SMU Science and Technology Law Review

Volume 14 | Number 3 Article 8

January 2011

Digging for the Digital Dirt: Discovery and Use of Evidence from Social Media Sites

John G. Browning

Digging for the Digital Dirt: Discovery and Use of Evidence from Social Media Sites

*John G. Browning**

"The Internet has opened new channels of communication and self-expression . . . . Countless individuals use message boards, date matching sites, interactive social networks, blog hosting services, and video sharing websites to make themselves and their ideas visible to the world. While such intermediaries enable the user-driven digital age, they also create new legal problems."

-Fair Housing Council of San Fernando Valley v. Roommates.com, LLC 489 F.3d 921, 924 (9th Cir. 2007).

I. INTRODUCTION

Imagine encountering the following scenario during the litigation following an industrial accident: just as an expert witness is explaining how all required safety protocols and procedures were diligently followed, opposing counsel confronts him with postings from YouTube videos shot by some of the defendant company's own employees showing how they cut corners. Or perhaps the defendant driver in a devastating accident denies that he was in a hurry and not paying attention, only to be confronted with his own tweets about being behind schedule. For plaintiff's counsel, consider the sinking feeling when your client, a grieving widow who has just finished testifying about the void left by the loss of her husband, is impeached with salacious photos and postings from her boyfriend's MySpace page—all of which are dated months before the accident in which her husband was killed. And of course, there is nothing quite like the look on the face of a "severely and permanently injured" plaintiff who has spun his tale of woe for the jury about barely being able to walk and who now has to explain the photos from his Facebook page depicting his completion of a recent 10k run or a mountain climb in the Pacific Northwest.

Scenarios like these are occurring with increasing frequency in civil litigation—thanks not only to the explosive growth in and sheer pervasiveness of social media, but also to the legal profession's eagerness to exploit the treasure trove of information to be mined from social networking sites. Roughly half of Internet users in the United States have a profile on a social

---

* John G. Browning is the managing partner of the Dallas office of Lewis Brisbois Bisgaard & Smith LLP, where he handles a wide variety of civil litigation, including cyberliability and technology-related legal issues. He received his B.A. with general and departmental honors from Rutgers University in 1986 and his J.D. from the University of Texas School of Law in 1989. He is the author of *The Lawyer's Guide to Social Networking: Understanding Social Media's Impact on the Law* (West 2010).

networking site.[1] According to a recent Nielsen survey, individuals devote 22.7% of their online time to social networking.[2] Not only does this reflect an increase of 43% over the previous year, it also shows that social networking usage is growing more rapidly than any other online activity.[3] Facebook, founded in 2004 by Mark Zuckerberg as a way for Harvard University students to stay in touch, now boasts 600 million users.[4] Roughly half of all Facebook users visit the site at least once a day.[5] In March 2010, Facebook surpassed Google as the most-visited website in the world.[6] In December 2010 alone, Americans spent 49.3 billion minutes on Facebook.[7]

The social networking/micro-blogging site Twitter—which allows its users to "tweet" updates of up to 140 characters directly from their cell phones and other wireless devices—was founded in 2006.[8] Lured by such immediacy and simplicity, Twitter's ranks quickly swelled to 190 million users.[9] The site went from handling 20,000 tweets a day in 2007 to a staggering 65 million a day by 2010.[10] Even a site that bills itself as more professional and business-oriented, LinkedIn, has over 90 million members.[11]

1. *The Infinite Dial 2010: Digital Platforms and the Future of Radio*, EDISON RES. & ARBITRON, (Apr. 8, 2010), http://www.edisonresearch.com/home/archives/2010/04/the_infinite_dial_2010_digital_platforms_and_the_future_of_r.php.

2. *What Americans Do Online: Social Media and Games Dominate Activity*, NIELSEN WIRE, Aug. 2, 2010, http://blog.nielsen.com/nielsenwire/online_mobile/what-americans-do-online-socialmedia-and-games-dominate-activity/.

3. *Id.*

4. Nicholas Carson, *Facebook Has More Than 600 Million Users, Goldman Tells Clients*, BUSINESS INSIDER, (Jan. 5, 2011), http://www.businessinsider.com/facebook-has-more-than-600-million-users-goldman-tells-clients-2011-1.

5. Julianne Pepitone, *Facebook CEO has "made every mistake you can make,"* CNNMONEY.COM, (Nov. 16, 2010), http://money.cnn.com/2010/11/16/technology/zuckerberg_facebook_web2/index.htm.

6. Julianne Pepitone, *Facebook Traffic Tops Google For the Week*, CNNMONEY.COM, (Mar. 16, 2010), http://money.cnn.com/2010/03/16/technology/facebook_most_visited/.

7. *Facebook's Fast U.S. Growth Begins to Slow*, DALLAS MORNING NEWS, Jan. 23, 2011, at 3D.

8. Dominic Rushe, *How Twitter Has Become the People's Voice on the Eve of Its Fifth Birthday*, THE GUARDIAN, (Feb. 13, 2011), http://www.guardian.co.uk/technology/2011/feb/13/twitter-peoples-voice-fifth-birthday.

9. *Id.*

10. *Id.*

11. Brenton Cordeiro, *LinkedIn Plans to Raise up to $175 Million in IPO*, REUTERS, (Jan. 28, 2011), http://www.reuters.com/article/2011/01/28/us-linkedin-ipo-idUSTRE70Q8UA20110128.

Given this abundance of photos, video, statements, and other content flooding social networking sites, it is hardly surprising to find lawyers from virtually all areas of practice digging for such digital dirt. A February 2010 study conducted by the American Academy of Matrimonial Lawyers revealed that 81% of the attorneys responding reported finding and using evidence from social networking sites in their cases.[12] The most popular source of such information was Facebook, with 66% of all respondents indicating that they had found evidence on that site.[13] Prosecutors and criminal-defense attorneys alike have located useful—and sometimes case-making—information from social networking sites, as have family-law practitioners, personal-injury and products-liability specialists, employment lawyers, intellectual-property attorneys, defamation and media lawyers, insurance-coverage practitioners, and even securities litigators. The ranks of lawyers monitoring sites like Facebook and MySpace for useful tidbits of information encompass both the public and private sectors, and include not only outside counsel but in-house lawyers as well. In fact, a 2009 LexisNexis survey of corporate counsel revealed that use of social networks by those working in corporate legal departments had increased approximately 25% in 2009.[14]

Social media's inexorable spread across state, national, and even international boundaries, along with the Internet's transformative effect on how people conduct business, is changing traditional notions of jurisdiction. As one court observed, the Internet "makes it possible to conduct business throughout the world entirely from a desk top."[15] Courts across the country have wrestled with whether or not threatening YouTube videos, allegedly defamatory statements on LiveJournal, and even MySpace messages have been sufficient to warrant subjecting individuals in one state to a court's jurisdiction in another.[16]

As new media provides ever-increasing access to information that was once thought unavailable—and does so with the speed of a search engine—lawyers and courts have had to confront new problems in presenting cases.

12. *Big Surge in Social Networking Evidence Says Survey of Nation's Top Divorce Lawyers, Facebook is Primary Source for Compromising Information*, AMERICAN ACADEMY OF MATRIMONIAL LAWYERS, (Feb. 10, 2010), http://www.aaml.org/about-the-academy/press/press-releases/e-discovery/big-surge-social networking-evidence-says-survey-.

13. *Id.*

14. *Survey Reveals Substantial Growth in Online Social Networking by Lawyers Over the Past Year*, LEXISNEXIS PRODUCT CORNER, (Oct. 15, 2009), http://www.lexisnexis.com/community/ideas/blogs/product_corner/archive/2009/10/15/survey-reveals-socialnetworking-growth-.aspx.

15. Jones v. Beech Aircraft Corp., 995 S.W.2d 767, 772 (Tex. App.—San Antonio 1999, pet. dism'd w.o.j. [mand. denied]).

16. *See, e.g.*, Penachio v. Benedict, 2010 WL 4505996, at *1 (S.D.N.Y. Nov. 9, 2010); Miller v. Kelly, 2010 WL 4684029, at *1 (D. Colo. Nov. 12, 2010); State v. Pierce, 792 N.W.2d 83 (Minn. Ct. App. 2010).

Individuals who have long since grown accustomed to gathering news and information on everything from restaurant reviews to medical advice online are now populating the jury box. As a result, jurors are venturing online in increasing numbers to look up legal terms, view crime scenes on Google Earth, comment on the proceedings via Facebook, or even communicate with parties and witnesses through social media. Such online misconduct by "Googling jurors" has resulted in an alarming number of mistrials and overturned verdicts in recent years, prompting a number of states (including, most recently, Texas) to revise their jury instructions to address social media limitations.[17] By the same token, lawyers are exploiting people's tendency to reveal their online selves by scouring social media sites as part of the jury selection process—from voir dire to "voir Google," if you will.[18]

Litigators have seen evidence from social networking sites prove crucial in all kinds of cases—not just the incriminating Facebook statements of a criminal defendant, or the damaging Twitterpics or YouTube video in a bitter child-custody battle. Glowing testimonials on LinkedIn can make or break an employment case. Customer reviews and comments posted on social media sites have formed the evidence of likelihood of confusion that is so pivotal in trademark-infringement litigation.[19] Postings, and even something as seemingly trivial as a friend request, have surfaced in product-liability, insurance-coverage matters, and even securities litigation. In some instances, judges are not even waiting for parties to bring such evidence to them, but instead are taking judicial notice of it themselves. In one case, for example, a Social Security disability claimant sought additional benefits because of asthma.[20] After the Commission of Social Security denied the claim, an administrative-law judge upheld it and denied the claimant's appeal, finding that his symptoms were not credible.[21] The judge noted that, "in the course of its own research, it discovered one profile on what is believed to be Plaintiff's Facebook page where she appears to be smoking . . . . If accurately depicted, Plaintiff's credibility is justifiably suspect."[22]

17. Brian Grow, *As Jurors Go Online, U.S. Trials Go Off Track*, REUTERS, (Dec. 8, 2010), http://www.reuters.com/article/2010/12/08/us-internet-jurors-idUSTRE6B74Z820101208 (shows that since 1999, there have been at least 90 reported decisions involving verdicts challenged as a result of Internet-related juror misconduct).

18. Ana Campoy & Ashby Jones, *Searching for Details Online, Lawyers Facebook the Jury*, THE WALL STREET JOURNAL, (Feb. 22, 2011), http://online.wsj.com/article/SB10001424052748703561604576150841297191886.html.

19. Chipotle Mexican Grill, Inc. v. Chipotles Grill of Jonesboro, Inc., 2011 WL 2292357, at *4 (E.D. Ark. June 9, 2011).

20. Purvis v. Comm'r of Soc. Sec., 2011 WL 741234, at *1 (D. N.J. Feb. 23, 2011).

21. *Id.*

22. *Id.* at *7 n.4.

With the expanding use of social media evidence by lawyers, of course, come new professional risks and pitfalls. Attorneys must remain mindful of the fact that existing ethical rules apply to communications in the digital age as well. Lawyers have found themselves in ethical hot water for making Facebook posts about a case, betraying client confidences, criticizing a judge in blog posts, and sending tweets in which they link to sealed documents.[23] Even victorious attorneys have found their social media posts about time spent on a case and other issues sought during a post-trial dispute over attorney's fees.[24] And, as is discussed at greater length elsewhere in this article, several bar association ethics opinions have been issued dealing with the ethical questions raised by an attorney's use of social media sites while investigating and litigating a case.[25]

Clearly, the cultural tsunami that is social media is altering the legal landscape. Less than 10 years ago, there was no cause of action for defamation by Twitter, no crime of creating a false online persona, and it would not have been possible to serve a defendant with process via a social networking site—yet all three exist today.[26] This article will demonstrate that the body of case law developed thus far on the use of social networking is instructive on a whole host of discoverability and evidentiary issues, as litigants and courts alike grapple with what can be obtained from an opposing party's social networking profile, as well as how such content may be used in the courtroom. Litigators in all areas of civil litigation need to understand not only the types of useful evidence to be gleaned from social networking sites, but also how to go about locating and obtaining such evidence, as well as the authentication issues and privacy concerns that have been raised with respect to the admissibility of content from a social networking profile. For lawyers on either side of the docket, and across virtually any area of litigation, evi-

23. JOHN G. BROWNING, THE LAWYER'S GUIDE TO SOCIAL NETWORKING: UNDERSTANDING SOCIAL MEDIA'S IMPACT ON THE LAW 149-63 (2010).

24. Muniz v. United Parcel Serv., Inc., 2011 WL 311374, at *8 (N.D. Cal. Jan. 28, 2011).

25. *See, e.g.*, Philadelphia Bar Ass'n Prof'l Guidance Comm. Opinion 2009-02 (2009) (a lawyer may not use a third person who does not truthfully represent herself to "friend" a witness and obtain access to that witness's restricted social networking profile); New York City Bar Ass'n Comm. on Prof'l Ethics Formal Opinion 2010-02 (2010) (while a lawyer may access the publicly viewable pages of another party's social networking profile, he may not engage in trickery or misrepresentation in "friending" a witness to gain access to an otherwise private social networking page); San Diego County Bar Ass'n Legal Ethics Opinion 2011-02 (2011) (a lawyer may not "friend" the high-ranking employees of a party whom he knows to be represented by counsel).

26. *See* BROWNING, *supra* note 23.

dence from what Professor Daniel Solove has termed the "permanent chronicle of people's lives"[27] can be a potent weapon indeed.

II. What Is Out There and How to Get It

Courts have seemingly undergone a sea change in attitudes toward evidence originating from the Internet. Just twelve years ago, a federal court referred derisively to "voodoo information taken from the Internet," a source the judge regarded "as one large catalyst for rumor, innuendo, and misinformation," concluding that "any evidence procured off the Internet is adequate for almost nothing."[28] In more recent years, however, courts across the country have come to expect that lawyers will utilize online resources for everything from performing due diligence on a party being served[29] to jury selection.[30] At least one federal circuit court has recognized that it is perfectly acceptable for a judge to confirm his or her judicial intuition by conducting an Internet search.[31]

Lawyers love "smoking gun" revelations, and social media evidence can certainly provide those. Even popular culture has gotten into the act. During a first-season episode of the CBS legal drama *The Good Wife*, lawyers from the fictional Stern Lockhart Gardner firm were zealously representing a client needing an emergency medical procedure on her unborn child, for which she had been denied health insurance coverage.[32] On cross-examination, the defendant-insurer's lawyer confronted the husband and father about any misrepresentations he may have made when taking out the policy.[33] After he denied misleading the insurance company and acknowledged that on the application he stated he was a non-smoker, the husband was then impeached with photos from his Facebook page showing him smoking with buddies while on a camping trip.[34] With the speed of a search engine, the client's health care coverage was gone and the judge ruled in favor of the defendant.[35]

27. Daniel J. Solove, The Future of Reputation: Gossip, Rumor, and Privacy on the Internet 11 (2007).

28. St. Clair v. Johnny's Oyster & Shrimp, Inc., 76 F. Supp. 2d 773, 774–75 (S.D. Tex. 1999).

29. *See* Munster v. Groce, 829 N.E.2d 52, 61 n.3 (Ind. Ct. App. 2005) (recognizing the Internet as an acceptable means of "locating a missing litigant"); Dubois v. Butler *ex rel* Butler, 901 So. 2d 1029, 1031 (Fla. Dist. Ct. App. 2005).

30. *See* Carino v. Muenzen, No. L-0028-07, 2010 WL 3448071, at *9–10 (N.J. Super. Ct. App. Div. Aug. 30, 2010) (per curiam).

31. *See* United States v. Bari, 599 F.3d 176, 181 (2d Cir. 2010) (per curiam).

32. *The Good Wife: Heart* (CBS television broadcast Mar. 16, 2010).

33. *See id.*

34. *See id.*

35. *See id.*

To begin the search for social media evidence, see if the litigant or witness-in-question has any social networking profiles. This can be done within the confines of formal discovery, in which interrogatories are propounded inquiring about the party's use of such sites, screen names, passwords, and other account-related information. If it is preferable to proceed more informally, or if the subject is a witness or other non-party, conduct a search on Google, Bing, or other search engines for any social networking profile, or utilize search engines of social networking sites directly. Another option is to go to a site like Spokeo.com,[36] which aggregates information about any individual from many sites. If the subject is on multiple social media sites, this search should bring up any social media presence the individual has.

If an individual's online profile is privacy-restricted, and the subject is a party, more formal discovery efforts will be necessary. Assuming, however, that the individual has elected to keep most, if not all, of his or her profile publicly viewable, an abundance of information may be available. Studies show that a majority of social media users either decide to allow these profiles to remain public, or have an insufficient understanding of their privacy options,[37] making informal discovery a viable option. While photos, videos, and statements posted on a social networking site are what most lawyers seek during discovery, the evidentiary value of other features associated with such profiles should not be overlooked. For example, mood indicators and emoticons are often employed by a user to share his or her current mood. In personal-injury cases, the "smiley face" used by a plaintiff claiming to be in serious pain or severely depressed can be used against them. In a New York case involving allegations of police brutality, the officer in question was confronted not only with his Facebook status update that referenced watching the movie *Training Day*[38] "to brush up on proper police procedure," but also with the fact that his mood indicator had been set to "devious," complete with an angry red emoticon being licked by flames.[39]

Other often-overlooked features can also be used as valuable evidence in a case. The list of someone's Facebook "friends," for example, can lead to other potential witnesses or can itself serve as evidence to establish a witness's possible bias. Attorneys have also attempted, with varying degrees of success, to use status updates themselves as evidence. In *State v. Corwin*, the Missouri Court of Appeals upheld the exclusion of a sexual-assault victim's

36. SPOKEO.COM, http://www.spokeo.com (last visited Aug. 9, 2011).

37. *See* Alessandro Acquisti & Ralph Gross, *Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook*, PRIVACY ENHANCING TECHNOLOGIES WORKSHOP, CARNEGIE MELLON UNIVERSITY, at 13 (2006), *available at* http://citeseer.ist.psu.edu/viewdoc/summary?doi=10.1.1.73.2056. (reporting that nearly half of Facebook users surveyed gave incorrect answers when asked who could view their profiles on the site).

38. TRAINING DAY (Warner Bros. 2001).

39. *See* BROWNING, *supra* note 23, at 107-08.

Facebook status update.[40] In response to the victim's allegation of date rape, the defense tried to introduce status updates from other nights to purportedly demonstrate the victim's habit of binge drinking and inability to remember events.[41] The court held, however, that updates not "even tangentially related to the events of the night in question" were irrelevant and were properly excluded.[42] In November 2009, an armed-robbery suspect in New York was able to get all charges dismissed after his Facebook status update and other corroborating evidence—like server records and eyewitness testimony—established his alibi.[43] In one Canadian case, a plaintiff claimed that he was physically unable to return to his job, which involved office work at a computer.[44] However, the court upheld the defense's admission of the plaintiff's Facebook log-on/log-off server records to demonstrate his extensive late-night computer usage, thereby undermining the plaintiff's claims.[45]

Even basic profile information, like one's contacts or employer listed on LinkedIn, can be extremely useful evidence. In a recent age-discrimination case, casino gaming giant Harrah's maintained that it was not actually the plaintiff's employer.[46] However, in addition to showing that he received a Harrah's employee handbook and paychecks signed by Harrah's personnel, the plaintiff demonstrated that the primary defense witness—his supervisor—denied working for Harrah's on the stand yet identified Harrah's as his employer on his LinkedIn profile.[47] The judge found that the supervisor was not a credible witness and ruled for the plaintiff.[48]

Many lawyers assume that directly issuing a subpoena to a social networking site itself is the best way to formally obtain social media evidence. In reality, social networking sites are notoriously resistant to such efforts, perhaps due to the criticism and lawsuits leveled against them over alleged failures to protect user privacy. Sending subpoenas to social media sites raises privacy issues and Stored Communications Act[49] (SCA) implications that will be addressed later in this article. As a practical matter, a review of Facebook's view on its role in the discovery process reveals the potential futility of such actions.

40. State v. Corwin, 295 S.W. 3d 572, 579 (Mo. Ct. App. 2009).

41. *See id.*

42. *Id.*

43. BROWNING, *supra* note 23, at 214–16.

44. *See* Bishop v. Minichiello, 2009 BCSC 358 (Can.).

45. *Id.* at ¶¶ 56–67.

46. *See* Blayde v. Harrah's Entm't, Inc., No. 2:08-cv-02798-BBD-cgc, 2010 WL 5387486, at *1 (W.D. Tenn. Dec. 17, 2010) (mem. op.).

47. *See id.* at *8.

48. *See id.*

49. 18 U.S.C. §§ 2701–2712.

Facebook urges parties to civil litigation to resolve their discovery issues without involving Facebook. Almost without exception, the information sought by parties to civil litigation is in the possession of, and readily accessible to, a party to the litigation. Requests for account information are therefore better obtained through party discovery.

Federal law and Facebook policies prohibit the disclosure of user information. Specifically, the Stored Communication Act, 18 U.S.C. § 2701 et seq., prohibits Facebook from disclosing the contents of a user's Facebook account to any non-governmental entity even pursuant to a valid subpoena or court order. The most Facebook can provide is the basic subscriber information for a particular account.

If a Facebook user deletes content from their account, Facebook will not be able to provide that content. Effectively, Facebook and the applicable Facebook user have access to the same account. To the extent a user claims it does not have access to content (e.g., the user terminated their account), Facebook will restore access to allow that user to collect and produce the information to the extent possible.[50]

Facebook also charges a mandatory, non-refundable processing fee of $500 per user account, an additional $100 for a notarized declaration from the records custodian, and requires a valid California or Federal subpoena to be served on Facebook.[51] Out-of-state civil litigants must have their subpoena domesticated by a California court.[52] MySpace has similar policies, but also requires more information than a party might readily have, such as the "user's unique friend ID number or URL," the user's ZIP code, the password associated with the account, and the birth date provided to MySpace.[53] Another obstacle one might encounter is that an attorney's idea of social networking profile content is likely to be different from—and more extensive than—the basic subscriber information or account information that a site might be willing to release, albeit reluctantly.

The most effective methods of obtaining discovery of the contents of a party's social networking profile are propounding specific, well-tailored discovery requests to the party himself, or by having that party execute a consent form or authorization permitting the holder to obtain such content directly from a social networking site.[54] In terms of discovery requests, refrain from being excessively global (i.e., "all contents of any and all social

50. *Digital Forensics & eDiscovery Advisory—Facebook Subpoenas*, CONTINUUM WORLDWIDE (Oct. 13, 2010), http://continuumww.com/Libraries/PDFs/DF_eD_101310.sflb.ashx.

51. *Id.*

52. *Id.*

53. Sam Glover, *Subpoena MySpace information*, LAWYERIST.COM (July 17, 2009), http://lawyerist.com/subpoena-myspace-information.

54. *See* Joel Patrick Schroeder & Leita Walker, *Social Media in Civil Litigation*, FAEGRE & BENSON LLP (Oct. 14, 2010), http://faegre.com/12201.

media profiles of John Doe").[55] Instead, be specific in what is sought, and tie it to the claims or defenses in the case.[56] For example, instead of just a blanket request for all content, seek "all online profiles, postings, messages (including, but not limited to, tweets, replies, re-tweets, direct messages, status updates, wall comments, groups joined, activity streams, and blog entries), photographs, videos, and online communication" relating to particular claims, allegations of mental anguish or emotional distress, defenses, et cetera.

Mackelprang v. Fidelity National Title Agency of Nevada, Inc.[57] is particularly illuminating on the subject of what social media discovery might be deemed relevant or reasonably calculated to lead to the discovery of admissible evidence. *Mackelprang* involved claims of sexual harassment and a hostile work environment, allegedly culminating in emotional distress so severe that it led to plaintiff's two suicide attempts.[58] The court rejected the defense's efforts to obtain discovery of plaintiff's MySpace content and private messages regarding any of her sexual conduct or relationships.[59] It questioned the relevance of non-work-related sexual relationships, reasoning that "what a person views as acceptable or welcomed sexual activity or solicitation in his or her private life, [sic] may not be acceptable or welcomed from a fellow employee or a supervisor."[60] However, the court did permit discovery of the plaintiff's online accounts, any online statements referring to her lawsuits, any online activity around the time of her two alleged suicide attempts and attributed to the defendant's treatment of her, and any information relevant to her emotional-distress claims.[61] Incidentally, the defense claimed that the plaintiff "was voluntarily pursuing, encouraging or even engaging in extramarital relationships on or through MySpace."[62] The discovery allowed by the court revealed that Mackelprang had two MySpace pages: one created just before the lawsuit was filed, in which the plaintiff identifies herself as a happily married woman and loving mother of several children, and a second page created around the time of the alleged affairs in which she holds herself out as single and not wanting kids.[63]

55. *See* Rachel K. Alexander, *E-Discovery Practice, Theory, & Precedent: Finding the Right Pond, Lure, & Lines Without Going On A Fishing Expedition*, 56 S.D. L. REV. 25, 65 (2011).

56. *See* Schroeder, *supra* note 54.

57. Mackelprang v. Fidelity Nat'l Title Agency of Nev., Inc., No. 2:06-cv-00788-JCM-GWF, 2007 WL 119149, at *1 (D. Nev. Jan. 9, 2007).

58. *See id.* at *1, *8.

59. *See id.* at *6.

60. *Id.*

61. *See id.* at *8.

62. *Mackelprang*, 2007 WL 119149, at *3.

63. *See id.*

With respect to having the party sign a written consent, the SCA allows a holder of electronic communications like Facebook to provide the user's records with "the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service . . . ."[64] A properly drafted consent form should include the account holder or user's name, any user ID, group ID, or known screen name, along with the person's date of birth and address, including email address. The consent should also include—much like a well-drafted discovery request—a detailed description of what is being sought.

Finally, it should also bear the notarized signature of the person giving consent. If the party/account holder refuses to sign the consent, one should file a motion to compel and seek a court order forcing that party to execute the consent. The usual objections to granting a motion to compel are rooted in privacy concerns. And, as will be discussed in more detail, courts tend to cast a jaundiced eye on claims that something is "private" when it has already been communicated to one or more friends on a social networking site—even with privacy restrictions. Case authority indicates that a party may be compelled to produce information from private online profiles.[65] In the event that the information produced gives rise to a belief that information has been withheld, removed, or altered, consider requesting a forensic examination of the party's hard drive or wireless device. In Texas, for example, such access may be granted, particularly if the party's conduct suggests that the party may be withholding, concealing, or destroying discoverable electronic information.[66]

Gathering information from social networking profiles of those who have restricted access to part or all of their page—in effect allowing only designated "friends" to view private material—presents ethical issues as well. May a lawyer, or someone working for that lawyer, try to become someone's "friend" in order to gain access to private content? Of course, if the person is a represented party (such as the plaintiff in a personal-injury suit) the answer is a resounding "no." Rule 4.2 of the Rules of Professional Conduct stipulates that a lawyer may not communicate, or cause another person to communicate, with a person represented by counsel without the prior

64. 18 U.S.C. § 2702(b)(3) (2006).

65. *See, e.g.*, Romano v. Steelcase Inc., 907 N.Y.S.2d 650, 654 (N.Y. Sup. Ct. 2010) (holding that evidence on plaintiff's online profiles was likely material and necessary regardless of privacy settings); Flagg v. City of Detroit, No. 05-74253, 2008 WL 787061, at *1 (E.D. Mich. March 20, 2008) (where the city was compelled to produce the text messages of former Mayor Kwame Kilpatrick and the employee with whom he was having an affair on the grounds that even the records held by an Internet service provider were within the city's constructive control and custody). *See also* O'Grady v. Superior Court of Santa Clara County, 44 Cal. Rptr.3d 72, 88 (Cal. App. Ct. 2006).

66. *In re* Weekley Homes, 295 S.W.3d 309, 313–16 (Tex. 2009); *In re* Honza, 242 S.W.3d 578, 581–82 (Tex. App.—Waco 2008, no pet.).

consent of the party's attorney.[67] But even if the individual in question is not a represented party, an attorney must tread very carefully. Rule 4.1 of the Rules of Professional Conduct mandates that a lawyer, in the course of representing a client, may not knowingly "make a false statement of material fact or law to a third person."[68]

In 2009 and 2010, two bar associations' ethics opinions dealt with this issue head on. In March 2009, the Philadelphia Bar Association's Professional Guidance Committee dealt with an inquiry from an attorney about the propriety of asking a third party to "friend" a witness in order to gain access to her Facebook and MySpace pages.[69] The lawyer already deposed the witness, learned of her social media presence, and concluded that her testimony would be beneficial.[70] While the lawyer did not ask the witness about the information on her profiles or request access to them, the lawyer learned through subsequent visits that she had restricted access to "friends" only.[71] The lawyer wanted to know if he could ethically have a third party "friend" the witness to gain information to use against the witness without revealing the third party's affiliation with the lawyer.[72]

The Philadelphia Bar Association's Professional Guidance Committee found that such conduct runs the risk of violating several ethics rules, including Pennsylvania's equivalent of Rule 4.1.[73] Using a non-lawyer assistant, such as a paralegal, does not relieve an attorney of responsibility for the conduct of such assistants under Rule 8.4 of the Rules of Professional Conduct.[74] The Committee reasoned that failing to disclose the third party's affiliation with the lawyer "omits a highly material fact," an omission that:

> would purposefully conceal that fact from the witness for the purpose of inducing the witness to allow access, when she [might] not do so if she knew the third person was associated with the inquirer and the true purpose of the access was to obtain information for the purpose of impeaching her testimony.[75]

In September 2010, the New York City Bar Association's Committee on Professional Ethics also weighed in on the same issue confronted by its Phil-

67. MODEL RULES OF PROF'L CONDUCT R. 4.2 (2010).

68. MODEL RULES OF PROF'L CONDUCT R. 4.1 (2010).

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

70. *Id.*

71. *Id.*

72. *Id.*

73. *Id.*

74. Phila. Bar Ass'n on Prof'l Guidance, Op. 2009-02 (2009).

75. *Id.*

adelphia counterpart.[76] And, like Philadelphia, the New York City Bar's ethics authorities pointed to Rule 4.1's prohibition against knowingly making a false statement of fact to a third person, as well as to Rule 8.4's ban on conduct involving dishonesty, deception, fraud, or misrepresentation.[77] The New York opinion took note of the increasing use of social media sites by lawyers, and specifically mentioned potential ruses like creating a fake Facebook profile or contacting a YouTube account holder to access a "channel" in order to view his digital postings.[78] The New York City Bar Committee pointed out that pursuing such deceptive avenues was easier in cyberspace than in person, and increased the risk of strangers gaining unfettered access to all kinds of personal information.[79] The committee took pains to point out, however, that there are no ethical restrictions against lawyers accessing publicly viewable pages of another party's social-networking profiles.[80]

In May 2011, San Diego County Bar Association's Legal Ethics Committee tackled a somewhat different scenario—that of *ex parte* communication via social media to a represented party.[81] The facts involved a lawyer representing a plaintiff in a wrongful-discharge action against a former employer.[82] The lawyer wanted to know if it was permissible to send out "friend" requests to two employees at the defendant's company, hoping that these employees would make disparaging comments about the employer on Facebook (a forum in which the lawyer felt they'd be more forthright than in a deposition).[83] The committee rejected the idea that friend requests are not about "the subject of the representation" (and therefore innocuous).[84] The committee similarly swept aside the argument that "friending" a represented party is no different than accessing an opposing party's public website.[85]

76. *See* N.Y. City Bar Ass'n Comm. on Prof'l Ethics, Formal Op. 2010-2 (2010), http://www.nycbar.org/pdf/report/uploads/20071997-FormalOpinion2010-2.pdf.

77. *Id.*

78. *Id.*

79. *Id.*

80. *Id.* Similarly, the New York State Bar Association issued a formal ethics opinion stating that there is nothing unethical about a lawyer accessing the publicly viewable pages of an adverse party's social media profile for "the purpose of obtaining possible impeachment material for use in the litigation." N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Op. 843 (2010).

81. San Diego County Bar Ass'n on Legal Ethics, Op. 2011-2 (2011), http://www.sdcba.org/index.cfm?pg=LEC2011-2.

82. *Id.*

83. *Id.*

84. *Id.*

85. *Id.*

While the Committee, like its counterparts in New York and Philadelphia, embraced the concept that a lawyer may ethically access and view public social media profiles of parties other than the lawyer's client, it concluded that the rules of ethics bar an attorney from making an *ex parte* friend request of a represented party. Reasoning that "represented parties shouldn't have 'friends' like that," the committee sought to strike "the right balance between allowing unfettered access to what is public on the Internet about parties without intruding on the attorney-client relationship of opposing parties and surreptitiously circumventing the privacy even of those who are unrepresented."[86]

III. AUTHENTICATION ISSUES

Once social-networking evidence has been obtained, of course, the next hurdle is getting it admitted. As with all evidence, the offering party must be prepared to demonstrate that the content from a social networking site is (1) relevant, (2) authentic, and (3) not subject to being excluded under the hearsay or best evidence rules.[87] Satisfying the first and third prongs of this test will vary considerably based on the particular facts of each case. With regard to the authenticity requirement, courts have been reluctant to come up with unique rules for authenticating electronic data.[88] In dispensing with an appellant's contention that emails and text messages are "inherently unreliable" and would have to be the subject of a "whole new body of law," one court noted that electronic communications could be properly authenticated within the existing legal framework, since "the same uncertainties exist with traditional written documents. A signature can be forged, a letter can be typed on another's typewriter; distinct letterhead stationery can be copied or stolen."[89]

Upon a determination that the information is relevant and can be heard by the jury, Federal Rule of Evidence 901 requires that the attorney presenting the evidence make a *prima facie* showing of genuineness.[90] It is then up to the finder of fact to decide authenticity.[91] For example, in one commercial litigation and defamation case involving competing providers of satellite-tel-

86. *Id.*

87. *See* Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 538 (D. Md. 2007) (explaining that electronic information must be relevant, authentic, and not excluded under the hearsay rules).

88. *See generally* Steven Goode, *The Admissibility of Electronic Evidence*, 29 REV. LITIG. 1, 7 (2009) (explaining why "the existing rules of evidence are adequate to the task of addressing questions about the admissibility of such electronic evidence").

89. *In re* F.P., 878 A.2d 91, 95 (Pa. Super. Ct. 2005).

90. Fed. R. Evid. 901.

91. Telewizja Polska USA, Inc. v. Echostar Satellite, No. 02 C3293, 2004 WL 2367740, at *6 (N.D. Ill. Oct. 15, 2004).

evision programming, the plaintiff challenged archived pages of its own website claiming that the pages originated from an unreliable source and were not properly authenticated.[92] The court rejected that argument, noting that Rule 901 of the Federal Rules of Evidence requires simply a *prima facie* showing of genuineness.[93] The court concluded that, although the plaintiff was free to raise its reliability concerns with the jury, the fact that an affidavit declared that the pages were copies of the website as it appeared on the dates in question and the fact that the plaintiff failed to deny or challenge the veracity of the archived pages were sufficient to satisfy the authentication threshold.[94]

Authentication of digital information can be accomplished by direct proof, circumstantial evidence, or a combination of both. Federal Rule of Evidence 901(b)(1) allows authentication by "[t]estimony that a matter is what it is claimed to be,"[95] while 901(b)(4) permits authentication by "[a]ppearance, contents, substance, internal patterns, or other distinctive characteristics taken in conjunction with circumstances."[96] In the case of *In re F.P.*, the instant messages at issue were authenticated by direct proof—the person in question acknowledged his screen name, admitted authorship, and admitted to printing the instant messages from his computer.[97] In another case involving printouts of chat room logs, authentication was made by not only the appellant and other witnesses confirming his screen name, but also by the fact that when a meeting was arranged with that screen-name user, the appellant showed up to the arranged meeting.[98] Courts vary on the extent of testimony required by Federal Rule of Evidence 901(b)(1). Some courts require testimony showing that the individual to whom the information was attributed actually posted the information.[99] For example, such testimony could be proffered through an affidavit or a statement from someone with personal knowledge, perhaps the website's webmaster.[100] Another school of thought is considerably more permissive. These courts find it sufficient to have testimony from the person who created the screenshot being offered that the image "accurately reflects the content of the website and the image of the

92. *Id.*

93. *Id.*

94. *Id.*

95. FED. R. EVID. 901(b)(1).

96. FED. R. EVID. 901(b)(4).

97. *In re* F.P., 878 A.2d 91, 94 (Pa. Super. Ct. 2005).

98. United States v. Tank, 200 F.3d 627, 630–31 (9th Cir. 2000).

99. *In re* Homestore, Inc. Sec. Litig., 347 F. Supp. 2d 769, 782-83 (C.D. Cal. 2004).

100. *Id.*

page on the computer at which the [screenshot] was made."[101] Yet, somewhere in between the two ideas is another camp that requires different evidence depending on the circumstances. An excellent primer on the admissibility of all types of online information can be found in the case of *Lorraine v. Markel American Insurance Company*.[102] Although this case revolved around the enforcement of an arbitration award and did not deal specifically with social networking sites, it contains a very useful discussion of the admissibility of electronically stored information (ESI).[103] The court notes that ESI "comes in multiple evidentiary 'flavors' including e-mail, website ESI, Internet postings, digital photographs, and computer-generated documents and data files."[104] The opinion analyzes particular types of digital evidence and also examines authentication issues and hearsay concerns.

Printouts from a webpage commonly draw hearsay objections. Typically, however, courts apply the rationale that such printouts are not "statements" at all, but are rather merely images and text found on the websites.[105] In *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, the court observed that the pictures and webpages printed from the Internet had sufficient circumstantial indicia of authenticity, such as time and date stamps and web addresses, to support a reasonable juror in the belief that the documents were as they purported to be.[106]

To authenticate social-networking content, the party offering it must introduce sufficient evidence for a reasonable jury to conclude that the exhibit is what the sponsoring party claims it to be. At a minimum, one should proffer testimony from the person who performed the online research and printed the social media pages. Testimony should describe when and how the page was found, describe the circumstances of the search, and verify that the copy accurately reflects what was viewed online. The webpage itself and any page on the site reflecting its ownership should be printed out with the URL listed. Further, one should be prepared to offer evidence that the author of the posting or other social media content actually wrote it. This evidence can consist of an admission by the author, a stipulation entered into by the parties, the testimony of a witness who assisted in or observed the creation of the content or other indications or content from the profile itself that connects it to the author. One could also use evidence of similarities between the profile at issue and other already authenticated material as circumstantial evidence of authorship. One of the advantages of social media profiles is the

101. Toytrackerz LLC v. Koehler, No. 08-2297-GLR, 2009 WL 2591329, at *6 (D. Kan. Aug. 21, 2009).

102. Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 538 (D. Md. 2007).

103. *Id.*

104. *Id.*

105. *See, e.g.*, Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1155 (C.D. Cal. 2002).

106. *Id.* at 1154.

level of individualization frequently associated with them—photos of the author, background information, information about his or her hobbies and interests, and commentary by the user.[107] As will be discussed further, such individualization provides courts with a reasonable assurance under the Federal Rules of Evidence 901(b)(4) that the distinctive characteristics are sufficient for a jury to find that the purported author is indeed the one responsible for the social networking page's content.[108]

Courts considering the admissibility of evidence from sites like Facebook and MySpace, as well as other forms of digital evidence, have repeatedly noted that the evidence required to meet the authentication threshold is "quite low."[109] In *State v. Bell*, the appellate court affirmed the trial court's denial of a defense motion to exclude printouts of MySpace instant messages alleged to have been sent to a victim by the defendant under his MySpace screen name.[110] The court was not persuaded by defense arguments that MySpace chats can be readily edited from a user's homepage after the fact.[111] It found that the offering party may sufficiently authenticate the MySpace content in question through testimony that: "1) he ha[d] knowledge of the defendant's e-mail address and MySpace user name, 2) the printouts appear[ed] to be accurate records of his electronic conversations with [the] defendant, and 3) the communications contain[ed] code words known only to [the] defendant and his alleged victims."[112] Similarly, a Tennessee appellate court held that admitting the MySpace printouts at issue did not require authentication by a MySpace representative.[113] Here, it was sufficient that the witness testified that her husband had sent messages to her on MySpace, that she made printouts directly from her computer, and that the messages accurately reflected the communication she had with her husband.[114] Most courts are satisfied with authentication through circumstantial evidence of the content, location, and authorship of the social media content in question.[115] A few courts take the position that circumstantial evidence is an insufficient

107. *See, e.g.*, Tienda v. State, No. 05-09-00553-CR, 2010 WL 5129722, at *5 (Tex. App.—Dallas Dec. 17, 2010, pet. granted).

108. *Id.*

109. State v. Bell, 2008-Ohio-592, 882 N.E.2d 502, 512 (C.P. Clermont County Ct. 2008).

110. *Id.*

111. *Id.* at 511–12.

112. *Id.* at 512.

113. Dockery v. Dockery, No. E2009-01059-COA-R3-CV, 2009 WL 3486662, at *6 (Tenn. Ct. App. Oct. 29, 2009).

114. *Id.*

115. *See, e.g.*, People v. Fielding, No. C062022, 2010 WL 2473344, at *4–5 (Cal. Ct. App. June 18, 2010).

degree of authentication.[116] Still, others are satisfied with a minimal level of authentication. For instance, a Texas appellate court upheld a minor's conviction for vandalism based on what the victim reportedly read on the defendant's MySpace page, even though the victim had no personal knowledge that the defendant herself had typed that admission.[117]

In addition, courts will examine the purpose for which the social media evidence is being offered. For example, in *People v. Goins*, the appellate court ruled that a MySpace entry had been sufficiently authenticated, but upheld its exclusion at trial for the party's failure to elicit testimony inconsistent with the prior statement made on MySpace.[118] In one North Carolina case, the appellate court upheld the trial court's admission into evidence of an alleged child-abuse victim's MySpace page and reasoned that the minor's posting of suggestive photographs and use of provocative language was grounds for proper impeachment of prior inconsistent statements she made to police about her sexual history.[119] Similarly, in an Ohio statutory-rape case, the court of appeals upheld the defendant's admission of evidence that the victim had portrayed herself to be eighteen years old on her MySpace page, the admission of photos that the girl had posted, and the admission of witness testimony about the authenticity of those photos.[120]

In *People v. Liceaga*, a 2009 Michigan murder case, the trial court allowed the prosecution to admit the defendant's MySpace page photos—some depicting him holding a gun allegedly used in the crime—as well as others in which he was displaying a gang sign, as evidence of intent and planning.[121] The appellate court upheld the admission because it was allowed only for the limited purpose of establishing intent and planning and because its probative value exceeded any danger of unfair prejudice.[122] In *Hall v. State*, a Texas murder case, the court allowed the admission of incriminating statements from Hall's Facebook page as evidence of her guilt.[123] As proper evidence of motive, the court of appeals upheld the admission of Facebook postings stating, "I should really be more of a horrific person. Its [sic] in the works," as

116. *See, e.g.*, Commonwealth v. Williams, 926 N.E.2d 1162, 1172-73 (2010).

117. *In re* J.W., No. 10-09-00127-CV, 2009 WL 5155784, at *1–4 (Tex. Crim. App. Dec. 30, 2009, no pet.).

118. People v. Goins, No. 289039, 2010 WL 199602, at *2 (Mich. Ct. App. Jan. 21, 2010).

119. *In re* K.W., 666 S.E.2d 490, 494 (N.C. Ct. App. 2008).

120. State v. Gaskins, No. 06CA0086-M, 2007-Ohio-4103, 2007 WL 2296454, at *7–8 (Ohio Ct. App. Aug. 13, 2007).

121. People v. Liceaga, No. 280726, 2009 WL 186229, at *3–4 (Mich. Ct. App. Jan. 27, 2009).

122. *Id.* at *4.

123. Hall v. State, 283 S.W.3d 137, 149 (Tex. Crim. App. 2009, pet. ref'd.).

well as the admission of Hall's screen name, favorite quotes, and an online list of her favorite films, which were notable for their violent nature.[124]

The Eleventh Circuit took a contrary position.[125] Souksakhone Phaknikone, who called himself "Trigga Fully Loaded" on his MySpace page, was convicted in Georgia federal court of fifteen armed robberies and sentenced to 167 years in prison.[126] The trial court, over defense objections, admitted Phaknikone's MySpace profile, along with various photos from his MySpace page showing him brandishing a gun and bearing gang tattoos; however, the court allowed the evidence with a limiting instruction that the profile and photos could only be considered to prove intent or absence of mistake, and not to prove that the defendant behaved like a gangster.[127] The Eleventh Circuit disagreed, holding that such photos were inadmissible character evidence offered for no purpose other than to show action in conformity therewith under Federal Rules of Evidence 404(b).[128] But while it disapproved of the admission of this evidence, it ruled the error harmless and allowed the conviction to stand.[129]

Time and time again, courts have pointed to the degree of individualization that social networking profiles offer as a basis for satisfying the authentication threshold and, consequently, admissibility. For example, in the murder case of *Griffin v. Maryland*, the Maryland Court of Special Appeals considered the appellant's contention that the trial court had erred in admitting a MySpace printout that was not properly authenticated.[130] The printout was a redacted page from a MySpace profile belonging to the appellant's girlfriend, who had allegedly threatened an eyewitness via MySpace by writing, "JUST REMEMBER, SNITCHES GET STITCHES!! U KNOW WHO YOU [ARE]!!"[131] The printout in question came from a profile bearing the girlfriend's user name of "Sista Souljah," listing her birth date, featuring a photo of her and the appellant embracing, and including a blurb of the appellant's nickname "FREE BOOZY."[132] The court held that such individualization was more than enough to authenticate that the MySpace profile was hers.[133]

124. *Id.*

125. U.S. v. Phaknikone, 605 F.3d 1099 (11th Cir. 2010).

126. *Id.* at 1101, 1103–04.

127. *Id.* at 1104–06.

128. *Id.* at 1107.

129. *Id.*

130. Griffin v. State, 995 A.2d 791, 806 (Md. Ct. Spec. App. 2010).

131. *Id.* at 795.

132. *Id.* at 796.

133. *Id.* at 807.

Perhaps a recent Texas case provides the best articulation of how the highly individualized character of social media profiles satisfies the authentication requirements rules for admission of evidence. In *Tienda v. State*, a jury convicted the defendant of murder after an altercation with the victim, David Valadez.[134] The defendant's appeal centered on the supposedly improper admission of his MySpace page into evidence over defense objections that the social networking content was not properly authenticated.[135] The victim's sister found and testified to the defendant's MySpace profile, which had a photograph of the defendant with the caption, "Rest in peace, David Valadez."[136] His profile page also had an embedded link to an audio recording of a song played at the victim's memorial service, controversial and notorious statements such as, "Hector snitching on me," and, "it's cool if I get off," as well as defendant's photos displaying his electronic monitoring bracelet, and another that captioned, "str8 outta jail and n da club."[137] The Dallas Court of Appeals found all of these, and more, as indications of sufficient authenticity. It observed:

"The inherent nature of social networking websites encourages members who choose to use pseudonyms to identify themselves by posting profile pictures or descriptions of their physical appearances, personal backgrounds, and lifestyles. This type of individualization is significant in authenticating a particular profile page as having been created by the person depicted in it. The more particular and individualized the information, the greater the support for a reasonable juror's finding that the person depicted supplied the information."[138]

In short, the key to authenticating evidence from a party or witness's social networking profile is to demonstrate the connections between that individual and the evidence being offered. For example, a distinctive nickname that doubles as an online pseudonym, photos depicting the user or witness, comments unique to the individual, and references in the profile to groups or causes with which the person is affiliated are all valid and effective ways of showing these. More connections increase the likelihood that evidence offered will be authenticated. Moreover, all of these connections can be established through effective cross-examination. Remember, social networking is all about establishing connections—and so is authentication.

134. Tienda v. State, No. 05-09-00553- CR, 2010 WL 5129722, at *1(Tex. App.—Dallas Dec. 17, 2010, pet. granted).

135. *Id.* at *4.

136. *Id.* at *3.

137. *Id.*

138. *Id.* at *5.

IV. Discoverability Issues – The Privacy Argument

Perhaps the most hotly contested issue regarding the discoverability of social media evidence has been the notion that content posted to a social networking site is somehow cloaked in an expectation of privacy. Several scholars have pointed out an inherent contradiction in the notion. They argue that, although the Internet fosters a sense of anonymity for many, it provides much greater freedom to spread information, which actually results in a heightened likelihood of revealing what was once secret and private—to a sometimes disastrous effect.[139]

Although the very heart of social networking is the concept of sharing information and connecting with others, time and again privacy is cited as the basis for objecting to discovery into the content of someone's Facebook or MySpace profile. Moreover, time and again, courts have brushed these privacy objections aside. The Sixth Circuit, for example, held that users of social networking sites "logically lack a legitimate expectation of privacy in the materials intended for publication or public posting."[140] The Maryland Supreme Court observed that "the act of posting information on a social networking site, without the poster limiting access to that information, makes whatever is posted available to the world at large."[141] In 2009, a Minnesota appellate court held that information posted on social networking sites was deemed to be public information.[142] In another case, a mother embroiled in a custody proceeding objected to the use of her posts on MySpace, stating she was on a "hiatus from using illicit drugs."[143] The Ohio appellate court found the posts admissible due to their public nature, and consequently, the mother "[could] hardly claim an expectation of privacy regarding these writings."[144]

Moreno v. Hanford Sentinel, Inc. is another example where the court rejected the contention that postings on social media sites are private in nature. In this case, a MySpace user posted a diatribe about her hometown.[145] The online rant was found by another member of the community who wrote an angry defense in the form of an op-ed piece in the local paper, quoting liberally from the plaintiff's MySpace ramblings and identifying the plaintiff and her family.[146] The plaintiff subsequently sued the newspaper, claiming

139. *See, e.g.*, Solove, *supra* note 27.

140. Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001).

141. Indep. Newspapers, Inc. v. Brodie, 966 A.2d 432, 438 (Md. 2009).

142. Yath v. Fairview Clinics, N.P., 767 N.W.2d 34, 43–44 (Minn. Ct. App. 2009).

143. Dexter v. Dexter, 2006-P-0051, 2007 WL 1532084, at *6 (Ohio Ct. App. May 25, 2007).

144. *Id.*

145. Moreno v. Hanford Sentinel, Inc., 91 Cal. Rptr. 3d 858, 861 (Cal. Ct. App. 2009).

146. *Id.* at 861.

this alleged invasion of privacy had ruined the family's lives.[147] The appellate court upheld the dismissal of the case holding that the facts contained in the article, once previously posted on MySpace, were not at all private.[148]

One litigant has even tried to claim a "social-networking privilege." In *McMillen v. Hummingbird Speedway, Inc.*, the plaintiff was rear-ended while taking a "cool down lap" after a stock car race at the defendant's track, and he filed a personal-injuries suit.[149] A few days later, the plaintiff posted material on his social networking profile about engaging in activities such as fishing and attending the Daytona 500 race.[150] Understandably, the defense counsel wanted to introduce these comments as evidence for disproving plaintiff's disability and damages claims. Instead of requesting the plaintiff to turn over the relevant content of his social media accounts, defense counsel sought the login names and passwords for each of his accounts.[151] The plaintiff claimed a "social networking privilege," which was resoundingly rejected by the court.[152] In his ruling directing the plaintiff to produce not just the content of his profiles, but also the passwords and login information, the judge dispensed with the notion that social networking communications enjoyed any degree of confidentiality.[153] He wrote:

"[C]onfidentiality is not essential to maintain the relationships between and among social network users, either. The relationships to be fostered through those media are basic friendships, not attorney-client, physician-patient, or psychologist-patient types of relationships, and while one may expect that his or her friend will hold certain information in confidence, the maintenance of one's friendships typically does not depend on confidentiality."[154]

Courts are somewhat more receptive to privacy arguments when the rights of non-parties or minors are involved. For example, in one premises-liability case, the plaintiff was a patron of the well-known Coyote Ugly bar chain.[155] In the typical Coyote Ugly fashion, the plaintiff was encouraged to get up on the bar and dance, along with several of her friends. Unfortunately, she slipped and fell, striking the back of her head.[156] The defendant subpoe-

147. *Id.*

148. *Id.* at 862.

149. McMillen v. Hummingbird Speedway, Inc., No. 113 - 2010 CD, 2010 WL 4403285, at *1 (Pa. Ct. Com. Pl. Sept. 9, 2010).

150. *Id.* at *2.

151. *Id.*

152. *Id.* at *9.

153. *Id.* at *10.

154. *McMillen*, 2010 WL 4403285, at *10.

155. Barnes v. CUS Nashville, LLC, No. 3:09-cv-00764, 2010 WL 2265668, at *1 (M.D. Tenn. June 3, 2010).

156. *Id.* at *1.

naed Facebook for plaintiff's privacy-restricted content, including photos of the plaintiff and her friends dancing on the bar.[157] The court quashed the subpoena, and the defendant issued subpoenas to the plaintiff's friends.[158] To resolve the discovery dilemma, the judge crafted a rather novel solution. To protect the privacy interests of the third parties, he offered to create his own Facebook account and "friend" the witnesses "for the sole purpose of reviewing photographs and related comments *in camera* . . . and disseminat[ing] any relevant information to the parties."[159] After acting as a privacy filter for discovery purposes, the court would then close its Facebook account.[160]

In another case dealing with a sexual-assault charge, the status of a teenager victim as a minor enhanced the concerns over privacy. The plaintiff sued the school, alleging that its negligence and failure to supervise contributed to the attack, resulting in the young victim's severe emotional distress.[161] The defense attorneys sought the contents of the plaintiff's privacy-restricted MySpace and Facebook profiles (both via subpoena to the sites themselves and through discovery directed to the plaintiff). The defense argued the requested information was highly relevant to the issue of emotional distress as it would "shed light on the plaintiff's credibility by finding out what she wrote on social networking sites in unguarded moments."[162] The defense also argued that the plaintiff had waived her privacy rights to sources that could lead to admissible evidence of a very material issue—her mental state. Accordingly, the defense concluded that its request was analogous to seeking emails and similarly discoverable communications.[163] In contrast, the plaintiff's attorney argued in favor of a broad prohibition against the discoverability of social networking evidence in such cases, particularly where minors were concerned.[164] He maintained that the pervasive nature of communicating through computer or wireless device has somehow rendered minors, such as the plaintiff, to believe that the Internet allows them to confidentially communicate with their friends.[165] While the court did not go so far as to adopt this "teen social networking confidentiality" argument, it did decline to order the discovery. The court issued a protective order against the release of the social media evidence, saying that "it seemed like a

157. *Id.*

158. *Id.*

159. *Id.* at *1.

160. *Barnes*, 2010 WL 2265668, at *1.

161. *See* T.V. v. Union Twp. Bd. of Educ. No. UNN-L-4479-04, 2007. LEXIS 3005 (N.J. Super. Ct. Law. Div. June 8, 2007).

162. *Id.*

163. *Id.*

164. *Id.*

165. *Id.*

big step" to order the release of plaintiff's private communications.[166] However, in fairness, a key point for the court was the fact that the defense had not yet pursued more traditional avenues of discovery (such as finding out who the plaintiff's potential witnesses were and then interviewing or deposing them), or shown that the information could not be obtained through other means.[167]

Other courts, however, have been considerably less deferential to a teenager's privacy when social media is involved. In one such case, Tatum Bass, a South Carolina teenager, sued Miss Porter's School of Farmington, Connecticut, claiming the exclusive private academy failed to adequately protect her from bullying at the hands of a clique of girls at the school, and subsequently expelled her for absences caused by the resulting emotional distress.[168] Although the minor plaintiff acknowledged that part of her claims rested on Facebook postings and email correspondence during her time at the school, she hesitated, on privacy grounds, to provide the defense with the requested social media evidence.[169] Even though Facebook provided Miss Bass with approximately 750 pages of documents, she in turn only produced approximately 100 pages of that to the defense.[170] Rejecting the plaintiff's privacy arguments, the court ordered her to produce all of the documents.[171] The court made a point:

"Facebook usage depicts a snapshot of the user's relationships and state of mind at the time of the content's posting. Therefore, relevance of the content of plaintiff's Facebook usage as to both liability and damages in this case is more in the eye of the beholder than subject to strict legal demarcations, and production should not be limited to plaintiff's own determination of what may be 'reasonably' calculated to lead to the discovery of admissible evidence."[172]

The next cases move from situations similar to *Mean Girls* to another all-too-common reality of the lives of some teenage girls: eating disorders. Yet another court was required to balance the privacy interests of litigants against the opponent's need for discovery. In a class-action suit brought against a health insurance carrier over its declining coverage for eating disorders, such as bulimia or anorexia, the central issue was a New Jersey law

166. *T.V.*, 2007 LEXIS 3005, at *1.

167. *Id.*

168. Bass *ex rel.* Bass v. Miss Porter's Sch., 738 F. Supp. 2d 307, 323 (D. Conn. 2010).

169. Bass *ex rel.* Bass v. Miss Porter's Sch., No. 3:08-cv-1807 (JBA), 2009 WL 3724968, at *1 (D. Conn. Oct. 27, 2009).

170. *Id.*

171. *Id.* at *2.

172. *Id.* at *1.

mandating coverage for "biologically-based" mental illnesses.[173] Parents of children suffering from these eating disorders sued Horizon Blue Cross/Blue Shield (Horizon) for declining coverage, and Horizon took the position that the disorders in question were psychological in origin, and therefore, not covered.[174] Horizon sought support for its defense in the online postings made by the children on sites such as MySpace and Facebook, arguing that production of such writings on social networking sites would shed light on the emotional roots of the eating disorders.[175] The plaintiffs vehemently opposed having to produce such online journals and communications, arguing that doing so not only violated the children's privacy, but also would negatively impact their recovery.[176] U.S. Magistrate Judge Patty Shwartz ordered the production of the social networking content and later denied Plaintiffs' motion to reconsider.[177] Judge Shwartz pointed out that the plaintiffs themselves elected to file a lawsuit that would require them to disclose information concerning their children's eating disorders.[178] As she stated, "[t]he privacy concerns are far less where the beneficiary herself chose to disclose the information. In addition, journals or writings that have been shared with other health professionals who have treated the beneficiaries shall be provided to the defendant's experts as they are a part of their medical records."[179]

Plaintiffs raising privacy concerns have fared better when they have been able to bring the circumstances of the case within the context of the federal Stored Communications Act (SCA) and the protections that it provides.[180] In *Crispin v. Christian Audigier, Inc.*, the defendant garment manufacturer was sued for copyright infringement of Crispin's protected work.[181] Audigier issued subpoenas to a number of third parties seeking communications referencing its company between Crispin and certain other entities, including a tattoo artist and sites such as Facebook, MySpace, and Media Temple (a web-hosting and visualization-services provider).[182] Crispin moved to quash the subpoenas on several grounds. Crispin's most important assertion was that the subpoenas violated the provisions of the SCA, which

173. Beye v. Horizon BlueBlue Cross/Blue Shield of New Jersey, 568 F. Supp. 2d 556, 559 (D. N.J. 2008).

174. *Id.* at 560.

175. Beye v. Horizon Blue Cross/Blue Shield of New Jersey, No. 06-5337 (FSH), 2007 WL 7393489, at *1 (D. N.J. Dec. 14, 2007).

176. *Id.* at *1 n.1.

177. *Id.* at *2.

178. *Id.* at *2 n.3.

179. *Id.*

180. 18 U.S.C. § 2701 (2006).

181. Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 968 (C.D. Cal. 2010).

182. *Id.* at 968–69.

prohibited disclosure of the kind of electronic communications sought by the defendant.[183] The magistrate judge denied the motion, ruling the SCA did not apply since the materials in question were not held in electronic storage within the meaning of the statute.[184]

The district court largely reversed the lower court's ruling, finding that because there were actual messages and wall posts involved on Facebook and MySpace, the SCA would apply because the social networking sites could properly be considered providers of electronic communications services.[185] In a detailed, wide-ranging opinion, the court wrestled with the determination of whether social media sites, such as Facebook and MySpace—with Facebook's wall and MySpace's comments—were electronic communication service ("ECS") providers or remote computing service ("RCS") providers.[186] Under the SCA, the two categories have differing standards.[187] An ECS provider cannot "knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service,"[188] while an RCS provider cannot "knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service."[189] One difficulty noted by the court, and likely to resurface in future discussions of the applicability of the SCA to social media sites, is the fact that the statute was enacted in 1986, long before the advent of the Internet and social networking.[190] The court in *Crispin* found that a Facebook wall posting or a MySpace comment would not be protectable as a form of temporary, intermediate electronic storage, even though postings, once made, were stored for backup.[191] The court concluded that Facebook and MySpace, at least insofar as wall postings and comments were concerned, were ECS providers.[192] In short, the court quashed those portions of the subpoenas that sought "private messaging" and remanded for an evidentiary hearing on the allegedly private nature of the wall postings and comments.[193]

183. *Id.* at 969.

184. *Id.* at 980.

185. *Crispin*, 717 F. Supp. 2d at 981–82.

186. *Id.* at 980.

187. *Id.* at 972.

188. 18 U.S.C. § 2702(a)(1) (2006).

189. 18 U.S.C. § 2702(a)(2) (2006).

190. Crispin, 717 F. Supp. 2d at 971.

191. *Id.* at 988-89.

192. *Id.* at 989.

193. *Id.* at 991.

The *Crispin* case was cited in a recently decided federal case in Florida.[194] In that case, a plaintiff sued his former employer seeking back overtime pay.[195] The employer subpoenaed Facebook and MySpace accounts held by the plaintiff, presumably to buttress a defense that the employee was not entitled to overtime because of hours whiled away on the social media sites during working hours.[196] The plaintiff moved to quash the subpoenas on privacy grounds.[197] While the court denied the motion, it did so on a technicality: the motion to quash should have been filed in the federal district court in California where the subpoenas had been issued.[198] The judge went on to disagree with the defendant's position that Mr. Mancuso, an individual, lacked standing to challenge subpoenas issued to third parties like Facebook.[199] Looking to *Crispin*'s holding, the court came rather close to articulating a privacy right for an individual, as far as his or her social media information is concerned.[200] The judge cited *Crispin*'s ruling, saying that "an individual has a personal right of information in his or her profile and inbox on a social networking site and his or her webmail inbox in the same way that an individual has a personal right in employment and banking records. As with bank and employment records, this personal right is sufficient to confer standing to move to quash a subpoena seeking such information."[201]

However intriguing and unsettled the potential application of the SCA to social media may be, the undeniable fact remains that the vast majority of case authority around the country—and the clear trend in jurisprudence—is to reject claims that privacy concerns somehow trump a party's right to discovery of social networking evidence.[202] For example, in *Ledbetter, et al. v. Wal-Mart Stores, Inc.*, the repairmen plaintiffs alleged personal injuries resulting from an electrical accident at a Wal-Mart store.[203] These injuries included skin burns, hearing impairment, fatigue, chronic neck and wrist pain, sleep disturbance and anxiety, as well as "cognitive inefficiencies and depression."[204] The wife of one plaintiff also asserted a loss of consortium

194. Mancuso v. Florida Metropolitan University, Inc., 2011 WL 310726, at *1 (S.D. Fla. Jan. 28, 2011).

195. *Id.* at *1.

196. *Id.* at *1.

197. *Id.* at *1.

198. *Id.* at *2.

199. *Mancuso*, 2011 WL 310726, at *2.

200. *Id.* at *2.

201. Crispin, 717 F. Supp. 2d at 974.

202. *See* Ledbetter v. Wal-Mart Stores, Inc., No. 06-cv-01958-WYD-MJW, 2009 WL 1067018, at *2 (D. Colo. Apr. 21, 2009).

203. *Id.* at *1.

204. *Id.*

claim against the store.[205] Plaintiff's counsel objected to the defense's subpoenas seeking the claimants' records from Facebook, MySpace, and Meetup.com on privacy grounds.[206] Counsel also claimed that both physician-patient and spousal privileges applied to prevent the defense from obtaining the information sought.[207] The lawyers asked the court to conduct an *in camera* inspection of the information requested.[208] In doing so, the court found the plaintiffs waived their physician-patient privilege by virtue of bringing a personal injury lawsuit and that asserting a loss of consortium claim "injected the issue" of the marital relationship into the case.[209] The court rejected the applicability of either privilege and ruled the social networking evidence was reasonably calculated to lead to the discovery of admissible evidence.[210] Therefore, the court required the plaintiffs to disclose the information sought by the defense.[211] The court further ruled that an already-in-place protective order was sufficient to protect any privacy interests.[212]

In another case, the court rejected these privacy concerns once again, this time in the context of an employment-discrimination suit.[213] The Equal Employment Opportunity Commission ("EEOC") brought an action on behalf of two female employees at a self-storage firm. The employees, a property manager and an assistant manager, alleged that they and other female employees had been subjected to groping, sexual assault, sexual commentary, and other harassment by a male manager, resulting in extreme emotional distress.[214] Counsel for the self-storage company defendant sought discovery from the plaintiffs' MySpace and Facebook accounts. This included profiles, status updates, photos, and wall posts that "reveal, refer, or relate to any emotion, feeling, or mental state, as well as communications that reveal, refer, or relate to events that could reasonably be expected to produce a significant emotion, feeling, or mental state."[215]

The EEOC objected, claiming that the requests were harassing, would embarrass the plaintiffs, and would improperly infringe on their privacy.[216]

205. *Id.*

206. *Id.*

207. *Ledbetter*, 2009 WL 1067018, at *1.

208. *Id.*

209. *Id.*

210. *Id.*

211. *Id.* at *2.

212. *Ledbetter*, 2009 WL 1067018, at *2.

213. EEOC v. Simply Storage Mgmt., LLC, 270 F.R.D. 430 (S.D. Ind. 2010).

214. *Id.*

215. *Id.* at 436.

216. *Id.* at 432.

U.S. Magistrate Judge Lynch, however, overruled the EEOC by ordering the production the defendant sought. In doing so, he reminded the claimants that "locking" or setting their social networking profiles as private did not shield the profiles from discovery.[217] Additionally, while the social networking content sought would have to be relevant to a claim or defense in the case, the plaintiffs' allegations of depression and stress disorders were likely to be discussed at length in the social networking communications being sought, including when the stress purportedly occurred, to what degree, and what factors may have contributed to or caused the stress.[218] As for the plaintiffs' concerns, Judge Lynch disposed of their argument by pointing out that "the production here would be of information that the claimants have already shared with at least one other person through private messages or a large number of people through postings."[219]

Like Magistrate Judge Lynch, New York Supreme Court Justice Jeffrey Arlen Spinner does not believe the fact that a plaintiff has restricted access to or even deleted content from her social networking profile should diminish a defendant's right to conduct discovery efforts that include viewing the content of the plaintiff's Facebook and MySpace pages. In *Romano v. Steelcase, Inc.*, Kathleen Romano fell off an allegedly defective desk chair in 2003, while working at Stony Brook University.[220] She claimed to have sustained serious "permanent injuries," including herniated discs, which necessitated multiple surgeries and diminished her enjoyment of life.[221] Among other things, Romano claimed to be primarily housebound and bedridden as a result of the fall.[222] Noting that publicly-viewable portions of Romano's Facebook and MySpace profiles seemed at odds with her claims (she was purportedly smiling happily outdoors and making references to physical activities inconsistent with her tale of woe), counsel for Steelcase, the chair's manufacturer, served Romano with discovery, requesting an authorization for full access to her current and historical MySpace and Facebook information.[223] Romano objected on privacy grounds, arguing release of the information would violate her Fourth Amendment rights.[224]

Justice Spinner overruled her objections, saying "Plaintiffs who place their physical condition in controversy, may not shield from disclosure material, which is necessary to the defense of the action."[225] He ordered Romano

217. *Id.* at 434.

218. *EEOC*, 270 F.R.D. at 435.

219. *Id.* at 437.

220. Romano v. Steelcase, Inc., 907 N.Y.S.2d 650 (N.Y. Sup. Ct. Suffolk Co. 2010).

221. *Id.* at 653.

222. *Id.* at 654.

223. *Id.*

224. *Id.* at 655.

225. Romano, 907 N.Y.S.2d at 652.

to provide the requested authorization so the defendant could access Romano's social networking profiles, including any records that had previously been deleted or archived.[226] The court also swept aside Romano's argument about having a reasonable expectation of privacy, reminding her that she had voluntarily posted the very information she was now seeking to protect; since the plaintiff "knew that her information may become publicly available, she cannot now claim that she had a reasonable expectation of privacy," the court opined.[227] In addition, Justice Spinner noted that both MySpace and Facebook maintained privacy and terms of use policies that cautioned users that they post content at their own risk and at the risk of making such comments or information publicly available.[228] The court wrote, "Thus, when Plaintiff created her Facebook and MySpace accounts, she consented to the fact that her personal information would be shared with others, notwithstanding her privacy settings. Indeed, that is the very nature and purpose of these social networking sites or they would cease to exist."[229]

The common sense approach articulated in both the *EEOC v. Simply Storage Management* case and the *Romano v. Steelcase* opinion is indeed compelling. To paraphrase Magistrate Judge Lynch, one does not venture onto a social networking site to engage in a soliloquy. Moreover, as Justice Spinner points out, the sharing of information with others is the very reason why social networks exist in the first place. While the potential SCA implications of messages sent via social networking sites will no doubt continue to be explored, the trend in judicial consideration of privacy arguments over the discoverability of social media evidence is clear: if a litigant feels that information was good enough to share with his or her Facebook "friends" and later asserts claims to which that information may be relevant, then the information is good enough to produce to the other side in discovery.

Courts have similarly adopted a common sense approach when considering just what constitutes relevant social media content to which the seeking party may be entitled. Two recent cases from Pennsylvania illustrate this. In *Piccolo v. Paterson*, Bucks County Common Pleas Court Judge Albert Cepparulo denied the defendants' motion to compel the plaintiff to accept a

226. *Id.* at 657.

227. *Id.*

228. *Id.* at 656–57.

229. *Id.* at 657. Interestingly, two months after Justice Spinner's opinion, another New York court took a different approach and affirmed denial of the defense's motion seeking discovery of a personal injury litigant's social media profiles. However, the court did so due to the overly broad nature of the discovery requests and the lack of a factual predicate insofar as relevancy was concerned, and it specifically left the door open for the defense to submit more specific and narrowly-tailored discovery efforts for the court to entertain. *See* McCann v. Harleysville Ins. Co. of N.Y., 910 N.Y.S.2d 614, 615 (4th Dept. 2010).

friend request from defense counsel.[230] The case involved personal injuries claimed stemming from a May 2007 car accident. The plaintiff had ninety-five stitches to her face, subsequent surgery to repair scarring, and was permanently scarred. The defense attorney wanted access to Piccolo's Facebook page in order to view postings and photos, arguing that someone with a scar on her face might portray herself differently online than she might when seeking damages from a jury. The court rejected the defense's efforts, in part because of the lack of any demonstrated need for access to Piccolo's Facebook page.[231] As the plaintiff's attorney pointed out, Ms. Piccolo's status updates and pictures were not only already public, but she had previously provided the defense with dozens of photos of her face, allowed the insurance carrier to photograph her prior to suit, and even permitted the defense lawyer to take more pictures at a September 2010 deposition.

In another car-accident case, the plaintiff sued alleging physical and psychological injuries, including the inability to drive or ride a motorcycle for extended periods of time.[232] The defense sought access to Plaintiff's Facebook and MySpace accounts. When the plaintiff resisted, the court opted to conduct an *in camera* review of his social media profile.[233] The court concluded that while the bulk of the material was unrelated to the accident, and therefore not discoverable, a number of items should be and ultimately were produced, including photos of the plaintiff taking numerous motorcycle trips, photos of the plaintiff hunting, and various comments made by the plaintiff confirming his continued interest in riding motorcycles.[234]

V. CONCLUSION

The wall postings, YouTube videos, tweets, photos, and Facebook status updates that populate the landscape of emerging media are more than just what Jimmy Buffett might describe as digital "permanent reminders of a temporary feeling." Social networking sites like Facebook, MySpace, Twitter, and LinkedIn represent a paradigm shift in the way people communicate and share information. Such sharing, however, comes with a price. With increasing regularity, lawyers are ready and willing to plunder the digital treasure troves of information that these sites represent. Moreover, judges are more and more amenable to allowing access to the plethora of photos, comments, status updates, and other postings that many users of social media might regard, at least in their own minds, as off limits. The shifting balance between privacy rights and evidence gathering, in the context of a search for

230. Piccolo v. Patterson, No. 2009-04979 (C.P. Bucks County Pa. Ct. May 18, 2011).

231. *Id.*

232. Offenback v. Bowman, No. 10-CV-1789, 2011 WL 2491371, at *1 (M.D. Pa. June 23, 2011).

233. *Id.*

234. *Id.* at *2.

the truth, reflects the broader debate being waged not only across the legal landscape, but the cultural one as well. At 5,830 words long, Facebook's privacy policy may dwarf the U.S. Constitution, a paltry 4,543 words by comparison. But in a society in which individuals live more and more of their lives online, just how much privacy can one expect? The person posting commentary and photos on Facebook today may very well become tomorrow's litigant, hoisted by his own digital petard.