

# New York Law Journal

## Technology Today

WWW.NYLJ.COM

©2010 ALM

An ALM Publication

VOLUME 244—NO. 86

TUESDAY, NOVEMBER 2, 2010

### STATE E-DISCOVERY

# The Ethics of Social Networking Discovery

By  
**Mark A.  
Berman**



Just like conducting Westlaw or Lexis due diligence on an individual, social networking sites need to be reviewed as part of discovery protocol when seeking to obtain relevant information concerning a person or entity. Such searches should not be limited to being performed only in connection with personal injury litigations, but equally should extend, for example, to commercial, product liability, intellectual property, restrictive covenant and employment disputes.

Facebook and MySpace are not “friends” of litigants who would no doubt want to keep the contents of their social network postings private. And as the recent trial court decision in *Romano v. Steelcase, Inc.*<sup>1</sup> makes clear, not only may a court require a person to execute an authorization providing for a social networking site to produce one’s so-called “public” postings, but a court also may require such authorization to extend to private posts not accessible to the public, as well as to deleted and archived posts stored by the site.

However, the use of social networking sites by attorneys or investigators as an investigative tool is not unfettered and is circumscribed by ethical rules governing the conduct of counsel, as well as by statutes governing a person’s access to someone else’s information maintained on such sites.

Two recent ethical opinions issued by the New York State Bar Association<sup>2</sup> and the New York City Bar<sup>3</sup> address issues relating to counsel accessing social networking sites and



ISTOCK

they, as well as ethical opinions from other jurisdictions discussing this emerging area of electronic discovery, need to be reviewed before conducting social networking due diligence or an investigation. To not appreciate the ethical limitations concerning accessing a person’s social networking site could put counsel in an ethical quandary with the potential for civil liability.

In *Romano*,<sup>4</sup> the court addressed the issue of whether plaintiff’s posts and photos published to her Facebook and MySpace pages were discoverable in a personal injury case. The court found that “[i]n light of the fact that the public portions of Plaintiff’s social networking sites contain material that is contrary to her claims and deposition testimony,<sup>5</sup> there is a reasonable likelihood that the private portions of her sites may contain...evidence...all of which are material and relevant to the defense of this action” and “[p]reventing Defendant from accessing to Plaintiff’s private postings... would be in direct contravention to the liberal disclosure policy in New York State” and “would condone Plaintiff’s attempt to hide relevant information behind self-regulated privacy settings.”<sup>6</sup>

The court held that plaintiff had no expectation of privacy to her posts relying, in part, on *United States v. Lifshitz*,<sup>7</sup> which noted:

[u]sers would logically lack a legitimate expectation of privacy in materials intended for publication or public posting. They would lose a legitimate expectation of privacy in an e-mail that had already reached its recipient; at this moment, the e-mailer would be analogous to a letter-writer whose expectation of privacy ordinarily terminates upon delivery of the letter.<sup>8</sup>

The court found there was no legitimate reasonable expectation of privacy and

[t]hus, 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 else they would cease to exist. Since Plaintiff knew that her information may become publicly available, she cannot now claim that she had a reasonable expectation of privacy. As recently set forth by commentators regarding privacy and social networking sites, given the millions of users, “[i]n this environment, privacy is no longer grounded in reasonable expectations, but rather in some theoretical protocol better known as wishful thinking.”<sup>9</sup>

Accordingly, noting that the policies of Facebook and MySpace do not “guarantee complete privacy” and where defendant in *Romano* had attempted to obtain the sought-after information through a notice for discovery and a deposition, but was “thwarted” by plaintiff, and where plaintiff also had refused to provide her authorization for the release of the information to defendant,

MARK A. BERMAN, a partner at commercial litigation firm Ganfer & Shore, is secretary of the e-discovery committee of the Commercial and Federal Litigation Section of the New York State Bar Association. ANNE D. TABACK, an associate at Ganfer & Shore, assisted in the preparation of this article.

the court compelled plaintiff to provide the consent and authorization required by Facebook and MySpace<sup>10</sup> to gain access to plaintiff's current and historical pages and accounts, including all deleted or archived pages, and related materials.<sup>11</sup>

**Ethical Opinions**

In the state bar's Ethical Opinion 843, the question asked was "[m]ay a lawyer view and access the Facebook or MySpace pages of a party other than his or her client in pending litigation in order to secure information about the party for use in the lawsuit, including impeachment material, if the lawyer does not "friend" the party<sup>12</sup> and instead relies on public pages posted by the party that are accessible to all members of the network."<sup>13</sup> The opinion held that such conduct was permissible:

[a]s long as the lawyer does not 'friend' the other party or direct a third person to do so, accessing the social network pages of the party will not violate Rule 8.4. (prohibiting deceptive or misleading conduct),<sup>14</sup> Rule 4.1 (prohibiting false statements of fact or law), or Rule 5.3(b) (1) (imposing responsibility on lawyers for unethical conduct by nonlawyers acting at their direction.)<sup>15</sup>

In the city bar's Ethical Opinion 2010-2, the question asked was "[m]ay a lawyer, either directly or through an agent, contact an *unrepresented* person through a social networking website and request permission to access her web page to obtain information for use in litigation?"<sup>16</sup> The opinion held that:

[b]ecause non-deceptive means of communication ordinarily are available to obtain information on a social networking page—through ordinary discovery of the targeted individual or of the social networking sites themselves—trickery<sup>17</sup> cannot be justified as a necessary last resort. For this reason we conclude that lawyers may not use or cause others to use deception in this context.

Rather than engage in "trickery," lawyers can—and should—seek information maintained on social networking sites, such as Facebook, by availing themselves of informal discovery, such as the truthful "friending" of unrepresented parties, or by using formal discovery devices such as subpoenas directed to non-parties in possession of information maintained on an individual's social networking page.

Given the availability of these legitimate discovery methods, there is and can be no justification for permitting the use of deception to obtain information from a witness on-line.<sup>18</sup>

The opinion notes that it did not address the prohibitions of the Stored Communications Act §19 and the Electronic Communications Privacy Act, 18 U.S.C. § 2510 et seq, but cautioned that counsel ensure that her conduct comports with applicable law.

Individuals must be aware that, notwithstanding privacy settings, information posted on social networking sites may be "fair game" and fully discoverable in litigation.

Consequently, individuals must be aware that, notwithstanding privacy settings and the belief that information posted on a social networking site is private and one can control such information's dissemination to "uninvited visitors," information that was ever posted on such sites may be "fair game" and fully discoverable in litigation.

However, counsel and investigators need to be careful in accessing such information in order not to violate applicable ethical canons and statutes.



1. *Romano v. Steelcase, Inc.*, Index No. 2233/2006 (Sup. Ct. Suffolk Co., Sept. 21, 2010).  
 2. New York State Bar Association Committee on Professional Ethics, Formal Op. 843, Sept. 10, 2010.  
 3. The Association of the Bar of the City of New York Committee on Professional Ethics, Formal Op. 2010-2, Sept. 2010. The author of this article is a member of such committee and was involved in the opinion's drafting.  
 4. See, e.g., *Bass v. Miss Porter's School*, 2009 WL 3724968, \*1 (D. Conn. Oct. 27, 2009) ("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.") (internal quotations omitted).  
 5. 369 F.3d 173 (2d Cir. 2004).  
 6. Ordering such consent and authorization would be consistent with the Stored Communications Act, 18 U.S.C. § 2701(a)(1) et seq., which prohibits the subpoenaing of information from social networking sites.  
 7. NYS Ethical Opinion 843 provides that "[i]f a lawyer attempts to "friend" a represented party in a pending litigation, then the lawyer's conduct is governed by Rule 4.2 (the "non-contact" rule), which prohibits a lawyer from communicating with the represented party about the subject of the representation absent prior consent from the represented party's lawyer." NYS Formal Op. at § 5 fn. 1 (emphasis in original). The opinion further indicates that "[i]f the lawyer attempts to "friend" an unrepresented party, then the lawyer's conduct is governed by Rule 4.3, which prohibits a lawyer from stating or implying that he or she is disinterested, requires the lawyer to correct any misunderstanding as to the lawyer's role, and prohibits the lawyer from giving legal advice other than the advice to secure counsel of the other party's interests are likely to conflict with those of the lawyer's client." Id. (emphasis in original).

8. The opinion notes that this would include employing deception by the lawyer or someone directed by the lawyer to become a member of the network. Id. at § 5.  
 9. ABCNY Formal Op. at 1 (emphasis added).

10. "Trickery" would include, among other things, "making a 'friend request' falsely portraying the attorney or investigator as the witness's long lost classmate, prospective employer or friend of a friend" or emailing a "YouTube account holder, falsely touting a recent digital posting or potential interest as a hook as ask to subscribe to the account holder's 'channel' and view all her digital postings." Id. at 3.

11. Congress passed the Stored Communications Act in 1986 as part of the Electronic Communications Privacy Act. "The SCA was enacted because the advent of the Internet presented a host of potential privacy breaches that the Fourth Amendment does not address." (citations omitted). The SCA prevents "providers" of communication services from divulging private communications to certain entities and individuals. (citation omitted). It "creates a set of Fourth Amendment-like privacy protections by statute, regulating the relationship between government investigators and service providers in possession of users' private information."

*Cripsin v. Audigier*, \_\_\_ F. Supp.2d \_\_\_, 2010 2293238 at \*3 (C.D. Cal. May 26, 2010) (citations omitted) (Facebook and MySpace subpoenas seeking private messages quashed, and court vacated order permitting subpoenaing of Facebook wall postings and MySpace comments and remanded for a more complete evidentiary record).

The SCA make it "an offense to intentionally access stored communications without authorization or in excess of authorization." (*Pietrylo v. Hillstone Rest. Group*, 2008 WL 6085437, at \*3 (D.N.J. July 25, 2008)), but an exception exists "with respect to conduct authorized...by a user of that service with respect to a communications intended for that user." 18 U.S.C. 2701(c)(2). In denying defendant's motion for summary judgment under the SCA, the court in *Pietrylo* found a material issue of disputed fact to exist where a user provided a "password" to a MySpace page under "duress." The court found such "consent" may not have been "voluntary," and therefore not "authorized" under the SCA. Id. at \*4. Subsequently, a jury found for plaintiff, and the court stated, in ruling on defendant's motion for judgment as a matter of law, that the jury could "reasonably infer" from the testimony that the "purported 'authorization' was coerced or provided under pressure." *Pietrylo*, 2009 WL 3128420, at \*3 (D.N.J. Sept. 25, 2009). The court noted that there was evidence that defendant representative's accessed the site, "even though it was clear on the website that [it] was intended to be private and only accessible to invited members" and "that defendant's representatives knew that they were not authorized to access the contents of the [site] from the manner and means that [certain individuals] used to get access to the password-protected MySpace page." Id.

Reprinted with permission from the November 2, 2010 edition of the NEW YORK LAW JOURNAL © 2010 ALM Media Properties, LLC. All rights reserved. Further duplication without permission is prohibited. For information, contact 877-257-3382 or reprints@alm.com. # 070-11-10-12

**Ganfer & Shore, LLP**

360 Lexington Avenue  
 New York, New York 10017  
 212.922.9250  
 mberman@ganfershore.com