Published on *Privacy Rights Clearinghouse* (https://www.privacyrights.org)

Social Networking Privacy: How to be Safe, Secure and Social [1]

Posted Jun 01 2010
Revised Dec 01 2017

1. What does this guide cover?

This guide discusses some of the privacy and security implications of social networks and offer some general advice for taking steps to protect your privacy online.

2. What information are you sharing when you use social networks?

Social networks come in many shapes and sizes, most sharing similar features but designed to offer a different kind of service (and, of course, some social networks may change focus and features over time). Generally, the type of information that you can share on a social network includes:

- **Personal networks**: Most social networks allow users to create detailed online profiles and connect with other users in some way. This may involve users sharing information with other approved users, such as one's gender, age, familial information, interests, educational background and employment.
- **Status updates**: Similarly, most social networks allow users to post short status updates in order to communicate with other users quickly. Though there may be privacy settings to restrict access to status updates, these networks are frequently designed to broadcast information quickly and publicly.
- **Location Information**: Some social networks and platforms are designed to broadcast one's real-time location, either as public information or as an update viewable to authorized contacts. This might allow users to "check in" to a local event or business, or share one's location with certain contacts on their network.
- **Shared Web and User Content.** Many social networks platforms also encourage users to share content, such as music, photographs, videos and links to other webpages.

Predictably, all of this sharing reveals information about you, including meta-data and contextual information you may not even be aware of. By sharing this information online you may be providing enough information to allow advertisers to track you or hackers to take advantage of your online identity -- so it's crucially important to be aware of what information is given up and be conscious of what choices you can make to protect your privacy.

3. How may your social networking information be used and shared?

What information can be gleaned from the that which you share and post publicly, and what information can be gathered through electronic tracking and profile building around your social network use.

Publicly available information
Every social network allows you to post some information that is completely publicly accessible. This can be anything from your username to individual posts, to your entire account. These kind of "public" posts are not blocked behind any kind of access restriction. Anyone, including strangers, can view whatever is posted as "public." However, there may be other data that you share publicly without realizing it, and there are less obvious ways that your information may be treated as public without your

permission, including:

- Certain information may be publicly visible by default. In some situations, a user may be able to change the privacy settings to make the information "private" -- so that only approved users can view it. Other information must remain public; the user does not have an option to restrict access to it (frequently such information includes your account name).
- A social network can change its privacy policy at any time without a user's permission. Content that was posted with restrictive privacy settings may become visible when a privacy policy is altered.
- Approved contacts (people on your "Friends list" or people that "follow" you) may copy and repost information – including photos or personal information – without a user's permission, potentially bypassing privacy settings.
- Third-party applications that have been granted access may be able to view information that a user or a user's contacts post privately.
- Social networks themselves do not necessarily guarantee the security of the information that has been uploaded to a profile, even when those posts are set to be private. While security flaws and breaches are usually quickly fixed, there is great potential for taking advantage of leaked information.

Advertising

Your own publicly posted content isn't the only way that you can be tracked, and advertisers are very interested in the information that can be gathered by tracking a user's actions online. Some of the purposes of analysis may include:

- Tracking which websites a user has viewed and tracking movement from one website to another.
- Storing information associated with specific websites (such as items in a shopping cart).Building a profile around a user for the purpose of targeting advertisements.
- Analyzing aggregated data for marketing purposes

Behavioral advertising is the term used to describe the practice of tailoring advertisements to an individual's personal interests. Social networks that provide their services without user fees make a profit by selling advertising. This is often done through behavioral advertising, also known as targeting.

This practice is appealing to marketers because targeted advertisements are more likely to result in a purchase by a viewer than comparable non-targeted advertisements. They are valuable to social networks as they can be sold at a higher price than regular ads.

Despite the value the practice brings to social networks and advertisers, there are several concerns regarding behavioral advertising:

- You may not be aware that data is associated with their profiles.
- You may not be able to view all of the data associated with your profiles and have inaccuracies corrected.
- There are no maximum retention periods on data and no security requirements for the retention of data, leaving it susceptible to hackers and security risks.

Read more about behavioral advertising in PRC's Guide, *Online Privacy: Using the Internet Safely [2]*.

Third-party applications

Within the context of social networking, "third-party applications" are programs that interact with a social network without actually being part of that social network. These applications take many forms but some typical and popular forms include games that you may play with contacts, online polls or quizzes, or third party interfaces with the social network. To make these applications useful, social networks may allow developers automatic access to public information of users, and may even access some private information, when a user grants the application permission. Considering the value of behavioral advertising, it's easy to see why many third party applications themselves include tracking capabilities, to sell user information to advertisers.

The issue is that you may grant an application access to your profile without realizing the extent of the permissions being granted. Users may also mistakenly assume that third-party applications are held to the same standards as the primary social network. There are, of course, also rogue applications, which do not follow the policies and terms that govern applications.

Some facts to keep in mind when considering using third-party applications:

- They may not be covered by the social network's privacy policy. Most social networks do not take responsibility for the third-party applications that interact with their sites
- They may not be guaranteed to be secure.
- They may gain access to more information than is necessary to perform their functions.

- They may contain malware designed to attack the user's computer.
- Third-party developers may report users' actions back to the social networking platform.
- A social network may have agreements with certain websites and applications that allow them access to public information of all users of the social network.

As a general rule, use caution when using third-party applications. Remember that it is difficult to control what information they are gathering, how they might use it, and who they will share it with.

Government and law enforcement access
Law enforcement and government officials can monitor social networks for valuable information.

Law enforcement agencies can and do monitor social networks for illegal activity. During an investigation, law enforcement will often turn to a suspect's social network profiles to glean any information that they can.

Though each social network has adopted its own procedures for dealing with requests from law enforcement agencies, it's important to keep in mind that the degree to which these sites cooperate, or don't cooperate, with law enforcement may not be fully explained in the privacy policy.

Of course, information on social networking sites has been used as evidence during criminal and civil trials. This includes divorce trials, child custody battles, insurance lawsuits, criminal trials and cases brought by university police against students for inappropriate behavior or underage drinking, to name a few. Be aware that information entered as evidence in a court case could potentially become part of a public record. Read more about public records in PRC's Guide, *Government Records and Your Privacy [3].*

Credit
Creditors may mine social networking sites, including Facebook and LinkedIn, to supplement the information they gather from traditional credit reports. By supplementing credit reports with data from social networks, creditors claim that they may be able to offer loans to consumer who may not qualify under traditional underwriting methods.

Employment
Potential employers are generally permitted to use whatever information they can gather about an applicant in making a hiring decision. Although there are legal risks, including possible violation of antidiscrimination and privacy laws, employers are increasingly turning to social media to inform their decisions. It's is important to know what information can be seen by non-contacts and to consider what kind of conclusions might be drawn from it.

Though illegal, potential employers might discriminate based on information available from profile pictures and other easily available information on one's social networking profile. A 2013 Carnegie Mellon University Experiment [4] found that between 10% and 30% of U.S. firms searched job candidates' social media pages and, in certain states, job candidates whose public Facebook profiles indicated they were Muslim were less likely to be called for interviews than Christians. Be aware of revealing even basic information such as:

- Age
- Gender
- Race
- Disability
- Sexual orientation
- Political affiliations
- Other groups and contacts

The Fair Credit Reporting Act (FCRA) [5] is a law that not only regulates credit reports but also sets national standards for employment screening and background checks. It sets limits on what information employers can get from background checks and how they can use that information (see PRC's Guide,). However, the FCRA only applies to employers using third-party screening companies. Information that an employer gathers independently, including from informal Internet searches, is not covered by the FCRA.

Employers frequently monitor what employees post on social networking sites. In fact, many companies have social media policies that limit what you can and cannot post on social networking sites about your employer, and hire third-party companies to monitor online employee activity for them.

Some states have laws that prohibit employers from disciplining an employee based on off-duty activity on social networking

sites, unless the activity can be shown to damage the company in some way. In general, posts that are work-related have the potential to cause the company damage.

The National Labor Relations Board (NLRB) [6] has issued a number of rulings and recommendations involving questions about employer social media policies. The NLRB has indicated that these cases are extremely fact-specific. It has provided the following general guidance, however:

- Employer policies should not be so sweeping that they prohibit the kinds of activity protected by federal labor law, such as the discussion of wages or working conditions among employees.
- An employee's comments on social media are generally not protected if they are mere gripes not made in relation to group activity among employees.

4.Is anonymity an option on social networking sites?

Many users of social networks take precautions to mask their real identities, using fake names or pseudonyms in place of their real identity. Achieving true anonymity is easier said than done, and may in fact be impossible. Besides the fact that using a fake name is almost always a violation of the social network's terms and conditions, taking such steps can provide you with a false sense of security and privacy.

It is incredibly difficult to truly separate online and off-line identities. You can divulge identifying information through status updates, group memberships, photographs, friend networks and other indicators. Especially if you are using your pseudonym account to connect to friends and services linked to your real identity, any anonymity is limited, at best. There is still a high likelihood that you can be re-identified and tracked by bad actors and advertisers alike.

You can read more about anonymity and de-anonymization/reidentificaiton issues:

- Arvind Narayanan and Vitaly Shmatikov's paper, De-anonymizing Social Networks [7]
- The Electronic Frontier Foundation's Anonymity page [8]

5. Privacy policies

The vast majority of people skip over the privacy policy when joining a social network. However, users can glean a lot of useful information by reviewing a privacy policy before signing up for service. A social network's privacy policy will explain how the social network will collect and use information about people who visit the site.

When reviewing a privacy policy, remember:

- Privacy policies can change – sometimes dramatically-- after a user creates an account.
- Terms of service may have information just as important as the privacy policy, so always review those as well.
- The privacy policy only covers the social network. It does not, for example, cover third-party applications that interact with the website.

Also, try seeing what others have said about the policy. A simple Internet search could turn up thoughtful analysis of the policy, especially if the social network has been in the news. Read the California Attorney General's guide on reading and

understanding privacy policies [9] for more detailed information.

6. Fraud on social networks

Criminals frequently use social networks to connect with potential victims. This section discusses some of the typical scams and methods used to defraud consumers on social networks. Fraud may involve more than one of the techniques described below.

Identity theft

Identity thieves often turn to social networks to gather information about potential victims, who all too frequently volunteer enough information in public posts to allow a criminal to impersonate them online. In 2009, for example, researchers at Carnegie University Mellon published a study [10] showing that it is possible to predict most and sometimes all of an individual's 9-digit Social Security number using information gleaned from social networks and online databases.

Information often targeted by identity thieves includes:

- Email addresses and Passwords
- Bank account information and Credit card numbers
- Contacts
- Access to the user's device without their consent (for example, through malware)
- Social Security numbers

Some fraud techniques to watch out for include:

- Illegitimate third-party applications. These rogue applications may appear similar to other third-party applications but are designed specifically to gather information. This information may be sold to marketers but could also be useful in committing identity theft. These applications may appear as games, quizzes or questionnaires in the format of "What Kind of Famous Person Are You?"
- False connection requests. Scammers may create fake accounts on social networks and then solicit others to connect with them. These fake accounts may use the names of real people, including acquaintances, or may be entirely imaginary. Once the connection request is accepted, a scammer may be able to see restricted and private information on a user's profile.

If you believe you may be the victim of identity theft, and to learn more about protecting yourself from identity theft in general by reading PRC's Guide, *How to Reduce Your Risk of Identity Theft [11]*.

Malware
Malware (malicious software) is a term that describes a wide range of programs that install on a user's computer or smartphone, often through the use of trickery. Malware can spread quickly on a social network, infecting the computer of a user and then spreading to his or her contacts. This is because the malware may appear to come from a trusted contact, and as a result users are more likely to click on links and/or download malicious programs.

Some common techniques used in spreading malware include:

- Shortened URLs, particularly on status update networks or newsfeeds. These may lead the user to download a virus or visit a website that will attempt to load malware on a user's computer.
- Messages that appear to be from trusted contacts that encourage a user to click on a link, view a video or download a file.
- An email appearing to be from the social network itself, asking for information or requesting a user click on a link.
- Third-party applications that infect computers with malicious software and spread it to contacts.
- Fake security alerts – applications that pose as virus protection software and inform the user that his or her security software is out-of-date or a threat has been detected.

Social Engineering
Often the most effective fraud techniques are those that rely on exploiting the user's trust or tricking them through "social engineering [12]." There are a variety of social engineering techniques that trick users into disclosing sensitive information. This section describes a few of the well-known techniques.

- Phishing attacks are when emails, instant messages or other messages claiming to be from a trusted source ask for information. For example, an email may appear to be from a bank and could direct a user to enter a password at a fake login page, or tell a user to call a phone number or risk having their account closed.
- Spear phishing is a type of more targeted phishing attack, that appears to be from a colleague, employer or friend and are directed to a specific individual. Spear phishing can be even more difficult to detect and avoid then phishing, because the messages have been catered to you, individually. For tips on how to spot and avoid phishing attacks, see OnGuard Online's Phishing page [13].
- Misleading solicitations. A social network might use social engineering to make people feel obligated to join. This often occurs when one person joins and (often inadvertently) provides the social network with access to his or her contact list. The social network then sends out emails to all of his or her contacts, often implying they are from the individual who joined. The recipient may believe this is a personal invitation from the user and feel obligated to join the network, giving out his or her information and perhaps perpetuating the solicitations.
- Hijacked accounts. A legitimate account may be taken over by an identity thief or malware for the purpose of fraud such as posting spam, sending out malware, stealing the private data of contacts or even soliciting contacts to send money A user may not realize his or her account has been hijacked for quite some time.

7. Tips

There are many ways that information on social networks can be used for purposes other than what the user intended. Below are some practical tips to help users minimize the privacy risks when using social networks. Be aware that these tips are not 100% effective. Any time you choose to engage with social networking sites, you are taking certain risks. Common sense, caution and skepticism are some of the strongest tools you have to protect yourself.

When registering an account:

- Use a strong password different from the passwords you use to access other sites. Ideally, use a password manager to generate and store your passwords.
- If you are asked to provide security questions, use information that others would not know about you, or, even better, don't use accurate information at all. If you are using a password manager, record the false questions and answers and refer to your password manager if you need to recover your account.
- Consider creating a new email address to use only with our social media profile(s).
- Provide the minimum amount of personal information necessary, or that you feel comfortable providing.
- Review the privacy policy and terms of service.
- During the registration process, social networks often solicit you to provide an email account password so that they can access your address book. If you consider using this feature, make sure to read all terms so that you understand what will be done with this information.

General privacy tips for using social networks

- Become familiar with the privacy settings available on any social network you use, and review your privacy settings frequently. On Facebook, for example, you may want to make sure that your default privacy setting is "Friends Only". Alternatively, use the "Custom" setting and configure the setting to achieve maximum privacy.
- Be careful sharing your birthday, age, or place of birth. This information could be useful to identity thieves and to data mining companies. If you do consider posting your birthday, age or place of birth, restrict who has access to this information using the site's privacy settings.
- Try to stay aware of changes to a social network's terms of service and privacy policy. Consider subscribing to an RSS feed for (or following) Tosback [14], a project of the Electronic Frontier Foundation [15], to track changes in website policies (which covers some, but not all social networks).
- Don't be afraid to un-tag photos of yourself and ask to have content removed.
- Consider using an ad-blocker and/or a script-blocker. This may cause some websites to not function, but it will help prevent tracking and malware – both while you're using your social network and browsing the web more generally.
- Be careful when posting any sort of location or using geo-tagging features.
- Use caution when using third-party applications. For the highest level of safety and privacy, avoid them completely. If you consider using one, review the privacy policy and terms of service for the application.
- If you receive a request to connect with someone and recognize the name, verify the account holder's identity before accepting the request. Consider calling the individual, sending an email to his or her personal account or even asking a question only your contact would be able to answer.
- If you receive a connection request from a stranger, the safest thing to do is to reject the request. If you decide to accept the request, use privacy settings to limit what information is viewable to the stranger and be cautious of posting personal information to your account, such as your current location as well as personally identifiable information.
- Take additional precautions if you are the victim of stalking, harassment or domestic violence.
- Consider pruning your "friends" list on a regular basis. It's easy to forget who you've connected to over time, and therefore who you are sharing information with.
- Be sure to log off from social networking sites when you no longer need to be connected. This can reduce the amount of tracking of your web surfing and will help prevent strangers from infiltrating your account.

Source URL (modified on April 9, 2018): https://www.privacyrights.org/consumer-guides/social-networking-privacy-how-be-safe-secure-and-social

Links
[1] https://www.privacyrights.org/consumer-guides/social-networking-privacy-how-be-safe-secure-and-social
[2] https://www.privacyrights.org/consumer-guides/online-privacy-using-internet-safely
[3] https://www.privacyrights.org/consumer-guides/government-records-and-your-privacy
[4] https://www.wsj.com/articles/bosses-may-use-social-media-to-discriminate-against-job-seekers-1384979412
[5] https://www.ecfr.gov/cgi-bin/text-idx?SID=2b1fab8de5438fc52f2a326fc6592874&mc=true&tpl=/ecfrbrowse/Title16/16CIsubchapF.tpl

[6] https://www.nlrb.gov/news-outreach/fact-sheets/nlrb-and-social-media
[7] http://randomwalker.info/social-networks/Conclusion.html
[8] http://w2.eff.org/Privacy/Anonymity/
[9] http://oag.ca.gov/privacy/facts/online-privacy/privacy-policy
[10] http://www.pnas.org/content/early/2009/07/02/0904891106.full.pdf+html
[11] https://www.privacyrights.org/consumer-guides/how-reduce-your-risk-identity-theft
[12] https://www.social-engineer.org/social-engineering/social-engineering-infographic/
[13] http://www.onguardonline.gov/articles/0003-phishing
[14] https://tosback.org/
[15] https://www.eff.org/