I recently attended 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 focused on the legal and ethical issues facing lawyers and investigators using social networking contents in legal matters. (For a concise summary of the conference, see Social Networking - Legal and Ethical Issues for Lawyers and Investigators). Unlike other conferences, more questions were raised than could be answered. This was no reflection on the presenters. It reflected the fact that legal issues involving privacy and the gathering and use of social networking content as evidence are evolving much more quickly than legal answers can be found.

Four significant themes emerged from the conference:

1. The public has little understanding of the risk involved in giving personal information to membership networking sites (i.e.,. Facebook, MySpace, etc.) and in posting content on the site;

2. Existing law does not adequately address the legal implications of the methods used to gather, and/or the use of, evidence from social networking sites;

3. There are no specific ethical guidelines for lawyers to follow in participating in, or gathering evidence from, social network sites; and

4. The evolution of third-party applications used in conjunction with social network sites is changing the landscape on a continuous basis.

I hope to address each of these themes in a series of post that may or may not be consecutive. For the moment, let's take a look at the first issue: what is the public's expectation that the content of their site is protected from scrutiny by the public at large? Does the public have an understanding that information provided to the site for membership is protected?

First, it is doubtful the public gives serious consideration to the privacy of personal information provided to sign up for the site (called transactional information). In fact, I'd bet the thought never even crosses their minds. They're busy thinking about posting cool photos and taking fun quizzes. The idea that the information they just punched into those little boxes is now permanently stored on giant servers, and that the company that owns those servers may be required to give out the information in response to a subpoena or warrant is just not on their radar.

What is the public's expectation that the contents of their membership site is private to all but their friends? Probably pretty high. After all, sites provide "privacy settings" that

enable you to block unwanted visitors, among other things. Users have what I call the "appearance of control" over what is disseminated to the public.

And that's all it really is: an appearance of control. The fact is that both transactional information and content can be obtained through either legal or deceptive methods and you will never know it until someone decides they want to talk to you. In person. Legally, information can be obtained by either warrant or subpoena, depending on the nature of the matter (civil or criminal) matter and information (transactional or content). But more insidious is that there are many deceptive practices used by both public and private investigative sectors, which include, but certainly not limited to, creation of a fake social profile and attempts to "friend" either the subject of the investigation or a witness to activities giving rise to the investigation. (Whether any evidence obtained through deceptive practices is admissable is another conversation.)

In her guest post entitled Friend or Foe: UC Berkeley Investigates the Legal Landscape of Social Networking, Aspen Baker states:

There were a lot of big questions around what defines “content.” Is “content” what you write on your wall or post on your friends page, or is it also “transactional,” the information collected about your use of the social network: what did you search for? What pages did you visit? Most of the panelists thought everything should be deemed content and should therefore be considered, and protected, as private communications.

It was also noted that social context is incredibly important to our ideas of privacy and that privacy has a lot to do with expectations. We may not expect what we post on a friend’s wall to be private, but we probably expect that sending a private message will. However, according to Paul Ohm, Professor of Law at the University of Colorado Law School, email services such as Gmail are changing our expectations of privacy, as we find tailored advertisements in our internet browsers. If we are comfortable with getting advertisements for running shoes after emailing a friend about our trail run, what legal implication does this have for future expectations of privacy?

As I mentioned, these questions were raised and discussed, but any conclusions were really a matter of opinion. There simply are no legal guidelines on these cutting-edge issues.

Mark Howitson, Deputy General Counsel to Facebook, stated that Facebook tries to educate the public in its terms of use and disclaimers regarding the risks of privacy invasion when posting content on their site. Interestingly, Facebook takes the position that by using their site, the public assumes the risk. But others on the panel, and many in the audience, disagreed. On some intangible level it seems unreasonable to assume the public even considers these matters, or has any expectation that law enforcement agencies might be digging around in profiles on membership sites. In her blog, Aspen Baker calls this the "buyer beware" argument and states that: ". . .we, the users, not only need to beware of the consequences of our participation, but most importantly, we need

to be consumer advocates who fight for our own protections and demand legal, and wide-ranging respect for our privacy online."

This is clearly only the beginning of what will be a very long discussion in and out of courts of law, as it raises many fourth amendment concerns (to be discussed in Part II of this series). As participants in social networking and media, however, we need to begin expressing our views and creating a knowledge base that can not only benefit consumers, but also effect public policy and legal challenges to our privacy. Please voice your concerns here, to your friends and wherever the issue is discussed.