



2015 CLM Annual Conference

Palm Desert

**Advanced Issues in Dealing with Social Media:  
Ethical Concerns and Admissibility Pitfalls  
Handout 1**

**Presenters:** David Brown, *Huie Fernambucq & Stewart LLP*  
Stephen Henning, *Wood Smith Henning & Berman LLP*  
Phyllis Modlin, *Markel Service, Incorporated*

**FORMAL OPINION NO. 2013-189**

**Accessing Information about Third Parties Through a Social  
Networking Website**

**Facts:** Lawyer wishes to investigate an opposing party, a witness, or a juror by accessing the person's social networking website. While viewing the publicly available information on the website, Lawyer learns that there is additional information that the person has kept from public view through privacy settings and that is available by submitting a request through the person's website.

**Questions:**

1. May Lawyer review a person's publicly available information on a social networking website?
2. May Lawyer, or an agent on behalf of Lawyer, request access to a person's non-public information?
3. May Lawyer, or an agent on behalf of Lawyer, use a computer username or other alias that does not identify Lawyer when requesting permission from the account holder to view non-public information?

**Conclusions:**

1. Yes.
2. Yes, qualified.
3. No, qualified.

**Discussion:**

1. Lawyer may access publicly available information on a social networking website.<sup>1</sup>

Oregon RPC 4.2 provides:

In representing a client or the lawyer's own interests, a lawyer shall not communicate or cause another to communicate on the subject of the representation with a person the lawyer knows to be represented by a lawyer on that subject unless:

- (a) the lawyer has the prior consent of a lawyer representing such other person;
- (b) the lawyer is authorized by law or by court order to do so; or
- (c) a written agreement requires a written notice or demand to be sent to such other person, in which case a copy of such notice or demand shall also be sent to such other person's lawyer.

Accessing the publicly available information on a person's social networking website is not a "communication" prohibited by Oregon RPC 4.2. OSB Formal Ethics Op No 2005-164 discusses the propriety of a lawyer accessing the public portions of an adversary's website and concludes that doing so is not "communicating" with the site owner within the meaning of Oregon RPC 4.2. The Opinion compared accessing a website to reading a magazine article or purchasing a book written by an adversary. The same analysis applies to publicly available information on a person's social networking webpages.<sup>2</sup>

---

<sup>1</sup> Although Facebook, MySpace, and Twitter are current popular social networking websites, this opinion is meant to apply to any similar social networking websites.

<sup>2</sup> This analysis is not limited to adversaries in litigation or transactional matters; it applies to a lawyer who is accessing the publicly available information of any person. However, caution must be exercised with regard to jurors. Although a lawyer may review a juror's publicly available information on social networking websites, communication with jurors before, during, and after a proceeding is generally prohibited. Accordingly, a lawyer may not send a request to a juror to access non-public personal information on a social networking website, nor may a lawyer ask an agent to do so. *See* Oregon RPC 3.5(b) (prohibiting ex parte communications with a juror during the proceeding unless authorized to do so by law or court order); Oregon RPC 3.5(c) (prohibiting communication with a juror

**2. Lawyer may request access to non-public information if the person is not represented by counsel in that matter and no actual representation of disinterest is made by Lawyer.**

To access non-public information on a social networking website, a lawyer may need to make a specific request to the holder of the account.<sup>3</sup> Typically that is done by clicking a box on the public portion of a person's social networking website, which triggers an automated notification to the holder of the account asking whether he or she would like to accept the request. Absent actual knowledge that the person is represented by counsel, a direct request for access to the person's non-public personal information is permissible. OSB Formal Ethics Op No 2005-164.<sup>4</sup>

In doing so, however, Lawyer must be mindful of Oregon RPC 4.3, which regulates communications with unrepresented persons. Oregon RPC 4.3 provides, in pertinent part:

In dealing on behalf of a client or the lawyer's own interests with a person who is not represented by counsel, a lawyer shall not state or imply that the lawyer is disinterested. When the lawyer knows or reasonably should know that the unrepresented person misunderstands the lawyer's role in the matter, the lawyer shall make reasonable efforts to correct the misunderstanding.

---

The purpose of the rule is to avoid the possibility that a nonlawyer will believe lawyers "carry special authority" and that a nonlawyer will be "inappropriately deferential" to someone else's after discharge if (1) the communication is prohibited by law or court order; (2) the juror has made known to the lawyer a desire not to communicate; or (3) the communication involves misrepresentation, coercion, duress, or harassment); Oregon RPC 8.4(a)(4) (prohibiting conduct prejudicial to the administration of justice). *See, generally*, §61:808, ABA/BNA Lawyers' Manual on Professional Conduct and cases cited therein.

<sup>3</sup> This is sometimes called "friending," although it may go by different names on different services, including "following" and "subscribing."

<sup>4</sup> *See, e.g.*, New York City Bar Formal Opinion 2010-2, which concludes that a lawyer "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 . . . ."

## Formal Opinion No. 2013-189

---

lawyer. *Apple Corps Ltd. v. International Collectors Soc.*, 15 F Supp2d 456 (DNJ 1998) (finding no violation of New Jersey RPC 4.3 by lawyers and lawyers' investigators posing as customers to monitor compliance with a consent order).<sup>5</sup> A simple request to access non-public information does not imply that Lawyer is "disinterested" in the pending legal matter. On the contrary, it suggests that Lawyer is interested in the person's social networking information, although for an unidentified purpose.

Similarly, Lawyer's request for access to non-public information does not in and of itself make a representation about the Lawyer's role. In the context of social networking websites, the holder of the account has full control over who views the information available on his or her pages. The holder of the account may allow access to his or her social network to the general public or may decide to place some, or all, of that information behind "privacy settings," which restrict who has access to that information. The account holder can accept or reject requests for access. Accordingly, the holder's failure to inquire further about the identity or purpose of unknown access requestors is not the equivalent of misunderstanding Lawyer's role in the matter.<sup>6</sup> By contrast, if the holder of the account asks for additional information to identify Lawyer, or if Lawyer has some other reason to believe that the person misunderstands her role, Lawyer must provide the additional information or withdraw the request.

---

<sup>5</sup> See also ABA Model Rule 4.3, Cmt. [1] ("An unrepresented person, particularly one not experienced in dealing with legal matters, might assume that a lawyer is disinterested in loyalties or is a disinterested authority on the law even when the lawyer represents a client."). Cf. *In re Gatti*, 330 Or 517, 8 P3d 966 (2000), in which the court declined to find an "investigatory exception" and disciplined a lawyer who used false identities to investigate an alleged insurance scheme. ORPC 8.4(b), discussed *infra*, was adopted to address concerns about the *Gatti* decision.

<sup>6</sup> Cf. *Murphy v. Perger* [2007] O.J. No. 5511, (S.C.J.) (Ontario, Canada) (requiring personal injury plaintiff to produce contents of Facebook pages, noting that "[t]he plaintiff could not have a serious expectation of privacy given that 366 people have been granted access to the private site.")

If Lawyer has actual knowledge that the holder of the account is represented by counsel on the subject of the matter, Oregon RPC 4.2 prohibits Lawyer from making the request except through the person's counsel or with the counsel's prior consent.<sup>7</sup> See OSB Formal Ethics Op No 2005-80 (discussing the extent to which certain employees of organizations are deemed represented for purposes of Oregon RPC 4.2).

**3. Lawyer may not advise or supervise the use of deception in obtaining access to nonpublic information unless Oregon RPC 8.4(b) applies.**

Oregon RPC 8.4(a)(3) prohibits a lawyer from engaging in “conduct involving dishonesty, fraud, deceit or misrepresentation that reflects adversely on the lawyer’s fitness to practice law.”<sup>8</sup> See also Oregon RPC 4.1(a) (prohibiting a lawyer from knowingly making a false statement of material fact to a third person in the course of representing a client). Accordingly, Lawyer may not engage in subterfuge designed to shield Lawyer’s identity from the person when making the request.<sup>9</sup>

As an exception to Oregon RPC 8.4(a)(3), Oregon RPC 8.4(b) allows a lawyer “to advise clients and others about or to supervise lawful covert activity in the investigation of violations of civil or criminal law or constitutional rights, provided the lawyer’s conduct is otherwise in compliance with these Rules of Professional Conduct.” For purposes of the rule “covert activity” means:

[A]n effort to obtain information on unlawful activity through the use of misrepresentations or other subterfuge. “Covert activity” may be commenced by a lawyer or involve a lawyer as an advisor or

---

<sup>7</sup> *In re Newell*, 348 Or 396, 409, 234 P3d 967 (2010) (reprimanding lawyer who communicated on "subject of the representation").

<sup>8</sup> See *In re Carpenter*, 337 Or 226, 95 P3d 203 (2004) (lawyer received public reprimand after assuming false identity on social media website).

<sup>9</sup> See Oregon RPC 8.4(a), which prohibits a lawyer from violating the RPCs, from assisting or inducing another to do so, or from violating the RPCs “through the acts of another”).

**Formal Opinion No. 2013-189**

---

supervisor only when the lawyer in good faith believes there is a reasonable possibility that unlawful activity has taken place, is taking place or will take place in the foreseeable future.

In the limited instances allowed by Oregon RPC 8.4(b) (more fully explicated in OSB Formal Ethics Op No 2005-173), Lawyer may advise or supervise another's deception to access a person's nonpublic information on a social networking website.

**Approved by Board of Governors, February 2013.**



2015 CLM Annual Conference

Palm Desert

**Advanced Issues in Dealing with Social Media:  
Ethical Concerns and Admissibility Pitfalls  
Handout 2**

**Presenters:** David Brown, *Huie Fernambucq & Stewart LLP*  
Stephen Henning, *Wood Smith Henning & Berman LLP*  
Phyllis Modlin, *Markel Service, Incorporated*

**The Association of the Bar of the City of New York Committee on Professional Ethics**

**Formal Opinion 2012-2:  
JURY RESEARCH AND SOCIAL MEDIA**

**TOPIC:** Jury Research and Social Media

**DIGEST:** Attorneys may use social media websites for juror research as long as no communication occurs between the lawyer and the juror as a result of the research. Attorneys may not research jurors if the result of the research is that the juror will receive a communication. If an attorney unknowingly or inadvertently causes a communication with a juror, such conduct may run afoul of the Rules of Professional Conduct. The attorney must not use deception to gain access to a juror's website or to obtain information, and third parties working for the benefit of or on behalf of an attorney must comport with all the same restrictions as the attorney. Should a lawyer learn of juror misconduct through otherwise permissible research of a juror's social media activities, the lawyer must reveal the improper conduct to the court.

**RULES:** 3.5(a)(4); 3.5(a)(5); 3.5(d); 8.4

**Question:** What ethical restrictions, if any, apply to an attorney's use of social media websites to research potential or sitting jurors?

**OPINION**

**I. Introduction**

*Ex parte* attorney communication with prospective jurors and members of a sitting jury has long been prohibited by state rules of professional conduct (*see* American Bar Association Formal Opinion 319 ("ABA 319")), and attorneys have long sought ways to gather information about potential jurors during voir dire (and perhaps during trial) within these proscribed bounds. However, as the internet and social media have changed the ways in which we all communicate, conducting juror research while complying with the rule

prohibiting juror communication has become more complicated.

In addition, the internet appears to have increased the opportunity for juror misconduct, and attorneys are responding by researching not only members of the venire but sitting jurors as well. Juror misconduct over the internet is problematic and has even led to mistrials. Jurors have begun to use social media services as a platform to communicate about a trial, during the trial (see *WSJ Law Blog* (March 12, 2012), <http://blogs.wsj.com/law/2012/03/12/jury-files-the-temptation-of-twitter/>), and jurors also turn to the internet to conduct their own out of court research. For example, the Vermont Supreme Court recently overturned a child sexual assault conviction because a juror conducted his own research on the cultural significance of the alleged crime in Somali Bantu culture. *State v. Abdi*, No. 2012-255, 2012 WL 231555 (Vt. Jan. 26, 2012). In a case in Arkansas, a murder conviction was overturned because a juror tweeted during the trial, and in a Maryland corruption trial in 2009, jurors used Facebook to discuss their views of the case before deliberations. (*Juror's Tweets Upend Trials*, Wall Street Journal, March 2, 2012.) Courts have responded in various ways to this problem. Some judges have held jurors in contempt or declared mistrials (see *id.*) and other courts now include jury instructions on juror use of the internet. (See New York Pattern Jury Instructions, Section III, *infra.*) However, 79% of judges who responded to a Federal Judicial Center survey admitted that “they had no way of knowing whether jurors had violated a social-media ban.” (*Juror's Tweets*, *supra.*) In this context, attorneys have also taken it upon themselves to monitor jurors throughout a trial.

Just as the internet and social media appear to facilitate juror misconduct, the same tools have expanded an attorney’s ability to conduct research on potential and sitting jurors, and clients now often expect that attorneys will conduct such research. Indeed, standards of competence and diligence may require doing everything reasonably possible to learn about the jurors who will sit in judgment on a case. However, social media services and websites can blur the line between independent, private research and interactive, interpersonal “communication.” Currently, there are no clear rules for conscientious attorneys to follow in order to both diligently represent their clients and to abide by applicable ethical obligations. This opinion applies the New York Rules of Professional Conduct (the “Rules”), specifically Rule 3.5, to juror research in the internet context, and particularly to research using social networking services and websites.<sup>1</sup>

The Committee believes that the principal interpretive issue is what constitutes a “communication” under Rule 3.5. We conclude that if a juror were to (i) receive a “friend” request (or similar invitation to share information on a social network site) as a result of an attorney’s research, or (ii) otherwise to learn of the attorney’s viewing or attempted viewing of the juror’s pages, posts, or comments, that *would* constitute a prohibited communication if the attorney was aware that her actions would cause the juror to receive such message or notification. We further conclude that the same attempts to research the juror *might* constitute a prohibited communication even if inadvertent or unintended. In addition, the attorney must not use deception—such as pretending to be someone else—to gain access to information about a juror that would otherwise be unavailable. Third parties working for the benefit of or on behalf of an attorney must comport with these same restrictions (as it is always unethical pursuant to Rule 8.4 for an attorney to attempt to avoid the Rule by having a non-lawyer do what she cannot). Finally, if a lawyer learns of juror misconduct through a juror’s social media activities, the lawyer must promptly reveal the improper conduct to the court



## II. Analysis Of Ethical Issues Relevant To Juror Research

### A. Prior Authority Regarding An Attorney's Ability To Conduct Juror Research Over Social Networking Websites

Prior ethics and judicial opinions provide some guidance as to what is permitted and prohibited in social media juror research. First, it should be noted that lawyers have long tried to learn as much as possible about potential jurors using various methods of information gathering permitted by courts, including checking and verifying voir dire answers. Lawyers have even been chastised for *not* conducting such research on potential jurors. For example, in a recent Missouri case, a juror failed to disclose her prior litigation history in response to a voir dire question. After a verdict was rendered, plaintiff's counsel investigated the juror's civil litigation history using Missouri's automated case record service and found that the juror had failed to disclose that she was previously a defendant in several debt collection cases and a personal injury action.<sup>2</sup> Although the court upheld plaintiff's request for a new trial based on juror nondisclosure, the court noted that "in light of advances in technology allowing greater access to information that can inform a trial court about the past litigation history of venire members, it is appropriate to place a greater burden on the parties to bring such matters to the court's attention at an earlier stage." *Johnson v. McCullough*, 306 S.W.3d 551, 558-59 (Mo. 2010). The court also stated that "litigants should endeavor to prevent retrials by completing an early investigation." *Id.* at 559.

Similarly, the Superior Court of New Jersey recently held that a trial judge "acted unreasonably" by preventing plaintiff's counsel from using the internet to research potential jurors during voir dire. During jury selection in a medical malpractice case, plaintiff's counsel began using a laptop computer to obtain information on prospective jurors. Defense counsel objected, and the trial judge held that plaintiff's attorney could not use her laptop during jury selection because she gave no notice of her intent to conduct internet research during selection. Although the Superior Court found that the trial court's ruling was not prejudicial, the Superior Court stated that "there was no suggestion that counsel's use of the computer was in any way disruptive. That he had the foresight to bring his laptop computer to court, and defense counsel did not, simply cannot serve as a basis for judicial intervention in the name of 'fairness' or maintaining 'a level playing field.' The 'playing field' was, in fact, already 'level' because internet access was open to both counsel." *Carino v. Muenzen*, A-5491-08T1, 2010 N.J. Super. Unpub. LEXIS 2154, at \*27 (N.J. Sup. Ct. App. Div. Aug. 30, 2010).<sup>3</sup>

Other recent ethics opinions have also generally discussed attorney research in the social media context. For example, San Diego County Bar Legal Ethics Opinion 2011-2 ("SDCBA 2011-2") examined whether an attorney can send a "friend request" to a represented party. SDCBA 2011-2 found that because an attorney must make a decision to "friend" a party, even if the "friend request [is] nominally generated by Facebook and not the attorney, [the request] is at least an indirect communication" and is therefore *prohibited* by the rule against *ex parte*

communications with represented parties.<sup>4</sup> In addition, the New York State Bar Association (“NYSBA”) found that obtaining information from an adverse party’s social networking personal webpage, which is accessible to all website users, “is similar to obtaining information that is available in publicly accessible online or print media, or through a subscription research service as Niexi or Factiva and that is plainly *permitted*.” (NYSBA Opinion 843 at 2) (emphasis added).

And most recently, the New York County Lawyers’ Association (“NYCLA”) published a formal opinion on the ethics of conducting juror research using social media. NYCLA Formal Opinion 743 (“NYCLA 743”) examined whether a lawyer may conduct juror research during voir dire and trial using Twitter, Facebook and other similar social networking sites. NYCLA 743 found that it is “proper and ethical under Rule 3.5 for a lawyer to undertake a pretrial search of a prospective juror’s social networking site, provided there is no contact or communication with the prospective juror and the lawyer does not seek to ‘friend’ jurors, subscribe to their Twitter accounts, send jurors tweets or otherwise contact them. During the evidentiary or deliberation phases of a trial, a lawyer may visit the publicly available Twitter, Facebook or other social networking site of a juror but must not ‘friend’ the juror, email, send tweets or otherwise communicate in any way with the juror or act in any way by which the juror becomes aware of the monitoring.” (NYCLA 743 at 4.) The opinion further noted the importance of reporting to the court any juror misconduct uncovered by such research and found that an attorney must notify the court of any impropriety “before taking any further significant action in the case.” *Id.* NYCLA concluded that attorneys cannot use knowledge of juror misconduct to their advantage but rather must notify the court.

As set forth below, we largely agree with our colleagues at NYCLA. However, despite the guidance of the opinions discussed above, the question at the core of applying Rule 3.5 to social media—what constitutes a communication— has not been specifically addressed, and the Committee therefore analyzes this question below.

## **B. An Attorney May Conduct Juror Research Using Social Media Services And Websites But Cannot Engage In Communication With A Juror**

### **1. Discussion of Features of Various Potential Research Websites**

Given the popularity and widespread usage of social media services, other websites and general search engines, it has become common for lawyers to use the internet as a tool to research members of the jury venire in preparation for jury selection as well as to monitor jurors throughout the trial. Whether research conducted through a particular service will constitute a prohibited communication under the Rules may depend in part on, among other things, the technology, privacy settings and mechanics of each service.

The use of search engines for research is already ubiquitous. As social media services have grown in popularity, they have become additional sources to research potential jurors. As we discuss below, the central question an attorney must answer before engaging in jury research on a particular site or using a particular service is whether her actions will cause the juror to learn of the research. However, the functionality, policies and features of social media services change often, and any description of a particular website may well become obsolete quickly. Rather than attempt to catalog all existing social media services and their ever-changing offerings, policies and limitations, the Committee adopts a functional definition.<sup>5</sup>

We understand “social media” to be services or websites people join voluntarily in order to interact, communicate, or stay in touch with a group of users, sometimes called a “network.” Most such services allow users to create personal profiles, and some allow users to post pictures and messages about their daily lives. Professional networking sites have also become popular. The amount of information that users can view about each other depends on the particular service and also each user’s chosen privacy settings. The information the service communicates or makes available to visitors as well as members also varies. Indeed, some services may automatically notify a user when her profile has been viewed, while others provide notification only if another user initiates an interaction. Because of the differences from service to service and the high rate of change, the Committee believes that it is an attorney’s duty to research and understand the properties of the service or website she wishes to use for jury research in order to avoid inadvertent communications.

## 2. What Constitutes a “Communication”?

Any research conducted by an attorney into a juror or member of the venire’s background or behavior is governed in part by Rule 3.5(a)(4), which states: “a lawyer shall not . . . (4) communicate or cause another to communicate with a member of the jury venire from which the jury will be selected for the trial of a case or, during the trial of a case, with any member of the jury unless authorized to do so by law or court order.” The Rule does not contain a *mens rea* requirement; by its literal terms, it prohibits *all* communication, even if inadvertent. Because of this, the application of Rule 3.5(a)(4) to juror research conducted over the internet via social media services is potentially more complicated than traditional juror communication issues. Even though the attorney’s purpose may not be to communicate with a juror, but simply to gather information, social media services are often designed for the very purpose of communication, and automatic features or user settings may cause a “communication” to occur even if the attorney does intend not for one to happen or know that one may happen. This raises several ethical questions: is every visit to a juror’s social media website considered a communication? Should the intent to research, not to communicate, be the controlling factor? What are the consequences of an inadvertent or unintended communications? The Committee begins its analysis by considering the meaning of “communicate” and “communication,” which are not defined either in the Rule or the American Bar Association Model Rules.<sup>6</sup>

Black’s Law Dictionary (9th Ed.) defines “communication” as: “1. The expression or exchange of information by speech, writing, gestures, or conduct; the process of bringing an idea to another’s perception. 2. The information so expressed or exchanged.” The Oxford English Dictionary defines “communicate” as: “To impart (information, knowledge, or the like) (to a person; also formerly with); to impart the knowledge or idea of (something), to inform a person of; to convey, express; to give an impression of, put across.” Similarly, Local Rule 26.3 of the United States District Courts for the Southern and Eastern Districts of New York defines “communication” (for the purposes of discovery requests) as: “the transmittal of information (in the form of facts, ideas, inquiries or otherwise).”

Under the above definitions, whether the communicator intends to “impart” a message or knowledge is seemingly irrelevant; the focus is on the effect on the receiver. It is the “transmission of,” “exchange of” or “process of bringing” information or ideas from one

person to another that defines a communication. In the realm of social media, this focus on the transmission of information or knowledge is critical. A request or notification transmitted through a social media service may constitute a communication even if it is technically generated by the service rather than the attorney, is not accepted, is ignored, or consists of nothing more than an automated message of which the “sender” was unaware. In each case, at a minimum, the researcher imparted to the person being researched the knowledge that he or she is being investigated.

### 3. An Attorney May Research A Juror Through Social Media Websites As Long As No Communication Occurs

The Committee concludes that attorneys may use search engines and social media services to research potential and sitting jurors without violating the Rules, as long as no communication with the juror occurs. The Committee notes that Rule 3.5(a)(4) does not impose a requirement that a communication be willful or made with knowledge to be prohibited. In the social media context, due to the nature of the services, unintentional communications with a member of the jury venire or the jury pose a particular risk. For example, if an attorney views a juror’s social media page and the juror receives an automated message from the social media service that a potential contact has viewed her profile—even if the attorney has not requested the sending of that message or is entirely unaware of it—the attorney has arguably “communicated” with the juror. The transmission of the information that the attorney viewed the juror’s page is a communication that may be attributable to the lawyer, and even such minimal contact raises the specter of the improper influence and/or intimidation that the Rules are intended to prevent. Furthermore, attorneys cannot evade the ethics rules and avoid improper influence simply by having a non-attorney with a name unrecognizable to the juror initiate communication, as such action will run afoul of Rule 8.4 as discussed in Section II(C), *infra*.

Although the text of Rule 3.5(a)(4) would appear to make any “communication”—even one made inadvertently or unknowingly—a violation, the Committee takes no position on whether such an inadvertent communication would in fact be a violation of the Rules. Rather, the Committee believes it is incumbent upon the attorney to understand the functionality of any social media service she intends to use for juror research. If an attorney cannot ascertain the functionality of a website, the attorney must proceed with great caution in conducting research on that particular site, and should keep in mind the possibility that even an accidental, automated notice to the juror could be considered a violation of Rule 3.5.

More specifically, and based on the Committee's current understanding of relevant services, search engine websites may be used freely for juror research because there are no interactive functions that could allow jurors to learn of the attorney's research or actions. However, other services may be more difficult to navigate depending on their functionality and each user's particular privacy settings. Therefore, attorneys may be able to do some research on certain sites but cannot use all aspects of the sites' social functionality. An attorney may not, for example, send a chat, message or "friend request" to a member of the jury or venire, or take any other action that will transmit information to the juror because, if the potential juror learns that the attorney seeks access to her personal information then she has received a communication. Similarly, an attorney may read any publicly-available postings of the juror but must not sign up to receive new postings as they are generated. Finally, research using services that may, even unbeknownst to the attorney, generate a message or allow a person to determine that their webpage has been visited may pose an ethical risk even if the attorney did not intend or know that such a "communication" would be generated by the website.

The Committee also emphasizes that the above applications of Rule 3.5 are meant as examples only. The technology, usage and privacy settings of various services will likely change, potentially dramatically, over time. The settings and policies may also be partially under the control of the person being researched, and may not be apparent, or even capable of being ascertained. In order to comply with the Rules, an attorney must therefore be aware of how the relevant social media service works, and of the limitations of her knowledge. It is the duty of the attorney to understand the functionality and privacy settings of any service she wishes to utilize for research, and to be aware of any changes in the platforms' settings or policies to ensure that no communication is received by a juror or venire member.

### **C. An Attorney May Not Engage in Deception or Misrepresentation In Researching Jurors On Social Media Websites**

Rule 8.4(c), which governs all attorney conduct, prohibits deception and misrepresentation.<sup>7</sup> In the jury research context, this rule prohibits attorneys from, for instance, misrepresenting their identity during online communications in order to access otherwise unavailable information, including misrepresenting the attorney's associations or membership in a network or group in order to access a juror's information. Thus, for example, an attorney may not claim to be an alumnus of a school that she did not attend in order to view a juror's personal webpage that is accessible only to members of a certain alumni network.

Furthermore, an attorney may not use a third party to do what she could not otherwise do. Rule 8.4(a) prohibits an attorney from violating *any* Rule "through the acts of another." Using a third party to communicate with a juror is deception and violates Rule 8.4(c), as well as Rule 8.4(a), even if the third party provides the potential juror only with truthful information. The attorney violates both rules whether she instructs the third party to communicate via a social network or whether the third party takes it upon herself to communicate with a member of the jury or venire for the attorney's benefit. On this issue, the Philadelphia Bar Association Professional Guidance Committee Opinion 2009-02 ("PBA 2009-02") concluded that if an attorney uses a third party to "friend" a witness in order to access information, she is guilty of deception because "[this action] omits a highly material fact, namely, that the third party who asks to be allowed access to the witness' pages is doing so only because she is intent on obtaining information and sharing it with a lawyer for

use in a lawsuit.” (PBA 2009-02 at 3.) New York City Bar Association Formal Opinion 2010-2 similarly held that a lawyer may not gain access to a social networking website under false pretenses, either directly or through an agent, and NYCLA 743 also noted that Rule 8.4 governs juror research and an attorney therefore cannot use deception to gain access to a network or direct anyone else to “friend” an adverse party. (NYCLA 743 at 2.) We agree with these conclusions; attorneys *may not* shift their conduct or assignments to non-attorneys in order to evade the Rules.

#### **D. The Impact On Jury Service Of Attorney Use Of Social Media Websites For Research**

Although the Committee concludes that attorneys may conduct jury research using social media websites as long as no “communication” occurs, the Committee notes the potential impact of jury research on potential jurors’ perception of jury service. It is conceivable that even jurors who understand that many of their social networking posts and pages are public may be discouraged from jury service by the knowledge that attorneys and judges can and will conduct active research on them or learn of their online—albeit public—social lives. The policy considerations implicit in this possibility should inform our understanding of the applicable Rules.

In general, attorneys should only view information that potential jurors intend to be—and make—public. Viewing a public posting, for example, is similar to searching newspapers for letters or columns written by potential jurors because in both cases the author intends the writing to be for public consumption. The potential juror is aware that her information and images are available for public consumption. The Committee notes that some potential jurors may be unsophisticated in terms of setting their privacy modes or other website functionality, or may otherwise misunderstand when information they post is publicly available. However, in the Committee’s view, neither Rule 3.5 nor Rule 8.4(c) prohibit attorneys from viewing public information that a juror might be unaware is publicly available, except in the rare instance where it is clear that the juror intended the information to be private. Just as the attorney must monitor technological updates and understand websites that she uses for research, the Committee believes that jurors have a responsibility to take adequate precautions to protect any information they intend to be private.

#### **E. Conducting On-Going Research During Trial**

Rule 3.5 applies equally with respect to a jury venire and empanelled juries. Research permitted as to potential jurors is permitted as to sitting jurors. Although there is, in light of the discussion in Section III, *infra*, great benefit that can be derived from detecting instances when jurors are not following a court’s instructions for behavior while empanelled, researching jurors mid-trial is not without risk. For instance, while an inadvertent communication with a venire member may result in an embarrassing revelation to a court and a disqualified panelist, a communication with a juror during trial can cause a mistrial. The Committee therefore re-emphasizes that it is the attorney’s duty to understand the functionality of any social media service she chooses to utilize and to act with the utmost caution.

### **III. An Attorney Must Reveal Improper Juror Conduct to the Court**

Rule 3.5(d) provides: “a lawyer shall reveal promptly to the court improper conduct by a member of the venire or a juror, or by another toward a member of the venire or a juror or a

member of her family of which the lawyer has knowledge.” Although the Committee concludes that an attorney may conduct jury research on social media websites as long as “communication” is avoided, if an attorney learns of juror misconduct through such research, she *must* promptly<sup>8</sup> notify the court. Attorneys must use their best judgment and good faith in determining whether a juror has acted improperly; the attorney cannot consider whether the juror’s improper conduct benefits the attorney.<sup>9</sup>

On this issue, the Committee notes that New York Pattern Jury Instructions (“PJI”) now include suggested jury charges that expressly prohibit *juror* use of the internet to discuss or research the case. PJI 1:11 Discussion with Others - Independent Research states: “please do not discuss this case either among yourselves or with anyone else during the course of the trial. . . . It is important to remember that you may not use any internet service, such as Google, Facebook, Twitter or any others to individually or collectively research topics concerning the trial . . . For now, be careful to remember these rules whenever you use a computer or other personal electronic device during the time you are serving as juror but you are not in the courtroom.” Moreover, PJI 1:10 states, in part, “in addition, please do not attempt to view the scene by using computer programs such as Goggle Earth. Viewing the scene either in person or through a computer program would be unfair to the parties . . . .” New York criminal courts also instruct jurors that they may not converse among themselves or with anyone else upon any subject connected with the trial. NY Crim. Pro. §270.40 (McKinney’s 2002).

The law requires jurors to comply with the judge’s charge<sup>10</sup> and courts are increasingly called upon to determine whether jurors’ social media postings require a new trial. *See, e.g., Smead v. CL Financial Corp.*, No. 06CC11633, 2010 WL 6562541 (Cal. Super. Ct. Sept. 15, 2010) (holding that juror’s posts regarding length of trial were not prejudicial and denying motion for new trial). However, determining whether a juror’s conduct is *misconduct* may be difficult in the realm of social media. Although a post or tweet on the subject of the trial, even if unanswered, can be considered a “conversation,” it may not always be obvious whether a particular post is “connected with” the trial. Moreover, a juror may be permitted to post a comment “about the fact [of] service on jury duty.”<sup>11</sup>

#### **IV. Post-Trial**

In contrast to Rule 3.4(a)(4), Rule 3.5(a)(5) allows attorneys to communicate with a juror after discharge of the jury. After the jury is discharged, attorneys may contact jurors and communicate, including through social media, unless “(i) the communication is prohibited by law or court order; (ii) the juror has made known to the lawyer a desire not



to communicate; (iii) the communication involves misrepresentation, coercion, duress or harassment; or (iv) the communication is an attempt to influence the juror's actions in future jury service.” Rule 3.5(a)(5). For instance, NYSBA Opinion 246 found that “lawyers may communicate with jurors concerning the verdict and case.” (NYSBA 246 (interpreting former EC 7-28; DR 7-108(D).) The Committee concludes that this rule should also permit communication via social media services after the jury is discharged, but the attorney must, of course, comply with all ethical obligations in any communication with a juror after the discharge of the jury. However, the Committee notes that “it [is] unethical for a lawyer to harass, entice, or induce or exert influence on a juror” to obtain information or her testimony to support a motion for a new trial. (ABA 319.)

## V. Conclusion

The Committee concludes that an attorney may research potential or sitting jurors using social media services or websites, provided that a communication with the juror does not occur. “Communication,” in this context, should be understood broadly, and includes not only sending a specific message, but also any notification to the person being researched that they have been the subject of an attorney’s research efforts. Even if the attorney does not intend for or know that a communication will occur, the resulting inadvertent communication may still violate the Rule. In order to apply this rule to social media websites, attorneys must be mindful of the fact that a communication is *the process of bringing an idea, information or knowledge to another’s perception*—including the fact that they have been researched. In the context of researching jurors using social media services, an attorney must understand and analyze the relevant technology, privacy settings and policies of each social media service used for jury research. The attorney must also avoid engaging in deception or misrepresentation in conducting such research, and may not use third parties to do that which the lawyer cannot. Finally, although attorneys may communicate with jurors after discharge of the jury in the circumstances outlined in the Rules, the attorney must be sure to comply with all other ethical rules in making any such communication.

---

1. Rule 3.5(a)(4) states: “a lawyer shall not . . . (4) communicate or cause another to communicate with a member of the jury venire from which the jury will be selected for the trial of a case or, during the trial of a case, with any member of the jury unless authorized to do so by law or court order.”

2. Missouri Rule of Professional Conduct 3.5 states: “A lawyer shall not: (a) seek to influence a judge, juror, prospective juror, or other official by means prohibited by law; (b) communicate *ex parte* with such a person during the proceeding unless authorized to do so by law or court order.”



3. The Committee also notes that the United States Attorney for the District of Maryland recently requested that a court prohibit attorneys for all parties in a criminal case from conducting juror research using social media, arguing that “if the parties were permitted to conduct additional research on the prospective jurors by using social media or any other outside sources prior to the in court voir dire, the Court’s supervisory control over the jury selection process would, as a practical matter, be obliterated.” (Aug. 30, 2011 letter from R. Rosenstein to Hon. Richard Bennet.) The Committee is unable to determine the court’s ruling from the public file.

4. California Rule of Profession Conduct 2-100 states, in part: “(A) While representing a client, a member shall not communicate directly or indirectly about the subject of the representation with a party the member knows to be represented by another lawyer in the matter, unless the member has the consent of the other lawyer.”

5. As of the date of this writing, May 2012, three of the most common social media services are Facebook, LinkedIn and Twitter.

6. Although the New York City Bar Association Formal Opinion 2010-2 (“NYCBA 2010-2”) and SDCBA 2011-2 (both addressing social media “communication” in the context of the “No Contact” rule) were helpful precedent for

the Committee's analysis, the Committee is unaware of any opinion setting forth a definition of "communicate" as that term is used in Rule 4.2 or any other ethics rule.

7. Rule 8.4 prohibits "conduct involving dishonesty, fraud, deceit or misrepresentation," and also states "a lawyer or law firm shall not: (a) violate or attempt to violate the Rules of Professional Conduct, knowingly assist or induce another to do so, or do so through the acts or another." (Rule 8.4(c),(a).)

8. New York City Bar Association Formal Opinion 2012-1 defined "promptly" to mean "as soon as reasonably possible."

9. Although the Committee is not opining on the obligations of jurors (which is beyond the Committee's purview), the Committee does note that if a juror contacts an attorney, the attorney must promptly notify the court under Rule 3.5(d).

10. *People v. Clarke*, 168 A.D.2d 686 (2d Dep't 1990) (holding that jurors must comply with the jury charge).

11. *US v. Fumo*, 639 F. Supp. 2d 544, 555 (E.D. Pa. 2009) *aff'd*, 655 F.3d 288 (3d Cir. 2011) ("[The juror's] comments on Twitter, Facebook, and her personal web page were innocuous, providing no indication about the trial of which he was a part, much less her thoughts on that trial. Her statements about the fact of her service on jury duty were not prohibited. Moreover, as this Court noted, her Twitter and Facebook postings were nothing more than harmless ramblings having no prejudicial effect. They were so vague as to be virtually meaningless. [Juror] raised no specific facts dealing with the trial, and nothing in these comments indicated any disposition toward anyone involved in the suit.") (internal citations omitted).

© The Association of the Bar of the City of New York



2015 CLM Annual Conference  
Palm Desert

**Advanced Issues in Dealing with Social Media:  
Ethical Concerns and Admissibility Pitfalls  
Handout 3**

**Presenters:** David Brown, *Huie Fernambucq & Stewart LLP*  
Stephen Henning, *Wood Smith Henning & Berman LLP*  
Phyllis Modlin, *Markel Service, Incorporated*



NEW YORK STATE BAR ASSOCIATION  
*Serving the legal profession and the community since 1876*

---

ETHICS OPINION 843

---

NEW YORK STATE BAR  
ASSOCIATION Committee on  
Professional Ethics

Opinion # 843 (09/10/2010)

**Topic:** Lawyer's access to public pages of another party's social networking site for the purpose of gathering information for client in pending litigation.

**Digest:** A lawyer representing a client in pending litigation may access the public pages of another party's social networking website (such as Facebook or MySpace) for the purpose of obtaining possible impeachment material for use in the litigation.

**Rules:** 4.1; 4.2; 4.3; 5.3(b)(1); 8.4(c)

**QUESTION**

1. May 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 that party for use in the lawsuit, including impeachment material, if the lawyer does not "friend" the party and instead relies on public pages posted by the party that are accessible to all members in the network?

**OPINION**

2. Social networking services such as Facebook and MySpace allow users to create an online profile that may be accessed by other network members. Facebook and MySpace are examples of external social networks that are available to all web users. An external social network may be generic (like MySpace and Facebook) or may be formed around a specific profession or area of interest. Users are able to upload pictures and create profiles of themselves. Users may also link with other users, which is called "friending." Typically, these social networks have privacy controls that allow users to choose who can view their profiles or contact them; both users must confirm that they wish to "friend" before they are linked and can view one another's profiles. However, some social networking sites and/or users do not require pre-approval to gain access to member profiles.

3. The question posed here has not been addressed previously by an ethics committee interpreting New York's Rules of Professional Conduct (the "Rules") or the former New York Lawyers Code of Professional Responsibility, but some guidance is available from outside New York. The Philadelphia Bar Association's Professional Guidance Committee recently analyzed the propriety of "friending" an unrepresented adverse witness in a pending lawsuit to obtain potential impeachment material. See Philadelphia Bar Op. 2009-02 (March 2009). In that opinion, a lawyer asked whether she could cause a third party to access the Facebook and MySpace pages maintained by a witness to obtain information that might be useful for impeaching the witness at trial. The witness's Facebook and MySpace pages were not generally accessible to the public, but rather were accessible only with the witness's permission (i.e., only when the witness allowed someone to "friend" her). The inquiring lawyer proposed to have the third party "friend" the witness to access the witness's Facebook and MySpace accounts and provide truthful information about the third party, but conceal the association with the lawyer and the real purpose behind "friending" the witness (obtaining potential impeachment material).

4. The Philadelphia Professional Guidance Committee, applying the Pennsylvania Rules of Professional Conduct, concluded that the inquiring lawyer could not ethically engage in the proposed conduct. The lawyer's intention to have a third party "friend" the unrepresented witness implicated Pennsylvania Rule 8.4(c) (which, like New York's Rule 8.4(c), prohibits a lawyer from engaging in conduct involving "dishonesty, fraud, deceit or misrepresentation"); Pennsylvania Rule 5.3(c)(1) (which, like New York's Rule 5.3(b)(1), holds a lawyer responsible for the conduct of a nonlawyer employed by the lawyer if the lawyer directs, or with knowledge ratifies, conduct that would violate the Rules if engaged in by the lawyer); and Pennsylvania Rule 4.1 (which, similar to New York's Rule 4.1, prohibits a lawyer from making a false statement of fact or law to a third person). Specifically, the Philadelphia Committee determined that the proposed "friending" by a third party would constitute deception in violation of Rules 8.4 and 4.1, and would constitute a supervisory violation under Rule 5.3 because the third party would omit a material fact (i.e., that the third party would be seeking access to the witness's social networking pages solely to obtain information for the lawyer to use in the pending lawsuit).

5. Herein contrast, the Facebook and MySpace sites the lawyer wishes to view are accessible to all members of the network. New York's Rule 8.4 would not be implicated because the lawyer is not engaging in deception by accessing a public website that is available to anyone in the network, provided that the lawyer does not employ deception in any other way (including, for example, employing deception to become a member of the network). Obtaining information about a party available in the Facebook or MySpace profile is similar to obtaining information that is available in publicly accessible online or print media, or through a subscription research service such as Nexis or Factiva, and that is plainly permitted.<sup>[1]</sup> Accordingly, we conclude that the lawyer may ethically view and access the Facebook and MySpace profiles of a party other than the lawyer's client in litigation as long as the party's profile is available to all members in the network and the lawyer neither "friends" the other party nor directs someone else to do so.

## CONCLUSION

6. A lawyer who represents a client in a pending litigation, and who has access to the Facebook or MySpace network used by another party in litigation, may access and review the public social network pages of that party to search for potential impeachment material. As 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), 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).

(76-09)

---

<sup>[1]</sup>One of several key distinctions between the scenario discussed in the Philadelphia opinion and this opinion is that the Philadelphia opinion concerned an unrepresented *witness*, whereas our opinion concerns a *party* - and this party may or may not be represented by counsel in the litigation. If a lawyer attempts to "friend" a *represented* party in a pending litigation, then the lawyer's conduct is governed by Rule 4.2 (the "no-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. If 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 if the other party's interests are likely to conflict with those of the lawyer's client. Our opinion does not address these scenarios.

© 2014 New York State Bar  
Association



2015 CLM Annual Conference  
Palm Desert

**Advanced Issues in Dealing with Social Media:  
Ethical Concerns and Admissibility Pitfalls**

**Presenters:** David Brown, *Huie Fernambucq & Stewart LLP*  
Stephen Henning, *Wood Smith Henning & Berman LLP*  
Phyllis Modlin, *Markel Service, Incorporated*

**The Association of the Bar of the City of New York Committee on Professional and Judicial 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, 5.3(b)(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.<sup>[1]</sup> 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.<sup>[2]</sup> 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.<sup>[3]</sup> The prevalence of these and other social networking websites, and the potential 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.<sup>[4]</sup> 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, 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 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.<sup>[5]</sup> 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.<sup>[6]</sup>

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.

---

<sup>1</sup>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).

[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).

[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.”).

© The Association of the Bar of the City of New York