Social-networking sites like Facebook< URL >, Twitter < URL > and others create unexpected property and privacy risks that many people are unaware of. Even under the best circumstances, when you posting your whereabouts, location, activities, photographs and private interests online, you exposes that your information not only to your circle of friends, but at a minimum also to the organization-people who that operates run the service. At worst, you may be feeding information to a great many nasty people. Other consequences can result if the information is obtained outside of appropriate authorization.

Individual Privacy

Among the pressing individual privacy issues encountered online, some of the scarier scenarios include stalking, impersonation, and property crimes. Online stalking and harassment have been well publicized in recent years < URL to a review > and simply not only add the use of technology to the traditional crimes but can also escalate the level of harassment. Both can escalate into more serious personal crimes. For example, < insert a brief summary to a specific case and provide a reference >.

Timely information about a victim's whereabouts also enables property crime like car theft or burglary. Police statistics suggest that…. < URL >.

Impersonation Identity theft may not seem like a big deal to most people, is the fastest growing crime in America < URL > but it is a serious issue and SSN Social networking and other sites can serve as shopping centers for identity thieves. < URL for reference > Criminal hackers can use require users to present credentials like a user name and password to prove to the service that they are, in fact, the person associated with those credentials. Unfortunately, attackers can utilize any number of reliable methods to compromise user credentials. Even if an attacker doesn’t "hack into a laptop" to steal a password, most people use simple passwords that are easy to guess or predict if they have some personal information about the potential victims post about themselves such as—(children's names, pets, locations, birthdays, vehicles, and sports, etc.)—exactly the type of information available on social networks. to guess effectively at passwords for goldmines such as online access to financial accounts.

Stolen credentials identity could can be used by an attacker to make disparaging or inappropriate comments on a shared forum while impersonating the victim, thus causing embarrassment and even opening up the victim to legal pursuit for defamation < URL for specific case if possible >. The victim may need to apologize and attempt to redeem their reputation. This may not be a big deal for some people, but that same level of compromise also provides a n attacker imposter
might even be able the ability to post child pornography in a victim's photo album – a felony.<URL to specific law using Cornell’s law pages> Now we’re talking about serious crime. Taken a step further, if the victim, simply by visiting their own home page, would likely discover the offense and in doing so, transfer the pornography to the cache of their Web browser on their local computer and thus, Now they have inadvertently violated yet more laws by transferring the material to their computer.<URL for specific law> (Possession and transmission of child pornography are distinct crimes). With a little planning on the part of an attacker, the victim could be arrested, prosecuted and convicted of a felony crime. You may discount a few off-color comments on “your Wall”, but going to jail and becoming a life-long registered sex offender is serious business.

Another risk comes from the common practice of using the same password for multiple accounts. Do you use the same password on Facebook, Twitter, Blogspot, Photobucket, your email and your bank account? What if an attacker uses your online bill pay to mail themselves a check?

Abuse by Service Providers and “Partners”

Most social networks are designed with good privacy controls; However, security is largely a human problem, and people make mistakes. Employees or vendors of the service provider can make mistakes accidentally or intentionally disclose otherwise protected information. Large disclosures of consumer data are a common occurrence in the news because they are frequently associated with financial or identity fraud.<URL>http://www.privacyrights.org/ar/ChronDataBreaches.htm>

As it is now, corporations can collect and assimilate massive databases and use that amounts of information and then apply it to market products, predict elections or track down terrorists (among other things). It’s called data mining, and it’s big business.<URL to statistical article> As an example, tweeting(?)? about your Starbucks BarStucks instant coffee at the office may be used to estimate market growth potential for their new instant-coffee offering.<URL> A good estimate may affect the stock price, which may create or destroy millions of dollars in the stock market.<URL> Inappropriate use of the same information may enable insider trading to benefit from the information before it is known to Starbucks BarStucks or the public. It’s no secret that demographic information is valuable in many organizations and political parties. The potential for government abuse of this type of information is also a subject of lively debate in ethics,<URL> privacy rights<URL> and security<URL> circles.

Companies also perform background checks on individuals using social networking sites. Right now, these checks are primarily performed when an individual applies for a job or a security clearance, but we may (read: will) also see a day when your health insurance company checks into your “lifestyle” to judge the rates you should be paying for medical coverage. From another standpoint, you may have gotten a kick out of sharing your antics at the bar via your mobile phone camera, but how would you feel if those same time-stamped pictures were displayed in court while you were fighting being fired for wearing a t-shirt with your employer’s logo on it at the time?

In the second part of this two-part series, Jeff Keith discusses intellectual-property issues on SN sites and concludes with some simple recommendations pulled over for drunk driving a half-hour after they were taken! that you can pass on to your employees and your families.
In the previous article in this two-part series,

**Other Intellectual-Property Issues**

When members post photos, essays or other materials on their social networking or other SN sites, they frequently also sign-away their control of the materials by accepting the terms of service for the site. Photobucket, for example, reserves the right to re-use and sell individual content for any reason at any time. If you ever see a real-estate commercial on television with a picture of your house from your Photobucket account, don't be surprised. More importantly, don't expect any royalty payments for the use of your images.

Facebook has been all over the news lately in 2008 regarding its controversial change to its privacy policy that allowed Facebook to permanently retain and reuse content from individual users. Following public pressure and lots of negative publicity, Facebook reverted their terms to exclude the "permanent" provisions for content re-use. Since Facebook is also in the news about its business model and how it will make money off of the service, speculation as to how the company might leverage the information on user pages is also the subject of a lively debate.

Another intellectual-property issue is the violation of property rights of others when SN users post copyright photographs by professional photographers on their sites or when they post pictures on other people without permission of the subjects. These... (etc.) (laws) (specific case) (refs with URLs).

**Conclusion Recommendations**

While social networking SN sites and other similar sharing or communications technologies enable us to catch up with new and old friends, share pictures and maintain friendships or relationships with others, there are a number of subtle but serious privacy and intellectual-property implications in using these services. Some practical suggestions:

- Don’t use the same password for SN sites as for financially-sensitive sites; in general, don’t use the same password across any Web sites.
- Don’t post other people’s intellectual property on your site without written permission.
- Think carefully before you post intimate details of your life, your preferences, your activities and your crimes on the ’Net.
- Every user should actually read the terms of service and privacy policies of these services before using them and consider potential risks when posting or maintaining content on the sites.

Do your children or those of your relatives and friends use SN sites? Probably. Pass these articles and recommendations on to them. Let SN stand for social-networking and not for S______ N______ (come up with something cute that starts with S and N and means something bad).

* * *

Jeff Keith < contact e-mail > is... (bio 2-3 sentences).

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >