Staying Private in Public

How to Limit Your Exposure on Social Network Sites

Tips for Consumers

Consumer Information Sheet 14 • June 2014

How we interact with people has changed radically in the 21st century. Today, more and more of us, young and old, are going online to share our opinions, experiences, photos and videos.[1] We expand and nurture our personal and professional relationships using Facebook, LinkedIn, Twitter and YouTube. Simply put, we socialize on social networks now.

Social Network Types

Social networks fall into loose categories. There are personal networks like Facebook and MySpace; status update networks like Twitter and Google Buzz; location networks like Foursquare and Loopt; and content sharing networks like YouTube and Flickr. Social networks can combine features or change completely over time. What they have in common is that they need information about you to succeed.

What You Share

The people who run social networks want you to share information about yourself. They say that this allows them to "personalize" your account so you "enjoy the maximum social experience." The more details you give social networks, the better they can contour your life online.

Maybe you are a Basset Hound owner. The social network "reads" your references to Basset Hounds on your profile and sends you names of other Basset Hound owners on the network for you to contact. You contact those owners who contact other owners who contact other owners – it can go on forever. By sharing your love of Basset Hounds, you have launched an active expanding group of Basset Hound owners. That's social networking.

Online social networks encourage us to share photos and videos, "tagged" with the subjects' names, age, gender, other biographical information such as education, employment and hometown, contacts including how to reach them, status updates (what we're doing now and location), interests, likes and dislikes.

You Can Control Your Social Network Experience

As we interact with others in the physical or "real" world, we use common sense, practice good manners, and obey the law. If we are human and make a mistake, we try to correct the wrong and move on. It's a smart way to live.

When we socialize on the Internet the same principles should apply. In sharing our comments, tweets, photos, status updates, messages, and profiles, "trust" takes on enormous weight. We can only hope our "friends" will think before revealing our secrets to their "friends." In a place where our "friends" may each have 5,000 "friends," that's a lot of trust.

You can control your social network experience and what you share.

Your Privacy Settings

Most social networks automatically set your account so that "everyone" can see who you are and what you do[2]. You don't have to accept that exposure. You can decide how public you want to be.

An article in Consumer Reports reveals that one in four households don't use their social network privacy settings.[3] You can buck that trend. Regularly visit your "Account" to customize your privacy settings to suit your tastes.

Also read (and re-read) the social network's privacy policy to learn how the site handles your personal information. This includes information you post and information you provide if you register. It also includes information collected when you browse or visit the sites. Look in the policies for opportunities to control the use of your information by the sites and others with whom they share it.

Being Choosy

- Keep your circle of friends recognizable. If you let an unknown person join your network, his or her unknown friends can have access to your information too. Judge strangers as strangers, just as in the "real" world.
- You can say no when your social network suggests adding a friend or feature or app to your account. If you change your mind, you can add them later.
- Take a minute and think about what you share online. Don't discuss medical conditions or anything you wouldn't want to see on a billboard.
- If you share things like your pet's names, don't use those names in your passwords. Bad guys scan social media pages for that kind of information to help them discover your online passwords.
- Don't post your home address or phone number.
- Protect your email address - don't post it. Use the social network's messaging tool instead.
- Be careful about revealing where you are, also known as your "real-time" location.
- Never post that you'll be away from home. Check out *www.pleaserobme.com* to see how easy it can be for bad guys to rob you.
- Don't provide your full birth date in your profile – omit the year.
- Don't label or "tag" your children's photos with their names on your social network. Ask friends and family that post photos of your children not to tag the photos they post.
- Use a strong password for access to your social network pages and NEVER share it.
- Use strong password-like strategies for answers to security questions. For example, answer "What was your first pet's name?" with "D0naLDuck%67."
- Always supervise your children on Facebook, MySpace and Twitter or any other social network where they are likely to be sharing personal information with internet "friends."
- Protect your information by protecting your computer with the best anti-malware software available. See our *Consumer Information Sheet 12: Protect Your Computer From Viruses, Hackers, and Spies.*

Watch Out for Apps

Many social networking sites invite you to download applications (apps) offered by third parties. The apps are not covered by the social network's privacy policy. Games and quizzes are the most popular and well-known examples of social network apps.

The Federal Trade Commission confirms that the companies behind some of these apps are likely to have access to the information you or your friends post on the social network.[4] And *Consumer Reports* says that apps infect millions of computers with viruses yearly.

If you enjoy using apps, take some extra time to protect yourself and your computer. Look for application privacy settings in the social networking site's privacy policy. Read the notice that pops up when you start to download an app. Consider whether the app is worth the "information cost" you would pay.

The ACLU has its own fun quiz that reveals the ups and downs of apps. Look for it on their web site at *www.aclu.org.*

For Additional Information

Federal Trade Commission, ***Protecting Privacy in an Era of Rapid Change***, December 2010, available at *www.ftc.gov/os/2010/12/101201privacyreport.pdf*.

Hoofnagle, Chris Jay, King, Jennifer, Li, Su and Turow, Joseph, ***How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?*** (April 14, 2010). Available at SSRN: *http://ssrn.com/abstract=1589864.*

Ito, Mizuko et al. ***Hanging Out, Messing Around, and Geeking Out: Kids Living and Learning with New Media***. Cambridge, MA: MIT, 2010.

Kirkpatrick, David. ***The Facebook Effect: The Inside Story of the Company That Is Connecting the World***. New York: Simon & Schuster, 2010.

Marwick, Alice E., Diego M. Diaz, and John Palfrey. ***Youth, Privacy and Reputation***. The Berkman Center for Internet & Society Research Publication Series:, 13 Apr. 2010, available at *http://cyber.law.harvard.edu/publications.*

Palfrey, John G., and Urs Gasser. ***Born Digital: Understanding the First Generation of Digital Natives***. New York: Basic, 2008.

Privacy Rights Clearinghouse, ***Fact Sheet 35: Social Networking Privacy: How to be Safe, Secure and Social***, available at *www.privacyrights.org/social-networking-privacy*.

Wolinsky, Art, ***Protecting Privacy on Facebook***, tutorial available at *www.wiredsafety.org/fbprivacy/index.html*.

This fact sheet is for informational purposes and should not be construed as legal advice or as policy of the State of California. If you want advice on a particular case, you should consult an attorney or other expert. The fact sheet may be copied, if (1) the meaning of the copied text is not changed or misrepresented, (2) credit is given to the California Department of Justice, and (3) all copies are distributed free of charge.

NOTES

[1] Overview, "Older Adults and Social Media l Pew Research Center's Internet & American Life Project." Pew Research Center's Internet & American Life Project. Web. 27 Dec. 2010. *http://www.pewinternet.org/Reports/2010/Older-Adults-and-Social-Media.aspx*

[2] Facebook Privacy Policy November 23, 2010, *www.facebook.com/?ref=home#!/privacy/explanation*. php: "The settings you choose control which people and applications can see your information. You can share your information with friends, friends of friends or everyone, and we offer presets to help you do that. Or, if you prefer, you can customize your settings."

[3] Consumer Reports, June 2010.

[4] p.6 *http://www.ftc.gov/os/2010/12/101201privacyreport.pdf*.