THE ASSOCIATION OF THE BAR OF THE CITY OF NEW YORK
COMMITTEE ON PROFESSIONAL ETHICS

FORMAL OPINION 2010-2

OBTAINING EVIDENCE FROM SOCIAL NETWORKING WEBSITES

TOPIC: Lawyers obtaining information from social networking websites.

DIGEST: A lawyer may not attempt to gain access to a social networking website under false pretenses, either directly or through an agent.

RULES: 4.1(a), 5.3(c)(1), 8.4(a) & (c)

QUESTION: May 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?

OPINION

Lawyers increasingly have turned to social networking sites, such as Facebook, Twitter and YouTube, as potential sources of evidence for use in litigation.[1] In light of the information regularly found on these sites, it is not difficult to envision a matrimonial matter in which allegations of infidelity may be substantiated in whole or part by postings on a Facebook wall.[2] Nor is it hard to imagine a copyright infringement case that turns largely on the postings of certain allegedly pirated videos on YouTube. The potential availability of helpful evidence on these internet-based sources makes them an attractive new weapon in a lawyer's arsenal of formal and informal discovery devices.[3] The prevalence of these and other social networking websites, and the potential

[1] Social networks are internet-based communities that individuals use to communicate with each other and view and exchange information, including photographs, digital recordings and files. Users create a profile page with personal information that other users may access online. Users may establish the level of privacy they wish to employ and may limit those who view their profile page to "friends" – those who have specifically sent a computerized request to view their profile page which the user has accepted. Examples of currently popular social networks include Facebook, Twitter, MySpace and LinkedIn.

[2] See, e.g., Stephanie Chen, Divorce attorneys catching cheaters on Facebook, June 1, 2010, http://www.cnn.com/2010/TECH/social.media/06/01/facebook.divorce.lawyers/index.html?hpt=C2.

[3] See, e.g., Bass ex rel. Bass v. Miss Porter's School, No. 3:08cv01807, 2009 WL 3724968, at *1-2 (D. Conn. Oct. 27, 2009).

benefits of accessing them to obtain evidence, present ethical challenges for attorneys navigating these virtual worlds.

In this opinion, we address the narrow question of whether a lawyer, acting either alone or through an agent such as a private investigator, may resort to trickery via the internet to gain access to an otherwise secure social networking page and the potentially helpful information it holds. In particular, we focus on an attorney's direct or indirect use of affirmatively "deceptive" behavior to "friend" potential witnesses. We do so in light of, among other things, the Court of Appeals' oft-cited policy in favor of informal discovery. See, e.g., Niesig v. Team I, 76 N.Y.2d 363, 372, 559 N.Y.S.2d 493, 497 (1990) ("[T]he Appellate Division's blanket rule closes off avenues of informal discovery of information that may serve both the litigants and the entire justice system by uncovering relevant facts, thus promoting the expeditious resolution of disputes."); Muriel, Siebert & Co. v. Intuit Inc., 8 N.Y.3d 506, 511, 836 N.Y.S.2d 527, 530 (2007) ("the importance of informal discovery underlies our holding here"). It would be inconsistent with this policy to flatly prohibit lawyers from engaging in any and all contact with users of social networking sites. Consistent with the policy, we conclude that an attorney or her agent may use her real name and profile to send a "friend request" to obtain information from an unrepresented person's social networking website without also disclosing the reasons for making the request.[4] While there are ethical boundaries to such "friending," in our view they are not crossed when an attorney or investigator uses only truthful information to obtain access to a website, subject to compliance with all other ethical requirements. See, e.g., id., 8 N.Y.3d at 512, 836 N.Y.S.2d at 530 ("Counsel must still conform to all applicable ethical standards when conducting such [ex parte] interviews [with opposing party's former employee]." (citations omitted)).

The potential ethical pitfalls associated with social networking sites arise in part from the informality of communications on the web. In that connection, in seeking access to an individual's personal information, it may be easier to deceive an individual in the virtual world than in the real world. For example, if a stranger made an unsolicited face-to-face request to a potential witness for permission to enter the witness's home, view the witness's photographs and video files, learn the witness's relationship status, religious views and date of birth, and review the witness's personal diary, the witness almost certainly would slam the door shut and perhaps even call the police.

In contrast, in the "virtual" world, the same stranger is more likely to be able to gain admission to an individual's personal webpage and have unfettered access to most, if not all, of the foregoing information. Using publicly-available information, an attorney or her investigator could easily create a false Facebook profile listing schools, hobbies,

[4] The communications of a lawyer and her agents with parties known to be represented by counsel are governed by Rule 4.2, which prohibits such communications unless the prior consent of the party's lawyer is obtained or the conduct is authorized by law. N.Y. Prof'l Conduct R. 4.2. The term "party" is generally interpreted broadly to include "represented witnesses, potential witnesses and others with an interest or right at stake, although they are not nominal parties." N.Y. State 735 (2001). Cf. N.Y. State 843 (2010)(lawyers may access public pages of social networking websites maintained by any person, including represented parties).

interests, or other background information likely to be of interest to a targeted witness. After creating the profile, the attorney or investigator could use it to make a "friend request" falsely portraying the attorney or investigator as the witness's long lost classmate, prospective employer, or friend of a friend. Many casual social network users might accept such a "friend request" or even one less tailored to the background and interests of the witness. Similarly, an investigator could e-mail a YouTube account holder, falsely touting a recent digital posting of potential interest as a hook to ask to subscribe to the account holder's "channel" and view all of her digital postings. By making the "friend request" or a request for access to a YouTube "channel," the investigator could obtain instant access to everything the user has posted and will post in the future. In each of these instances, the "virtual" inquiries likely have a much greater chance of success than if the attorney or investigator made them in person and faced the prospect of follow-up questions regarding her identity and intentions. The protocol on-line, however, is more limited both in substance and in practice. Despite the common sense admonition not to "open the door" to strangers, social networking users often do just that with a click of the mouse.

Under the New York Rules of Professional Conduct (the "Rules"), an attorney and those in her employ are prohibited from engaging in this type of conduct. The applicable restrictions are found in Rules 4.1 and 8.4(c). The latter provides that "[a] lawyer or law firm shall not . . . engage in conduct involving dishonesty, fraud, deceit or misrepresentation." N.Y. Prof'l Conduct R. 8.4(c) (2010). And Rule 4.1 states that "[i]n the course of representing a client, a lawyer shall not knowingly make a false statement of fact or law to a third person." Id. 4.1. We believe these Rules are violated whenever an attorney "friends" an individual under false pretenses to obtain evidence from a social networking website.

For purposes of this analysis, it does not matter whether the lawyer employs an agent, such as an investigator, to engage in the ruse. As provided by Rule 8.4(a), "[a] lawyer or law firm shall not . . . violate or attempt to violate the Rules of Professional Conduct, knowingly assist or induce another to do so, or do so through the acts of another." Id. 8.4(a). Consequently, absent some exception to the Rules, a lawyer's investigator or other agent also may not use deception to obtain information from the user of a social networking website. See id. Rule 5.3(b)(1) ("A lawyer shall be responsible for conduct of a nonlawyer employed or retained by or associated with the lawyer that would be a violation of these Rules if engaged in by a lawyer, if . . . the lawyer orders or directs the specific conduct or, with knowledge of the specific conduct, ratifies it . . . .").

We are aware of ethics opinions that find that deception may be permissible in rare instances when it appears that no other option is available to obtain key evidence. See N.Y. County 737 (2007) (requiring, for use of dissemblance, that "the evidence sought is not reasonably and readily obtainable through other lawful means"); see also ABCNY Formal Op. 2003-02 (justifying limited use of undisclosed taping of telephone conversations to achieve a greater societal good where evidence would not otherwise be available if lawyer disclosed taping). Whatever the utility and ethical grounding of these limited exceptions -- a question we do not address here -- they are, at least in

most situations, inapplicable to social networking websites. Because 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 cannot be justified as a necessary last resort.[5] 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 the information from a witness on-line.[6]

Accordingly, a lawyer may not use deception to access information from a social networking webpage. Rather, a lawyer should rely on the informal and formal discovery procedures sanctioned by the ethical rules and case law to obtain relevant evidence.

September 2010

[5] Although a question of law beyond the scope of our reach, the Stored Communications Act, 18 U.S.C. § 2701(a)(1) et seq. and the Electronic Communications Privacy Act, 18 U.S.C. § 2510 et seq., among others, raise questions as to whether certain information is discoverable directly from third-party service providers such as Facebook. Counsel, of course, must ensure that her contemplated discovery comports with applicable law.

[6] While we recognize the importance of informal discovery, we believe a lawyer or her agent crosses an ethical line when she falsely identifies herself in a "friend request". See, e.g., Niesig v. Team I, 76 N.Y.2d 363, 376, 559 N.Y.S.2d 493, 499 (1990) (permitting ex parte communications with certain employees); Muriel Siebert, 8 N.Y.3d at 511, 836 N.Y.S.2d at 530 ("[T]he importance of informal discovery underlie[s] our holding here that, so long as measures are taken to steer clear of privileged or confidential information, adversary counsel may conduct ex parte interviews of an opposing party's former employee.").