SANDS ANDERSON

# Jeff Geiger Counters

## Lawyers Spy on FaceBook? Watching the Detectives….

September 30, 2010

By: Jeff Geiger.

Here's the situation: a witness is heavily involved in social media such that she will "friend" anyone that asks. Some have wondered whether an attorney or her assistant could use their real identity and gain access to, for example, a FaceBook site after the account holder accepts the friend request.

While Virginia has not formally weighed in on the issue, the Philadelphia Bar Association Professional Guidance Committee Opinion 2009-02 concluded that such an investigation would constitute unethical pre-texting. Specifically, a paralegal seeking access to the witness' social media pages would be doing so under false pretenses, i.e. to find out information about the witness without revealing the true nature of the inquiry. To do so would be in violation of Rule 4.1 (making a false statement of fact to a third-person), Rule 8.4 (misconduct to engage in conduct involving dishonesty), and Rule 5.3 (responsibility for non-lawyer assistants). My sense is that the Virginia State Bar would agree.

This opinion is not without its detractors and count me as one of them. No, I am not saying that we can use private investigators to fraudulently gain access to a witness' MySpace account. What I am saying is that it appears that the disciplinary authorities have not caught up to the technology (just as they failed to do with the revolution in media with respect to lawyer advertising). Think of the private investigator sitting in the proverbial tinted van, videotaping a person claiming a disability, who is mowing the lawn—clearly that is acceptable. The Philadelphia Bar rejected the videotaping analogy, noting that: "The videographer does not have to ask to enter a private area to make the video. If he did, then similar issues would be confronted, as for example, if the videographer took a hidden camera and gained access to the inside of a house to make a video by presenting himself as a utility worker." Yet, the reference to privacy holds less credence in my mind given the very nature of the social network at issue. Does society really believe that you have a reasonable expectation of privacy at a social media site? Just as an owner of private property (think shopping center) can allow a person to come on to the property, so can the account holder of a social media page (even while not checking the bona fides of the invitee). Clearly, it would not be deceitful if the lawyer found a friend of the witness, who allowed her to view the witness' social network page.

Similarly, the Association of the Bar of the City of New York Committee on Legal Ethics (quite a mouthful) issued its Formal Opinion 2010-2 in September, concluding that a lawyer may not attempt to gain access to a social networking website under false pretenses. In doing so, the NYC opinion assumes that the lawyer is engaging in trickery and reasons that:

"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."

The distinction to be made with the NYC opinion is that it assumes that the access is gained by "trickery." The door appears to be opened to the so-called "truthful 'friending' of unrepresented parties" and witnesses. Presumably, if you provide truthful information, that would be enough to pass muster. The bottom line is my abhorrence of a mindset that seeks to conflate all actions to the lowest common denominator and assumes that lawyers will engage in misconduct and that the public is so stupid that it needs to be protected from itself. If you put your information on the Internet and allow others to view it, so be it. Am I wrong?