Use of Social Networking Sites in Mass Tort Litigation

A Defense Perspective

by Stuart M. Feinblatt, Beth S. Rose and Gwen L. Coleman

James Gleick, in his acclaimed recent book *The Information*, describes the centrality of information in our modern technological age.[1] He views information as "the blood and the fuel, the vital principle" of the world. Of course, litigators have long recognized the importance of information, particularly regarding opposing parties, key witnesses and the subject matter of the pending lawsuit.

Assume you are a defense attorney defending a mass tort in which dozens of plaintiffs claim they have become disabled and homebound because they ingested your client's pharmaceutical. Suppose you could obtain evidence created by one of the plaintiffs—such as photographs or even videos—showing the allegedly disabled plaintiff skating or skiing. What if you could find proof that the plaintiff was a member of a 'victim's rights group' long before he sued, thereby creating a solid statute of limitations defense? What if there are writings showing the plaintiff was fully aware of the characteristics of the pharmaceutical (*i.e.*, side effects, warnings) he now claims were hidden from him?

Where could such valuable information be found? A very fertile source may well be social networking sites such as Facebook, Twitter, MySpace or LinkedIn. These sites are part of what is known as web 2.0. Web 1.0 was the initial version of the Internet, involving generally static websites where users could extract data in a one-way flow of information. Web 2.0, as one commentator has noted, is a much more dynamic platform intended to "facilitate the sharing of information among users." Web 2.0 has transformed the Internet into "a platform for services whose purpose is to harness collective intelligence."[2] In the world of web 2.0, visitors to websites are no longer mere passive viewers of information, instead they play an active role in creating the information contained on these sites.

Several social networking sites are at the center of web 2.0. These sites are 'social' because the participants freely share information with others regarding their daily activities, opinions, and interests, as well as the successes and sometimes failures of themselves, their family members and friends. The popularity of these social networking sites has exploded over the last few years. For example, Facebook has over 500 million active users.[3] Millions of people, probably including many readers of this article, spend 55 minutes or more per day on Facebook and other social networking sites.[4] The total number of estimated social networking users worldwide is probably closing in on one billion.[5]

Although hard to define, social networking sites have been characterized by one commentator as "web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse the list of connections and those made by others within the system."[6]

Beyond the most prominent social networking sites, it is fair to say that social networking extends to other forms of user-generated content on the Internet, such as blogs, communications on message boards, pictures or videos shared on sites such as YouTube or Flickr, and consumer reviews posted

on websites such as TripAdvisor.com.

The amount of information that can be gleaned from users' postings on these sites is virtually unlimited. Consider Facebook as an example. The typical user posts a 'profile' that is an open window to that person's opinions, values, interests and activities. Among other things, the typical profile may disclose the user's age; educational and work background; political and religious views; favorite books, movies, and products; and daily activities. As one court has noted, social media sites and other forms of electronic communication are likely to contain "statements involving observation of events surrounding us, statements regarding how we feel, our plans and motives, and our feelings (emotional and physical)."[7] The profile typically also contains photographs and perhaps videos that are fertile sources of information about the poster.

Of course, Facebook is a dynamic site where a user typically receives and responds to comments from other users. This feature further enhances the amount of information that can be obtained when it is part of a site.

Before turning to how defense counsel in mass tort litigation can use social networking information, a few special features of social networking sites must be kept in mind. These features challenge even the most skillful litigator seeking to obtain, preserve, authenticate and admit such information into evidence.

First, users typically control who can view their information and the types of information that can be shared. Internal controls generally cause the information to fall into three categories: public information that is available to everyone, semi-private information released only to authorized 'friends,' and largely private information that is only released to a single person or a few people.[8]

Second, the data kept on social networking sites is very dynamic, and users are constantly adding, deleting and altering information, and interacting with other users.

Finally, unlike the old paradigm where information was typically stored on the user's personal computer hard drive, social networking information is typically stored on servers maintained by the social networking site itself (or third-party hosts) and not on the user's own computer.[9]

Obtain Publicly Available Information About a Plaintiff or Witness

Assuming defense counsel wants to obtain and use information that plaintiffs or witnesses have posted about themselves on a social network, the first step should be to search the Internet for publicly available information (using Google, Yahoo or another search engine). This should allow counsel to determine whether the party or witness is active on one or more social networking sites. While, as noted above, some social networks offer internal controls that allow users to choose who can access and review their private information, a litigant can obtain information the user has placed in the public realm without 'friending' a plaintiff or witness.

Significantly, courts have predictably held that there is no expectation of privacy in this information because the user deliberately chose to make it publicly available to all Internet users.[10] Thus, counsel can review wall posts, status updates, photographs, messages and other information that plaintiffs and witnesses have made available to the general public on Facebook, MySpace and other social networking sites.[11] After counsel obtains all information that is publicly available, the next step should be to obtain additional information through written discovery.

Serve Plaintiff With Formal Discovery Demands

If the plaintiff's claim is similar to numerous other claims arising from the same product or event, the New Jersey Supreme Court may designate the case, or category of cases, as a mass tort to be assigned to a mass tort judge for coordination and management.[12] Shortly thereafter, a case management plan/order will likely be entered that will, among other things, typically require the parties preserve all documents containing information that is potentially relevant to the litigation.[13] Counsel should consider requesting that the preservation order specifically address social networking information contained on the parties' computer hard drives.[14]

In New Jersey mass tort litigation, judges like to streamline the discovery process and avoid multiple requests from defendants for the same plaintiff information. Thus, standard practice has been for the judge to encourage the parties to meet and fashion fact sheets (*i.e.*, questionnaires) that defendants can direct to individual plaintiffs in standard, agreed-upon forms.[15] The mass tort judge may also enter an order requiring production of paper and electronic documents agreed to by the parties. The information obtained from the fact sheets and related document production may enable defense counsel to winnow down the playing field by discovering, early on in the litigation, whether the plaintiff actually used or was exposed to a particular manufacturer's product during the relevant time period, and can lead to the dismissal of manufacturers who are not identified.

Discovery orders entered in some ongoing New Jersey mass torts have addressed computer-based information, including, potentially, social networking sites.[16] A skillful litigator should include questions about the social networks subscribed to by the plaintiff, dates of each subscription, user names and passwords, and all documents and information relating to relevant social networking postings.

After the plaintiff has served full and

responsive answers to the fact sheets and related document requests (if applicable), defense counsel can, if necessary and authorized by the mass tort judge, use supplemental formal discovery methods (*e.g.,* interrogatories, requests for documents, depositions, requests for admissions) to obtain wall posts, status updates, photographs, messages and other information from the plaintiff or the social network provider (SNP).[17]

The formal discovery demands should require the plaintiff to update his or her social networking information and produce all responsive documents and information relating to relevant postings. As a practical matter, upon receiving these demands the plaintiff may claim the requested information and documents are not discoverable because they are subject to some 'privacy' privilege.

Notably, two leading cases have gone so far as to hold that there is no legitimate reasonable expectation of privacy in even the private portions of social network postings because users consent to sharing information with others, notwithstanding privacy controls, when they join a social networking site. These courts have effectively rejected any social networking privilege.

In *Romano v. Steelcase*, a trial court in Suffolk County, New York, held that a plaintiff had no expectation of privacy because "when [she] created her Facebook and MySpace accounts, she consented to the fact that her personal information would be shared with others, notwithstanding her privacy settings."[18] Similarly, in *McMillen v. Hummingbird Speedway, Inc.*, a Pennsylvania trial court decision, the court declined to recognize private communications on Facebook as confidential, and allowed the defendant access to the plaintiff's social network sites.[19]

The take-away from these well-reasoned cases is that there is no reasonable expectation of privacy associated with social networking postings.[20] Even the guidelines of some service providers make clear when the user initially subscribes to a social networking site that there is a great risk the information shared on the site will become publicly accessible.[21] The bottom line is that there is no guarantee that information designated as 'private' will remain private, since the personal information shared with 'friends' can be disseminated by those friends to third parties.[22] Moreover, there can be no privacy expectation because the social network operator typically monitors everything the user is posting.[23]

General discovery rules, of course, apply in the social networking realm. Indeed, courts have held that private social networking information is discoverable if it is "relevant to any party's claim or defense," and "reasonably calculated to lead to the discovery of admissible evidence."[24] When plaintiffs place their physical or mental condition in controversy, defendants are generally entitled to discover private information posted on social networking sites that may be relevant to the issue of damages and the extent of a plaintiff's injuries.[25] Information on a social networking site that is relevant to a party's or witness's credibility has also been deemed discoverable.[26]

Obtain a Court Order Requiring Plaintiff to Produce Social Networking Information

In the event a plaintiff refuses to produce 'private' information, defense counsel should be prepared to go to court to obtain appropriate relief. The court may require the defendant to demonstrate that relevant information likely appears in the 'private' portion of the profile (*i.e.*, information that is released only to select 'friends'). The defendant can argue that, since the public portion of the plaintiff's profile contained information relevant to the litigation, it is likely the private portion will also contain relevant information.[27]

Even if the court directs the plaintiff to produce private wall posts and other information, the amount of information that can be produced may necessarily be limited. This is inevitable because, as noted above, the social networking information is maintained on the provider's computer and not the user's. The user, at best, can only turn over current 'snapshots' of the information that appears on the social networking pages. The user cannot produce deleted or altered information, because he or she typically cannot preserve historical social network information on his or her personal computer.

While it is unlikely that most users copy or backup this information, a plaintiff is obligated to preserve the information as soon as litigation is reasonably anticipated. In fact, initial case management orders in mass tort litigation often require that all parties preserve all documents (including electronically stored information) that are potentially relevant to the litigation, and that they preserve and not delete, tamper with, alter, or erase computerized data until the litigation is fully resolved.[28]

Subpoena the Information Directly From the Social Network Provider

So where can you turn for historical social network evidence? The best source is to obtain the information directly from the SNP. Most SNPs have policies allowing for the disclosure of information in order to comply with the law. For example, Facebook's privacy policy states that it will "disclose information pursuant to subpoenas, court orders, or other requests (including criminal and civil matters) if we have a good faith belief that the response is required by law."[29] The MySpace privacy policy indicates that it may "disclose personally identifiable information to comply with the law or legal process."[30]

Therefore, in order to attempt to obtain the entire universe of current and archived information a user has historically posted

on a social networking site, defense counsel should serve the SNP with a third-party subpoena attaching a comprehensive set of written discovery demands. The demands should request all electronically stored information that has been transmitted through the SNP since the plaintiff or witness initially subscribed to the service. Fortunately, the SNP has the capacity to retrieve this information, since it stores social networking information on third-party servers for extended periods.

It should come as no surprise that the SNP may object to the discovery demands on the grounds that they are overly broad, vague and unduly burdensome. Defense counsel, therefore, should be careful to specifically tailor the demands to facilitate the discovery process (*i.e.*, relate the demands to the plaintiff's injuries, product at issue, etc.).[31]

The next challenge is that the SNP will probably rely on the Stored Communications Act to limit or shield the requested information from disclosure. This act prohibits SNPs from "knowingly divulging the contents of any communication while in electronic storage by that service."[32] There are limited exceptions. The act does not apply to electronic communications that are "readily accessible to the general public," but rather only restricts the SNP's ability to produce private communications that were transmitted through its servers.[33] It does permit, however, the production of private information as long as counsel obtains lawful consent from the user.[34]

Given these provisions, counsel can serve a carefully tailored third-party subpoena on an SNP to obtain public information.[35] In addition, it is advisable to attempt to obtain a court order that requires the plaintiff or witness to execute a consent and authorization form for the release of private information from the SNP. In short, with careful planning counsel can successfully obtain information from a social networking site, while complying with the provisions of the act.[36]

Best Practices for the Authentication and Admissibility of Social Networking Information at Trial

Assuming that a user's social networking information is relevant and discoverable, the final challenge for defense counsel will be to get the information admitted into evidence. Since the information is an out-of-court statement, it is subject to the hearsay rules.[37] Thus, while it cannot freely be offered for the truth of the matter asserted, a skillful defense counsel can successfully get the information admitted under a hearsay exception.[38]

The adversary may argue, however, that defense counsel did not comply with the rules of evidence and properly authenticate the social networking information prior to its admission.[39] Of course, defense counsel must lay the proper foundation by establishing that the plaintiff or witness actually authored the posting during the relevant time period.

The easiest way to prove this is to confirm in sworn testimony that the plaintiff or witness posted the statement. But this may not happen. Indeed, the plaintiff may argue that manipulations of information and hackings are prevalent on the Internet, and, therefore, the rules of evidence regarding authentication must be stringently applied to social network postings.[40]

Defense counsel should keep in mind that there are useful tools to authenticate social network data, such as hash marks (numerical identifiers assigned to a file), and metadata (information describing the date, time, and identity of the creator).[41] Or defense counsel can try to locate a non-party witness who can affirm that he or she viewed the user posting the information, and that the proffered evidence is an accurate copy of that information. The non-party witness can vouch for the authenticity of the information by attempting to link the user to the posting. For example, he or she can identify pictures appearing on the profile, affirm that the user's birthday is accurate or nicknames are correct, or affirm that the user is, in fact, affiliated with the organizations posted.[42]

Attorneys Must Play by the Ethics Rules

Remember that the ethics rules apply to social networking discovery. Counsel should not pretend to be a plaintiff's or witness's friend in order to obtain social network information that is relevant to the case. And certainly, counsel should not hire a third party to engage in this conduct either. State bars have found these practices to be improper and unethical because they omit a highly material fact—that the attorney or third party who asked to be allowed access to the social networking site is doing so for purposes of the litigation (*e.g.*, to obtain impeachment testimony, review incriminating photographs, or determine the extent of the plaintiff's physical or mental injuries).

The Philadelphia Bar Association's Professional Guidance Committee addressed this precise issue in a recent advisory ethics opinion.[43] An attorney sought guidance after learning, during the deposition of an unrepresented non-party witness, that the witness subscribed to MySpace and Facebook. Following the deposition, the attorney considered asking a third party to friend the witness in order to gain access to the private portions of his social network pages and retrieve information the attorney could potentially use to impeach the witness at trial.

The committee found that the attorney's proposed conduct was deceptive because the third party seeking access was not planning to disclose that his sole motivation for his contact with the witness was to obtain and share the information with the attorney for the purpose of impeaching her testimony. However, the committee did find that if an attorney directly and forthrightly makes a

friend request to the witness (presumably disclosing his or her identity as a lawyer and the purpose of the access), and if the witness grants that request, access to his or her profile pages would be permissible and not in violation of the ethics rules.

The New York City Bar Association's Committee on Professional Ethics recently analyzed whether an attorney could view and access the public portion of a party's Facebook or MySpace pages, without friending the party, in order to gain impeachment material.[44] The committee opined that an attorney could review and use the public portion of a party's social networking page in a pending litigation for impeachment purposes. However, in a footnote the committee suggested in *dictum* that the ethics rules prohibit an attorney from friending a party or recruiting a third person to do so if the party is represented by counsel (absent prior consent from the party's attorney). Notably, if the party is not represented by counsel, the attorney can send a friend request, as long as the attorney uses his or her real name and profile, and does not seek to give legal advice (other than the advice to obtain counsel if the other party's interests are likely to conflict with those of the lawyer's own client).[45]

Finally, the San Diego County Bar Legal Ethics Committee recently considered similar ethical issues.[46] In particular, the committee addressed whether an attorney, representing a former employee in a wrongful discharge action against a corporation, could send out a friend request to high-ranking employees at the defendant corporation whom the attorney's client had identified as being dissatisfied with the employer, and therefore likely to make negative comments about the employer on their Facebook pages.

Relying on California Rule of Professional Conduct 2-100, which prohibits an attorney from communicating directly or indirectly about the subject of the client's representation with another party known to be represented by another attorney in the matter, the committee first assumed that the high-ranking employees of the corporation are represented parties. Based on that assumption, the committee concluded that a generic request that the employees friend the attorney constituted improper communication with a represented party about the subject matter of the representation. This is so because the communication to the employees was motivated by the quest to obtain information regarding the subject matter of the lawsuit, namely damaging information about the client's former employer. The subject of the legal representation need not be directly referenced in the friend request for the request to be about or concerning the subject of the representation.

In addition, commenting favorably on the Philadelphia ethics opinion noted above, the committee concluded that an attorney violates his or her ethical duty not to deceive by making a friend request to a represented party without disclosing the reasons for the request. As the committee put it, "[r]epresented parties shouldn't have 'friends' like that and no one—represented or not, party or nonparty—should be misled into accepting such a friendship."

Conclusion

Social networking sites undoubtedly can be a potential treasure trove for defense counsel in mass tort litigation. Users of social networking sites often freely disclose valuable personal information about their claims, injuries and credibility that can be extremely relevant to their cases. Despite privacy controls, a litigator can effectively discover and utilize social networking information at trial through careful discovery planning and a basic understanding of this evolving technology. ⚖

Endnotes

1. James Gleick, *The Information: A History, A Theory, A Flood* (Pantheon 2011).
2. *See* Andrew C. Payne, Tribal Nation Economics and Legal Infrastructure: Note: Twitigation: Old Rules in a New World, 49 *Washburn L.J.* 841, 847 (2010) (*citing* Tim O'Reilly and John Battelle, Web Squared: Web 2.0 Five Years On 1 (2009)).
3. www.facebook.com/press/info. php. Facebook Factsheet (last revised date Dec. 22, 2010).
4. Eric Eldon, Facebook Occupies 7 Hours of the Average US User's January, NielsonWire (Feb. 16, 2010).
5. EBiz/MBA, Top 15 Most Popular Social Networking Websites, December 2010, www.ebizmba.com/articles/social-networking-websites.
6. Danah M. Boyd and Nicole B. Ellison, Social Network Sites: Definition, History, and Scholarship, 13 *J. Computer-Mediated Comm.* (Issue 1) (2007), available at http://jcmc.indiana.edu/vol. 3/issue 1/boyd.ellison.html.
7. *See Lorraine v. Markel Amer. Insur. Co.*, 241 F.R.D. 534, 569 (D. Md. 2007).
8. *See* Andrew C. Payne, Tribal Nation Economics and Legal Infrastructure: Note: Twitigation: Old Rules in a New World, 49 *Washburn L.J.* at 844-45. Despite these controls, as noted later in this article, Facebook and other social networks sites have very detailed privacy and security policies that courts have recognized generally eliminate a social networking user's expectation of privacy.
9. *Id.* at 863-64.
10. *See Guest v. Leis, et al.* 255 F.3d 325, 335-36 (6th Cir. 2001) (Internet users lack a legitimate expectation of privacy in materials intended for publication); *Independent Newspapers, Inc. v. Brodie*, 966 A.2d 432, 438 (Md. 2009) (information posted on a social networking site is available "to the world at large"); *Beye v. Horizon Blue Cross Blue Shield of New Jersey*, Civil Action No. 06-5337 (FSH), 2007

U.S. Dist. LEXIS 100915, *13 (D. N.J. Dec. 12, 2007) (plaintiffs were ordered to produce postings on Facebook and MySpace that were "shared with other people" about eating disorders); *Moreno v. Hanford Sentinel, Inc.*, 172 Cal. App. 4th 1125, 1130 (Cal. Ct. App. 2009) (no expectation of privacy in MySpace page because information was publicly accessible).

11. Although beyond the scope of this article, when evaluating jurors, litigants should also consider researching social network postings of jurors, and other information available on the Internet. In New Jersey, a plaintiff's counsel, during jury selection, accessed the Internet from his laptop computer to obtain public information about prospective jurors. Defense counsel objected and the trial court prohibited him from researching the jurors on grounds that it afforded counsel an unfair advantage. The Appellate Division reversed the ruling, finding that the use of the Internet was proper because the court was equipped with WiFi capability. The defense verdict remained intact because the court concluded that there was no prejudice from prohibiting the research. *See Carino v. Muenzen*, A-5491-08T1, 2010 N.J. Super. Unpub. LEXIS 2154, *27 (App. Div. 2010).
12. *New Jersey Mass Tort (Non-Asbestos) Resource Book*, 3rd Ed. (November 2007).
13. *Id*. at 13.
14. All parties have a duty to preserve hard copy and electronically stored information when litigation commences or is reasonably anticipated. A plaintiff's duty is more often triggered before litigation commences, in large part, because plaintiffs control the timing of litigation. *See Pension Comm. of the Univ. of Montreal Pension Plan v. Banc of Am. Sec. LLC*, 685 F. Supp. 2d 456, 466 (S.D.N.Y. 2010). In this regard, defense counsel should take steps to confirm that a plaintiff is preserving social media that is within his or her possession, custody or control.
15. *New Jersey Mass Tort (Non-Asbestos) Resource Book* at 26.
16. An example is the mass tort involving pelvic mesh. *See In re Pelvic Mesh Litigation/Bard*, Case Management Order No. 2, Case No. 292 (Law Div., Atlantic Cty., May 11, 2011). The order entered by Judge Higbee attaches a plaintiff fact sheet that requires, among other things, that plaintiffs produce all blogs, Facebook posts, and tweets they sent or received concerning the pelvic mesh product(s) at issue in the litigation. Another example is the mass tort involving Accutane and its generic equivalents. *See In re Accutane Litigation*, Order Re Completion of Fact Sheet Documents, Case No. 271 (Law Div., Atlantic Cty., Dec. 4, 2008). The orders entered by Judge Higbee in that mass tort relating to completion of fact sheets and production of electronic discovery from the plaintiffs' computers require, among other things, that the plaintiffs produce all chat room postings regarding the medication and all information downloaded from any website regarding the product.
17. These methods should also be used in cases in which fact sheets are not used.
18. 907 N.Y.S.2d 650 (N.Y. Sup. Ct., Suffolk Cty., Sept. 21, 2010).
19. No 113-2010 CD, 2010 Pa. Dist. & Cnty. Dec. LEXIS 270 (Pa. Ct .Common Pleas, Jefferson Cty., Sept. 9, 2010).
20. These courts note that there is no general privacy privilege that shields appropriate discovery requests. *See Romano v. Steelcase*, 907 N.Y.S.2d 650, 655-57 (N.Y. Sup. Ct., Suffolk Cty. Sept. 21, 2010); *McMillen v. Hummingbird Speedway, Inc.*, No. 113-2010 CD, 2010 Pa. Dist. & Cnty. Dec. LEXIS 270, *8-10 (Common Pleas Ct., Jefferson Cty, Sept. 9, 2010).
21. Facebook's privacy policy sets forth:

> Risks inherent in sharing information. Although we allow you to set privacy options that limit access to your information, please be aware that no security measures are perfect or impenetrable. We cannot control the actions of other users with whom you share your information. We cannot guarantee that only authorized persons will view your information. We cannot ensure that information you share on Facebook will not become publicly available. We are not responsible for third party circumvention of any privacy settings or security measures on Facebook. You can reduce these risks by using common sense security practices such as choosing a strong password, using different passwords for different services, and using up to date antivirus software.

22. *McMillen*, 2010 Pa. Dist. & Cnty. Dec. LEXIS at *8-10.
23. *Id*. at 8.
24. Fed. R. Civ. P. 26(b). *See Mackelprang v. Fidelity Nat'l Title Agency of Nev.*, 2007 U.S. Dist. LEXIS 2379, *25-26 (D. Nev. 2007) (proper method for obtaining information relating to plaintiff's emotional distress and mental condition was to serve discovery demands requesting that plaintiff produce relevant MySpace private messages); *McCann v. Harleysville Ins.*, 1179 CA 10-00612, 2010 N.Y. App. Div. LEXIS 8396, *1 (Nov. 12, 2010) (defendant was permitted to discover plaintiff's Facebook account but could not conduct a "fishing expedition"); *EEOC v. Simply Storage Mgmt.,* 270 F.R.D. 430, 436 (S.D. Ind. 2010) (plaintiff ordered to produce private profiles,

postings and messages on social networking site that were relevant to plaintiff's emotional state).

25. *See Romano v. Steelcase*, 907 N.Y.S.2d at 653-54 (Facebook and MySpace pages used to show that plaintiff's claim for loss of enjoyment of life was exaggerated because she had traveled to Florida and Pennsylvania and was not confined to her house); *McMillen v. Hummingbird Speedway, Inc.*, No 113-2010 CD, 2010 Pa. Dist. & Cnty. Dec. LEXIS 270, at *1-2 (Facebook page used to show that claim for permanent impairment was exaggerated because plaintiff went on fishing trip and attended Daytona 500).
26. *See In the Matter of K.W.*, 666 S.E.2d 490, 494-95 (Ct. App. N.C. 2008) (trial court improperly excluded MySpace page, which was admissible impeachment evidence as to prior sexual history in child abuse case); *People v. Javier*, 2009 Cal. App. unpub. LEXIS 6703, *53-54 (Aug. 19, 2009) (appellate court affirmed admissibility of MySpace page to impeach appellant's testimony and prior statements that he did not belong to a gang); *Clark v. State of Indiana*, 915 N.E.2d 126, 131 (Indiana S.C. 2009) (prosecution was permitted to confront the defendant with his statements on MySpace boasting about his crime); *State of Ohio v. Jaysen*, Case No. CA2008-05-044, 2009 Ohio App. LEXIS 2112, *29-32 (May 18, 2009) (trial court properly admitted MySpace online conversations to show sexual conduct).
27. *Romano v. Steelcase*, 907 N.Y.S.2d at 654 (ordering plaintiff to produce private information because "plaintiff's public profile page on Facebook shows her smiling happily in a photograph outside the confines of her home despite her claim that she has sustained permanent injuries and is largely confined to her house and bed").
28. *See, e.g., In Re: Accutane Litigation*, Case Management Order, Case No. 271 (Law Div., Atlantic Cty., May 9, 2005); *In Re: Levaquin Litigation*, Case Management Order No. 1, Case No. 286 (Law Div., Atlantic Cty., June 25, 2009); *In Re: Nuvaring Litigation*, Initial Order for Case Management, Case No. 284 (Law Div., Bergen Cty., March 10, 2009).
29. www.facebook.com/policy.php. How We Share Information (last revised Dec. 22, 2010).
30. www.myspace.com/Help/Privacy, Use: MySpace's Use of PII (personally identifiable information) (last revised Dec. 7, 2010).
31. *See Ledbetter v. Wal-Mart Stores, Inc.*, 06 cv 01958, 2009 U.S. Dist. LEXIS 126859, *5 (D. Colo., April 21, 2009) (holding that information sought in subpoenas to MySpace, Facebook and MeetUp.com was relevant and reasonably calculated to lead to the discovery of admissible evidence).
32. 18 U.S.C. §2701 *et seq*.
33. 18 U.S.C. §2511(2)(g). A California federal district court recently held that the SNP could invoke the act to protect private communications transmitted through its social networking site. *See Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965 (C.D. Cal. 2010). There, defendants served third-party subpoenas to Facebook and MySpace requesting all public and private communications that were relevant to the litigation. The plaintiff filed a motion to quash the subpoenas on grounds that the act prohibited the disclosure of electronically stored information, and on grounds that the subpoena was overbroad and sought irrelevant information. The court drew a distinction between the plaintiff's private messages and public wall postings and quashed the subpoena only with respect to private messages. It remanded for a determination of whether the plaintiff's privacy settings rendered the public wall postings unprotected under the act. As one article has noted, the *Crispin* court struggled with the application of the act to social networking sites because it was passed in an outdated 1980's computer environment. *See* Alan Klein, John M. Lyons and Andrew R. Sperl, Social Networking Sites: Subject to Discovery? *Natl L. J.* (Aug. 23, 2010).
34. 18 U.S.C. §2702 (b)(3) of the act provides that a SNP "may divulge the contents of a communication...(3) with the lawful consent of the originator or an addressee or intended recipient of such communication."
35. *See Mackelprang v. Fidelity Nat'l Title Agency of Nev.*, 2007 U.S. Dist. LEXIS 2379, at *5 (MySpace produced public communications relating to sexual harassment claims pursuant to subpoena).
36. *Romano*, 907 N.Y.S.2d at 657 (plaintiff ordered to execute a consent and authorization permitting defendant to access current, deleted and archived Facebook and MySpace records).
37. *See* N.J.R.E. 801 *et seq*.
38. *See supra* note 16.
39. *See* N.J.R.E. 901, which states that "the requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter is what its proponent claims."
40. *See Lorraine v. Markel Amer. Insur. Co.*, 241 F.R.D. at 537-38, 542-43 (litigants must comply with the rules of evidence regarding the admissibility and authentication of electronically stored information).
41. *Id*. at 546-47.
42. *People v. Javier*, 2009 Cal. App.

unpub. LEXIS 6703, *53-54 (Aug. 19, 2009) (witness confirmed that appellant's nickname was correct on MySpace page); *Griffin v. State*, 192 Md. App. 518, 543 (2010), *cert. granted*, 415 Md. 607 (2010) (trial court properly admitted into evidence girlfriend's MySpace profile page based on the authenticating witness's testimony that, among other things, a picture depicted her with the defendant, her birth date matched the date on the profile, and her nickname for the defendant appeared on the profile).

43. Opinion 2009-02 (March 2009).
44. Opinion 2010-2 (Sept. 29, 2010).
45. *See Id.* at ftn. 1.
46. Opinion 2011-2 (May 24, 2011).

Stuart M. Feinblatt *is a member of the law firm of Sills Cummis & Gross, P.C.* ***Beth S. Rose*** *is a member of the firm and is chair of the product liability practice group and co-chair of the litigation practice group.* ***Gwen L. Coleman*** *is of counsel to the firm. The views and opinions expressed in this article are those of the authors and do not necessarily reflect those of Sills Cummis or its clients.*