Peshek*, 798 N.W.2d 879, 881 (Wis. 2011).

[225] *See supra* Part II.

[226] *See supra* Part III.

3. Know how to use subpoenas and discovery effectively to obtain and preserve electronically stored information during the course of discovery;[227]
4. Learn how to use social media to their advantage by searching for information about jurors before and during voir dire and monitoring jurors throughout trial for potential misconduct;[228] and
5. Review their local jurisdiction's ethics opinions to determine how to use social media both effectively and ethically.[229]

[227] *See supra* Part IV.

[228] *See supra* Part V.

[229] *See supra* Part VI.