As I stated in Parts 1 and 2 of this series, these posts are based on the day-long conference entitled Social Networking: Friends or Foes? (now on MP3) hosted by the Samuelson Law, Technology & Public Policy Clinic, the Berkeley Center for Law & Technology, the Berkeley Center for Criminal Justice and the UC Berkeley School of Law. The discussion addressed the legal and ethical issues facing lawyers and investigators using social networking contents in legal matters. In Part 1, I discussed the public's expectation of privacy of the information posted on social network sites. In Part 2, I focused on the underlying law that relates to obtaining social network information for use in investigations and prosecutions of criminal and civil cases. Today, I will address ethical considerations regarding current practices to obtain or obstruct use of this information.

Being a real estate and business lawyer, I must admit to a degree of naivete regarding criminal investigative practices, and I don't much watch TV. So my big "Aha" moment of the conference was when FBI Supervisory Special Agent Jack Bennett stated without equivocation that the FBI creates false Facebook and other social networking identities and "friends" or "pokes" suspects or potential witnesses as a matter of course to gain access to their accounts.

In their defense, the FBI investigates a whole slew of cybercrimes: identity theft, organized cybercrime, sexual predators, hackers and terrorists just to name a few. And the FBI does not have a whole set of rules called Legal Ethics to abide by. The same cannot be said for lawyers investigating their cases.

So the question is, how far can a lawyer go in these investigative tactics? Is employing someone to "friend" a potential witness that different from hiring a private investigator to videotape a worker's compensation claimant? Does an attorney who advises a client to shut down his Facebook account obstruct justice? Is that different from advising a client not to talk to anyone about the case? What do you do when a client tells you there is evidence on a social networking site that could corroborate his story? Or impeach a witness? Do you get it any way you can? Would you be committing malpractice if you didn't?

Just as we've seen that there are no clear legal boundaries with respect to privacy, so a lawyer's ethical conduct in these circumstances is undefined. However, opinions are beginning to appear. The first is the opinion of the Philadelphia Bar Associations' Professional Guidance Committee, stating that a lawyer who hired a third party to "friend" a witness on Facebook and MySpace to gain access to personal files would violate Rules 8.4, which prohibits dishonesty, fraud, deceit or misrepresentation, and 4.1 regarding truthfulness in statements to others, of the Pennsylvania Rules of Professional Conduct.

However, in his very insightful and well-researched article, Evidence on Social Networking Sites, Ken Strutin cites the following exception to Pennsylvania's analysis in Opinion 737 of the New York County lawyers' Association's Committee on Professional Ethics:

Non-government attorneys may ... ethically supervise non-attorney investigators employing a limited amount of dissemblance in some strictly limited circumstances where: (i) either (a) the investigation is of a violation of civil rights or intellectual property rights and the lawyer believes in good faith that such violation is taking place or will take place imminently or (b) the dissemblance is expressly authorized by law; and (ii) the evidence sought is not reasonably available through other lawful means; and (iii) the lawyer's conduct and the investigators' conduct that the lawyer is supervising do not otherwise violate the Code (including, but not limited to, DR 7-104, the 'no-contact' rule) or applicable law; and (iv) the dissemblance does not unlawfully or unethically violate the rights of third parties.

Mr. Strutin also refers to Office of lawyer Regulation v. Hurley, No. 2007AP478-D (Wis.Sup.Ct. Feb. 11, 2009), where the Supreme Court of Wisconsin affirmed a referee's finding that an attorney, who hired a private investigator to deceptively acquire a victim's laptop to conduct a forensic analysis, did not violate ethics rules. His reasoning was that the same deference accorded law enforcement in utilizing deception in criminal investigations should be afforded the attorney. (If you would like a more thorough discussion of these issues, I encourage you to click on the link to the article I've cited here, which also includes footnotes to further resources.)

As the regulation of conduct in these arenas evolves, lawyers need to tread cautiously into these waters and carefully balance the right to effective assistance of counsel against a lawyer's obligations to be truthful. There are many creative ways to use technology to obtain information, and the enticement to cross some unknown ethical line has never been greater.

Other areas of ethical concern include such things as posting or blogging about clients, judges and cases, friending judges or opposing counsel, and other conduct that has been found to occur online (the list is long and humiliating). This kind of conduct moves beyond the duty of confidentiality to simple common sense, and can lead to circumstances that may prejudice your client, require recusal or other consequences nobody wants. What you put out there will be read or seen out there. By everyone. And people talk. Particularly online.