

Teen Privacy Online

Social Networking, Privacy Policies and Security Risks: How to protect your personal information online

- I. Online Privacy: Why It's Important
- II. Social Networking:
 - § You Can't Get Something for Nothing
 - § Know the Basics: Disclosure of Personal Information and Networking Behavior
 - § It Isn't all about Common Sense: Basic Technological KnowHow is a Necessity
 - § Think About Tomorrow when you are Acting Today
- III. Privacy Policies and How to Read Them
- IV. Security Risks
- V. Sources and Resources

Sponsored by:



Online Privacy: Why It's Important

Teenagers and young adults are among the most knowledgeable and creative users of the Internet, spending hours every week online surfing the Internet, doing homework, gaming, socializing with friends, and shopping. In almost all of these contexts, teens and young adults share personal information online. Personal information, also referred to as personally identifiable information (PII), is information that may be used to identify or contact you and includes your name, address, phone numbers, school name, birth date, social security number, photos of you, videos, credit card or bank account numbers, shopping habits or preferences, and any information about your life, likes and dislikes. When you give your phone number to a friend in your class and ask them to call you, for example, you are making a decision about sharing your personal information with another person.

The technologies used by a majority of teenagers today, including social networking sites on the Internet, Instant Messaging, chatrooms, filesharing networks, and cell phones make it much easier to share personal information with a much broader group of people. These technologies often allow those with real-time access to shared information to copy, store and forward that information. The information may also be archived or indexed by search engines and other technologies that may increase its accessibility on the Internet and make it difficult to remove. In short, these technologies greatly increase the possibility that your personal information may be shared or made available in a way that you do not intend or in a way that may have harmful consequences for you.

Today, in the United States and in 27 European countries, privacy professionals, corporations, government agencies, nonprofit and academic institutions, and students are coming together to celebrate Data Privacy Day. In honor of Data Privacy Day, privacy professionals will be working in schools across the nation today and throughout the coming month to raise awareness and generate discussion about online privacy -- encouraging use of the Internet and all of the communication and ecommerce tools it offers, while helping teenagers and young adults learn how to protect the privacy of their personal data and be safe online.

Privacy Defined

One way to think about privacy is as the right or opportunity to decide who has access to your personal information and how that information should be used. This presentation will review the people and entities that may have access to your personal information when you place it online, the ways that they may be using that information, and the things you can do to make sure your information is accessed and used only in the ways that are okay with you.

Keep in mind that knowledge is power. The more you learn about the way technology works, the more you can use it effectively to your advantage and avoid potential risks. The more you know, the more you can make considered decisions, act responsibly, and safeguard your personal information online.

Social Networking

When you create a personal profile on a website like Facebook, MySpace or Friendster, and interact with other people online, you are engaging in what is referred to as “social networking.” Depending on how you manage the privacy settings, participation in these networks allows you to meet, converse, and otherwise interact with other Internet users whom you accept as “friends,” who attend your school, who work with you, who live in your geographical area, or around the world.

Networking safely and in a way that protects the privacy of your personal information is the goal.

We hope you take away from this presentation four main ideas about data protection and privacy in the social networking context:

- 1) You usually can’t get something for nothing;**
- 2) Know the basics about disclosure of personal information and networking behavior;**
- 3) It isn’t all about common sense; and**
- 4) Think about tomorrow when you are acting today.**

First of all, some good news.

A recent study completed by the Pew Internet & American Life Project regarding Teens, Privacy & Online Social Networks (April 18, 2007) shows that most teenagers who use online social networks such as MySpace and Facebook are taking steps to protect themselves from the most obvious areas of risk by actively managing the personal information they share online – limiting the personal information on their social networking profiles, limiting access to those profiles, and acting cautiously with respect to people they do not know.

To assess the risks associated with your own online interactions and communications, you need to consider who has access to your information, and be aware of how they will use that information and how that use may affect you.

1) Usually – you can’t get something for nothing.

On many social networking sites, individuals can create accounts, sign on and create pages without paying fees of any kind. Creation of a page and participation on the site, using the sites’ vast array of communication tools -- gets you something – the ability to interact with people on-line who have similar interests, go to the same school, etc. While you don’t pay a fee, there is a cost to participation in these social networking sites. Understanding and thinking critically about what those costs are allows you to make an informed decision about how you wish to participate. It is to your benefit, for example, to understand how the providers of the service may be generating revenue. In most cases,

some form of advertising supports the service, as is the case in most “free” email and search engines.

Most social networks are open to surveillance and participation to some degree by a number of different people: site owners, marketers, parents, friends, other network participants, college officials, employers, and government agencies. Sex offenders and other on-line predators may also be on the site, often providing false information about themselves, despite both prohibitions of such behavior in contractual terms and other technological efforts to keep potentially harmful participants off of the system. Consider the personal information you are providing when you create an account and a profile on a social networking site, and think about how that information might be used.

What information do these groups of people want? And why?

Web Site Operators -- Site owners want to make sure that your time and use of the site is enjoyable to get you to remain on the site and recommend it to others. This customer satisfaction imperative benefits them by creating a larger audience for advertising and marketing purposes. The more people create accounts, the bigger the audience for the advertising, and the more valuable the advertising space becomes.

Companies that want to sell you things -- will be interested in your brand loyalties, buying habits, likes and dislikes. Marketers may use cookies to recognize your computer, to compile information about your computer’s interaction with various ads, and to deliver targeted advertising based on that information.

What does this mean for you? Possibly more personally-tailored advertising campaigns, materials, or emails directed toward you. You may not think this is a bad thing, and it may, in fact, be highly convenient for you. But it is also a cost and should be recognized as such – you are allowing a person or company to use your personally identifiable information to enable targeted advertising and maximize sales.

Parents – want information on how you, their child, are doing out there in the world – maybe information about drinking, drugs, sex, and friends.

Discussion questions: They probably would not read a diary, if you kept one under your bed. Should they read your blog (short for “Web log”), social network page, or on-line journal? Does it make a difference in your expectation of privacy if those materials are available for the review of others you don’t know on the Internet?

College officials and current or future employers – want to know what kind of person you are, and whether you are good student or employee material.

Sexual predators and pedophiles – may want to locate you and meet you in real physical space. They may pretend to be someone they are not in order to accomplish this.

So, what personal information are you going to decide to give these various people or entities?

2) Know the Basics: Disclosure of Personal Information and Networking Behavior

Basic guidelines for disclosure of personally identifiable information online:

Be sparing with personal information. If you network socially, give out only such personal information as is necessary to use the network effectively.

Do not use your first name or your birth date in your user name, and do not share your password with anyone.

In your profile, do not provide your last name, phone numbers, address, date of birth, school or team name, or travel plans. Do not provide your social security number, your family's financial information, bank account or credit card numbers.

Exceptions to the basic rule: You may have to provide your birth date to a social networking service in order to create an account, but you can arrange your privacy settings so your birth date is not visible on your profile. Or, if you want your friends to keep track of your birthday and send you cards, you can arrange your settings so the date is visible but not your birth year.

Also: Although you generally should not provide your school name online, some sites feature school-specific networks, and the name of the network will reveal your school online. Limiting your social networking participation to a school group, as opposed to the world at large, may provide an extra degree of protection and privacy for you.

Note: There are also some school-moderated/administered networking sites in which you enroll through the school. Such sites are often designed to be interactive learning environments and may, accordingly, be accessed by teachers and parents as well as students from the school or state. Participation in such sites may be limited to individuals whose access is approved by the school. The sites may be sponsored by companies, foundations or educational grants and may be associated with charitable or educational purposes that are not related to, or associated with, advertising.

The short quiz provided by CyberStreetSmart.org entitled, “What can your profile reveal?” at www.cyberstreetsmart.org/Networking/soc_friend.html is an interesting and interactive way to see how a personal page may reveal more than a user intends.

Privacy Settings

Use the privacy settings available on many social networking sites to secure your personal information and to reflect your level of comfort with the disclosure of that information, restricting access to your profile if you choose. Be aware that default settings often allow the sharing of information, and you must take affirmative steps to limit that sharing.

Access the Privacy Settings page on the social network of your choice and learn how to protect the privacy of your information.

Some social networking sites automatically mark the profiles of younger users as private and limit the ability of older users to browse younger users’ profiles. Some sites offer you the ability to set different privacy settings for different parts of your profile page. Accordingly, be aware that establishing privacy settings on any site can often be a multi-step process. You may be directed to make certain choices about your profile but directed to take separate actions to keep your notes, blog, or photos private.

Note to presenter: If you are using a connection to the Internet as part of this presentation, you could take this opportunity to access Facebook or MySpace or a similar social network suggested by a student, locate the privacy settings, and demonstrate how a user could make various privacy choices in the context of a particular site.

On Facebook, for example, adjusting privacy settings is a multi-step process. After clicking on “Settings,” then “Privacy Settings,” you will have the ability to adjust settings in each of the following categories: profile; search; news feed and wall; and applications. You must take separate actions to keep your notes private, and you deal with the privacy of photos on an album-by-album basis. Within each of the foregoing categories, there are numerous sub-categories that you must select privacy settings for on an individual basis. The setting choices are numerous. If you don’t understand them, contact the site and ask.

On MySpace, every user has the option of marking her profile private, and all users under the age of 16 are automatically assigned private profiles as a safety measure. Additionally, under 18s can never browse for under 16s and adults can never browse for under 18s.

Maintaining privacy requires diligence and maintenance.

Learn about the privacy settings of each site you use. If you don't understand the options, contact the site and ask.

Regardless of the settings you use, **privacy settings are not foolproof.** You should always continue to act cautiously when you place information about yourself online regardless of how restricted you believe your audience is.

Generally speaking, even if a site has a privacy policy in place, it cannot guarantee that content you post on the site will not be viewed by unauthorized persons. No matter how restrictive you make your own privacy settings, social networking sites cannot control how a "friend" might use the information or content to which you have given them access. In the end, you are the single best protector of your privacy by making smart choices about what information you share online.

Basics of On-line Social Networking Behavior:

Beyond appropriate restrictions on disclosure of personal data in online contexts, there are useful guidelines or general rules for online behavior that will help you protect your identity and your personal information now and long-term.

The Number One Rule

Unless you would be willing to attach something to a college application or resume, share it with your parents, your grandparents, current or future employers, don't post it. If you wouldn't put it on a poster and hang it on your locker or your dorm room door, don't post it.

In addition:

Be aware that when you journal or blog online, these entries are archived, or saved, and that the content of such entries can be searched. Some blogging sites offer you the ability to choose which subscribers can see what you have written, and some allow you to block any anonymous replies.

Think about why and how you are using your profile page. If you are blogging about your daily activities or your social life, be extremely cautious what personal information you provide about yourself *and others* in those contexts.

A Word about "Friends":

Don't invite people to be your friends on-line if you do not know them in the real world. Some people feel social pressure to accept when faced with a friend request. While it is undoubtedly awkward to decline someone's request to be your friend, it is often the safer approach. You should share the information on your profile page with people you actually know.

If you must accept a "friend" that you do not know, do so cautiously, recognizing that often people are not who they claim to be. 56% of teens who have profiles on social network interviewed by the PEW Foundation admitted to posting at least a few pieces of false information about themselves. Others may communicate using false identities for harmful purposes.

Also, if you do interact with "friends" you do not know in real life, CyberStreetSmart.org suggests that you watch for the following warning signs: requests for loans or monetary gifts; early expressions of love or affection; requests for you to ship or receive packages; professions that make online suitors particularly inaccessible; requests for you to cash checks or money orders; extensive grammatical, spelling, or linguistic errors; requests for passwords, PIN numbers or other personal information; and job offers or opportunities. Requests

for information about your family members or family plans may also be a red flag for suspicious activity.

A Word about Photos:

Many teens regularly post, tag and share photos on their personal profiles. While the photo tool is a convenient and expeditious way to share photos, you should always be very careful about what photos you choose to post.

- Do not post images of yourself that you wouldn't want to share with grandparents, colleges, and future employers.
- Don't post images of other people that they wouldn't post of themselves.
- **If possible, ask permission before posting an image of someone else on your site.** Be sure to let others know who has access to your site, so they will know the extent of their exposure if they agree to be on your site.
- If you post so many photos to your page that asking each individual is unrealistic, **make sure you always honor any individual's request to remove a specific photo of him or her from your page.** Along the same lines, if a friend is taking pictures or videos at a party, and you don't want pictures of you to appear online, affirmatively ask the person not to include such pictures on their profile page.

Avoiding Risky Behavior

Sex -- Just don't talk about it on the Internet, particularly with people you do not know.

If someone begins a conversation that is sexual or creepy in some way, block them, do not respond, and sign out. Don't even play along in what appears to be a joking fashion with a person you do not know.

And, as a general rule, never agree to meet someone in person that you "met" on the Internet. If you do arrange such a meeting:

- Research the person first. Find out whatever you can about the person online, using search engines.
- Bring a parent or other adult friend if possible.
- Meet in a very public place.
- Meet during the day.
- Make sure someone knows where you have gone and when you will be back.

How else can you protect your privacy?

Use services with age and identity verification systems and links that can be used to report inappropriate content, response systems that deal with such reports quickly and effectively, and staff members who review images and content for compliance with the site's guidelines.

Look for **privacy seals** from organizations like TRUSTe or the Better Business Bureau. Facebook, for example, has TRUSTe's seal of approval. The TRUSTe seal means that the company who displays that seal takes your privacy seriously and adheres to TRUSTe's strict privacy principles, including notice and disclosure, choice and consent. TRUSTe monitors the compliance of its member businesses and provides an arena in which you can file a privacy violation complaint that will be resolved effectively. You can click TRUSTe's icon on Facebook's privacy policy to visit TRUSTe's site and learn more about the significance of such a seal.

Note: You do not have to be a member of Facebook or MySpace to access their privacy policies. You should review privacy policies before providing your personal information to better understand the type of information the site collects and the ways in which that information might be used or shared as well as the controls on that information you may be able to request.

Talk with a parent, an older sibling, or another adult you trust about your use of the Internet and ask questions if you have them.

Educate your parents about technologies that are new to them. While they may not be as knowledgeable as you are about the way the machine works, they may have some very good ideas about how it should be used in a manner that will be safest for you.

- Check out any safety or privacy tips provided by the site you are using. MySpace features a Safety Tips page with materials for teens and parents (the link can be found at the bottom of the MySpace homepage). Facebook also offers privacy tips for its users in the context of its privacy page, <http://www.facebook.com/help.php?page=419>, and urges parents to become educated and to talk with their kids about the safe way to use social network services. Other online resources, many of which are listed at the conclusion of this presentation can provide additional safety and privacy information.

Always try to understand what information is being collected and who has access to it. Assume that personal information on the Internet may be stored or accessed for quite some time if it was ever generally available online.

3) It's not just common sense –

When it comes to using the Internet for the creation of personal profiles, common sense is essential, but alone, may not be enough. Our common sense is informed by rules we learn from our parents and just operating in daily life, going to school, playing sports, going out on the weekends.

Some rules your parents taught you like “don't ever get in a car with a person you do not know” or “don't open the door to someone you do not know” – still make sense. But others, like “don't talk to strangers,” seem inapt in the context of social networking on the Internet. Isn't that the whole point for some users? Meeting new people? According to the PEW Study, 49% of social networking teens use the networks to make new friends, and 31% of social networking teens have “friends” on their profiles whom they have never met.

There are lots of things about the Internet that are not immediately obvious or intuitive – even to a person who has grown up playing games online on a daily basis.

For example, **caching** –

Basically, caching means that if you put something on your profile page – even just for a day or two -- that information or image remains accessible to others on the Internet even after you take it down or change it. Search engines cache web sites, allowing photos, videos, and text to be retrieved long after the web site has been deleted. “Chat,” journaling, blogs, pictures and other postings become public information. In a sense, a social networking page gives you access to a brave new world of youthful indiscretion. It is up to you how you use it.

Related Tip regarding Public Access Computers: Caching also raises issues you should be aware of when using a public computer, such as a public (Internet café), college, or high school library computer. A cache may store websites that you have visited so the browser can store them locally instead of going to the website. Also remember that, on some sites, you are asked whether you wish to have your password stored locally. When you are not using your personal computer, you should decline these requests. The browser may also store temporary internet files, cookies, and information that you have entered into websites or the address bar. Caching may allow your habits or personal information to be tracked on a public computer.

After using a public computer, you can go to the “Preferences” or “Internet Options” folder in the browser and click on “Empty Cache” or “Delete Browsing History” to make sure that does not happen. Finally, close the browser before you leave the computer.

Note: People who use Apple or Linux should familiarize themselves with the procedures for deleting browsing histories on those computers.

4) **Think about tomorrow when you are acting today.**

Unintended Consequences

Do you know how much money it costs to remove a tattoo? It can cost hundreds or thousands of dollars, depending on the size and quality of the tattoo. A lot of adults are trying to come up with the money to remove tattoos that seemed like a good idea at one time. Even after removal, there could be a scar or some remaining color. This doesn't mean you should never get a tattoo – it just means you should be well aware of the costs and consequences associated with making such a decision, now and in the future, before you do it.

It is the same with social networking and blogging online – keep in mind that once you put them out there in cyberworld, information and images can be extremely difficult if not impossible to take back. Even when you delete information from your profile or site, older versions are still accessible to others.

- MySpace provides the following notice on its safety tips page: “**Think before you post.** What's uploaded to the net can be downloaded by anyone and passed around or posted online pretty much forever. You shouldn't post photos or info you wouldn't want adults to see or people to know about you.”

Do not jeopardize the privacy of others.

Back to the rules your parents taught you that work equally well in the real world and online – treat other people the way you would want to be treated. Respect the privacy – and the personally identifiable information – of others.

Don't identify others on your profile in a way they would not be willing to identify themselves on their own. Don't share the personal information of friends or others. And don't post images of people that they wouldn't post of themselves. **If possible ask permission before posting an image of someone else on your site and always respect requests to remove photos or the personal information of others.**

Privacy Policies

Most websites that you interact with will collect some personal information. Many sites/companies have privacy policies or privacy statements posted on their websites designed to tell you what they will do with this information. Before you give any personal information to a web site, look for the privacy statement. If you do not see one, that could be a cause for concern.

Although they are often long and involved and may not be as clear as one would hope, privacy policies generally try to convey:

What information the site will collect,
The purpose for which the site collects that personal information,
What it will do with the information that you provide to it,
Whether third parties may have access to that information, and
What steps the site will take to ensure the security of your information.

When you find the policy, make sure it addresses the following topics: notice, choice, access and security.

Notice: Web sites should tell you exactly what information they are collecting from you and how they are going to use it.

Choice: Web sites should allow you to exercise some choice over the collection and use of your personal information.

Access: You should have the ability to access your personal information maintained by the site and to correct any inaccuracies.

Security: Web sites should provide reasonable security to protect your information from loss, misuse, or alteration.

If a site makes a practice of selling your personal information to third parties, for example, this is where you will find that information. Look for the opportunity to opt-out of practices with which you are not comfortable.

A privacy statement should also provide: information about the registration process; any special services the site provides; co-branding (business arrangements with other companies and how those companies can access and use your personal information); links to any other sites; how the site uses cookies, which memorize your Internet address; and contact information.

The privacy policy can be treated as a legally binding document in the sense that a web site owner may face legal action if he or she does not adhere to its own privacy rules.

- Always keep in mind, however, that a policy is merely a policy.

- Because the policy is essentially the measure of your rights on the site in which you are participating, pay careful attention to the ways in which the policy limits the site's exposure and accountability.
- Look for a web seal that lets you know the site takes its policy and your privacy seriously.

General Rule: Look for privacy policies and READ them. But always continue to act cautiously online regardless of the policy's representations.

Security Risks

Passwords

Keep your **passwords** in a secure place, and do not share them. Experts suggest: the strongest passwords have at least 8 characters and include numbers and symbols; do not use your personal information, your login name or adjacent keys on the keyboard as passwords; change your password every 90 days or so; and use a different password for every online account you access (or at least a good variety).

File-Sharing Software

Avoid down-loading file-sharing software. If you use this software be extremely careful about the information you share in order to protect your personal information. Read end user agreements, understand whether you are allowing spyware to be installed on your machine, and understand the risks of free downloads.

Spyware

Spyware is a program that can be installed on your computer from a remote location to steal your personal or financial information or to monitor your online transactions to capture that information. Generally, you will not know that you are downloading spyware. It is often masked by some other program that you intend to download or an attachment that you intentionally open. That is one of the reasons why it is important to know something about the programs that you install on your computer and the email attachments that you open.

You can install **antispyware software** to detect and remove these spyware programs. A number of the anti-virus programs and security products are also capable of screening for various types of spyware if the appropriate settings are used.

Apart from spyware, other malicious types of code, like viruses, may also be associated with email attachments. These viruses are best prevented by up-to-date virus protection software, which may protect much of the information on your computer from the harmful effects of viruses. In many cases, viruses are transmitted through spam messages that use interesting titles but come from senders or addresses with which you are not familiar. You should always treat such messages with extreme caution and avoid opening attachments to emails from unfamiliar addresses.

Phishing

Beware of phishers: In **phishing** scams, criminals send out spam or pop-up messages in an attempt to lure victims into sharing their personal and financial information on fake websites. They often disguise themselves as well known businesses and set up fake websites. For example, you may receive an email from paypal or amazon.com, if you typically use those services, suggesting that there is some problem with your account and requesting you to click on a link, enter your personal information and resolve the issue. Don't do it. Be very suspicious of an email purporting to be from a company but providing a link that does not send you to the .com domain address of that company.

If you suspect that there may actually be a problem, go through your browser to access the site and contact the company to ask if there is a problem with your account. Companies like to know if they are being used as a phishing tool and often request that you forward the phishing email to them. **Antiphishing software** is available that recognizes or blocks fake or phishing web sites. Also, many sites provide guidance as to what types of information they will and will not request from you online. Some sites may also provide information and warnings about recent phishing attempts involving their sites.

Automatic Updates

Automatically updating your computer helps ensure that your information is protected from the latest threats.

Sources and Resources

The foregoing information was drawn largely from information found in a number of articles and on websites concerned about online safety and data protection. These sources and resources will provide additional, helpful information for you if you are interested in learning more about any of the privacy issues discussed today.

Please visit www.dataprivacyday.org for a list of sources and resources, along with links to educational videos about data protection and online safety.

Online Privacy: A Tutorial for Parents and Teachers, prepared as collaborative effort by TRUSTe, Symantec, and iKeepSafe (2007),

www.truste.org/parent_teacher_tutorial.php

A Privacy Paradox: Social Networking in the United States, by Susan B. Barnes, First Monday: peer-reviewed journal on the Internet, Vol. 11, No. 9 (Sept. 4, 2006)

PEW Internet & American Life Project, *Teens, Privacy & Online Social Networks: How teens manage their online identities and personal information in*

the age of MySpace (April 18, 2007), by Amanda Lenhart and Mary Madden, Senior Research Specialists.
Thoughts on Facebook, by Tracy Mitrano, Director of IT Policy and Computer Policy & Law Program, Cornell University (April 2006)
A Wider World: Youth, Privacy, and Social Networking Technologies, by Tracy Mitrano, *Educause Review* Vol. 41, No. 6 (Nov./Dec. 2006)
Ann Cavoukian, Ph.D, Information and Privacy Commissioner of Ontario, *How to Protect Your Privacy on Facebook*, www.ipc.on.ca
Facebook's Tracking of User Activity Riles Privacy Advocates, Members, by Vauhini Vara for *The Wall Street Journal Online* at D8, November 21, 2007, <http://online.wsj.com/public/article/SB119560466428899897.html>
New Facebook Ad Techniques Raise Privacy Concerns, by Heather Havenstein for *Computerworld*, (Nov. 10, 2007, <http://www.pcworld.com/printable/article/id,139494/printable.html>)

www.CyberStreetSmart.org
www.ftc.gov/bcp/menus/consumer/tech/privacy.shtm
www.onguardonline.gov
www.MySpace.com
www.facebook.com
www.connectsafely.org (formerly www.blogsafety.com)
www.netSMARTz.org
www.webwisekids.org
www.staysafeonline.org (National Cyber Security Alliance)
www.tcs.cybertipline.com
www.iKeepSafe.org
www.look-both-ways.com
www.xblock.isafe.org
www.wiredsafety.org
www.wiredkids.org

Sponsors

Intel Corporation
IAPP
Google
Microsoft
Quintiles Transnational Corp.
Womble, Carlyle, Sandridge & Rice

Creative Commons License

This work is licensed under the Creative Commons Attribution 3.0 Unported License. To view a copy of this license, visit <http://creativecommons.org/licenses/by/3.0/>
Or send a letter to Creative Commons, 171 Second Street, Suite 300, San Francisco, California, 94105, USA.

Any use of these materials requires attribution to the IAPP and Intel.