

Social Networking and Privacy

by Dillon Friedman and Angela Orebaugh



The Internet is arguably the most significant invention of the modern age. Every dispute or argument can now be resolved simply by entering a few related keywords into a user's preferred search engine. Over the last few years, access to information has been augmented by an explosion of user-generated content, or what is more commonly referred to as "social media." People profess having expertise (real or imagined) on a topic through wiki pages, discuss important issues through their blogs, and listen to others on their favorite podcasts.

Social networking has also worked its way into the lives of millions of people. It has become nearly impossible to go online and not encounter some form of social networking. Platforms such as Facebook, Google+, LinkedIn, and Twitter all appeal to the human desire for inclusion, connectedness, knowledge, and/or validation in different ways. They also offer an innovative way to share information with a massive audience. This popularity, however, has captured the attention of many government agencies and consumer-advocacy groups as these services have opened their users up to a multitude of privacy issues.

Facebook versus Google+

When people think of social networking, they often think of Facebook. According to Facebook's Statistics page, people

spend over 700 billion minutes per month on Facebook, and 50% of Facebook's 800 million active users log on to the site in a given day. [1] To join and interact on Facebook, users create profiles replete with information such as their education, employment history, music and movie taste, and date of birth. Users then create connections with friends by submitting a Friend Request, which that friend must approve, to share content between them. By default, some content, such as profile information, is shared publicly with other Facebook users. In fact, a person's profile will automatically display in search-engine results if their name is entered unless the user specifically changes their Privacy Settings.

Google+ launched in the summer of 2011, creating strong competition for Facebook in the social networking arena. Users create "Circles" and designate what data may be viewed by members of these groups. They then assign their contacts to different Circles based on their familiarity or comfort level with the person, which greatly facilitates how information is disseminated. Google+ marks Google's third attempt to enter the social networking arena after Google Wave and Google Buzz ended in early failures. Like these first two attempts, Google+ is now struggling as well. Despite reaching 25 million users in its first month and being lauded for its improved privacy

protections, user posts to Google+ dropped off 42% in the fall of 2011. [2]

The original differences between Facebook and Google+ privacy platforms illustrate the biggest puzzle for individuals and social media firms alike: opt-in versus opt-out. The latter approach satisfies these firms' desire to aggregate as much information as possible, which they can then sell to marketing and analytics firms interested in improving advertising by targeting specific groups. Firms such as Facebook that rely on this as a primary revenue stream assume that all information posted is intended to be made public unless the user specifically designates otherwise (opts out). An effective opt-out system requires two things: first, that the site in question provide reasonable privacy controls for its users and, second, that the site's users understand how the controls work. While most social media sites have implemented extensive privacy controls to maintain public trust, in many cases, the controls are either too complicated or the users fail to fully understand the impact of every mouse click. Because the average user has no idea how exposed their information is and what the larger impact of that exposure could be, many governing agencies and consumer-advocacy groups support a system under which users can specifically designate how and when



their information is shared, or opt-in.

Social-Networking Regulatory Issues

The opt-in versus opt-out issue has been complicated by the differing policies in two of the largest Internet-user markets, the United States and the European Union. The European Union, whose approach has been colored by conflicts like World Wars I and II during which information was collected to persecute groups of people, has adopted a number of policies, including Directive 95/46/EC and Directive 2002/58, establishing that data collection must be opted into to properly preserve the right to privacy. As a result of this view of privacy as a human right, many companies have encountered significant pushback, most notably from Germany, for perceived privacy issues. For example, over the last 2 years German courts have launched investigations into various functions on Facebook, such as the *Like* button and facial-recognition technology. [4, 5] Although Google+'s level of success in Europe is unknown at this time, its opt-in structure suggests that it will garner less scrutiny from European governments.

The United States, by contrast, takes what is referred to as a "sectoral" approach to data-protection legislation. Privacy legislation in the United States is adopted generally when certain issues arise or developments in certain

industries require it, though the individual's right to privacy has been ruled as implicit in the First Amendment. Generally speaking, the Federal Trade Commission is responsible for enforcing privacy statutes, but depending on the industry of the firm in question, enforcement can also fall to the Department of Transportation, the Department of Health and Human Services, the Federal Reserve, or the Comptroller of the Currency.

To date, the social networking industry has not been the subject of any one discrete piece of legislation, though several have been deemed relevant by policymakers. Many of the founders of today's popular social networking sites had barely been born when the Electronic Communications Privacy Act of 1986 (ECPA) was passed, long before the Internet became as ubiquitous as it is today. Because ECPA's privacy provisions have not been updated since 1986, the legislation allows law enforcement and/or the government to access any information stored on a third-party server with nothing more than a subpoena. By contrast, under the federal Wiretap Act, a law-enforcement agency wanting to tap a phone must have a warrant signed by a judge, with few exceptions. Frequent lobbying attempts to strengthen the requirements for accessing information stored on a

third-party server have thus far proven unsuccessful. [6]

Another piece of legislation related to social networking is the Children's Online Privacy Protection Act of 1998 (COPPA), which delineates how a commercial Web site directed at children under 13 years of age may collect and use data. COPPA also limits the information an operator can provide to advertisers without parental consent. Given the indiscriminate data-collection practices of many social networking sites, several, including Facebook, MySpace, and Twitter, do not allow children under the age of 13 to join their sites, and Google+ is currently only available to users 18 and over. It bears mentioning that Facebook was recently called to testify on Capitol Hill regarding how it protects children online.

Beyond legislation, social networking sites have proven responsive to the free market. For example, in August 2011, LinkedIn tried to implement "social ads," a new form of advertising that attached users' names and pictures to product endorsements. The blog post notifying LinkedIn users of this new development generated no substantial response, but when users actually saw the ads, the outcry was swift. Within a week, Ryan Roslansky, LinkedIn's Director of Product Management, published a blog post indicating that the company would no longer make use of users' names and

photos in ads. Instead, social ads now only inform users when a person in their network recommends a product or follows a company, however, LinkedIn users are still automatically opted-in to this social advertising. Users may opt out by going to *Settings > Account > Manage Social Advertising* and unchecking the *Linked In may use my name, photo in social advertising* check box.

General Social-Networking Privacy Recommendations

When using social networking services, it is important to understand the various privacy settings, select the most secure options, and periodically check for changes to options and settings. The following general privacy guidelines apply to social networking, regardless of platform—

- ▶ **Use your brain**—Although it sounds like common sense, the most important privacy feature is to think before you post. Status updates, photos, and comments can unintentionally reveal personal information. Do not include information that could give away personal or sensitive information about yourself or others. For example, some users do not reveal the names of their children, pets, or address online. It is also best to avoid the often-circulated surveys and questionnaires that request personal information.
- ▶ **Private may not be private**—Treat private messaging the same as public, as you never know when you are mistakenly cross-posting, or when messages could be leaked to the public. Also, many companies still retain records of private messages, even if they are not reviewing the content.
- ▶ **Applications do more than you think**—Consider the applications that you install and the information to which they request access, and remove applications that you are no longer using.

- ▶ **People are watching**—Be mindful of geo-location services such as Foursquare and built in check-in services on Facebook and other platforms. These services reveal your exact location, let criminals know you are not home, and could also reveal other information about your personal preferences.

Facebook Privacy Recommendations

Competition with Google+ has forced Facebook to improve how it addresses users' privacy concerns. Facebook created a Director of Privacy position and appointed Erin Egan, a privacy and data-security lawyer formerly with Covington and Burling. Starting in August 2011, Facebook began allowing users more direct control over who can access uploaded content. Facebook's List feature, with similar advantages as Google+ Circles, and "inline" privacy settings for posts, pictures, and status updates, have greatly simplified how Facebook users protect their information. Facebook users should be aware of the following privacy settings and best practices—

- ▶ **Friend Lists**—Facebook allows you to create custom lists of people to share content with and to use in sharing different aspects of your profile. You may configure these lists to be as simple as Friends, Family, and Professional, or you may get more detailed with Book Club, Work Friends, High School Friends, *etc.* Use the various lists to enable the most granular privacy settings.
- ▶ **Tagging**—By default, your friends can tag you in posts and photos, which will automatically show up on your profile. For privacy, enable Profile Review in the Tags section of the Privacy Settings to manually review and approve posts (including photos and videos) that you are tagged in before they appear on your profile. Remember that the posts and photos tagged with your name will still show up

on the person's wall who posted it, but not your wall until you approve it. If you remove the tag you can also send a message to the user who tagged you, requesting that they remove the post or photo, and you can also block that person entirely. Also note that any post or photo in which you tag someone is viewable by the person you tagged.

Customize the Tag Review feature in Privacy settings to approve or reject tags that friends post.

- ▶ **Search Visibility**—By default, some of your Facebook profile information will show up in Web searches. You can remove your profile from being displayed in Web search results by disabling Public search through *Privacy Settings > Apps, Games, and Websites > Public Search*.
- ▶ **Friend Visibility**—Your Friend List is visible to anyone by default unless you disable this feature. To make changes, choose *Edit Profile > Friends and Family*. You will see the drop-down option next to Friends that allows you to configure who can see your Friend List. This can be set to public, only you, friends, or any other custom list you have created.
- ▶ **Application Access**—Some applications have optional access that can be revoked. For example, many popular applications have a control that allows access to your data at any time, even when you are not using the application. This control option can be removed. Also, when reviewing applications, there are privacy settings for each application to limit who can see posts and activity from that application. Finally, remove applications you are no longer using.
- ▶ **Inline Privacy Controls for Content**—Take advantage of the individual privacy settings. You can choose specific lists for sharing posts, photo albums, individual

photos, and various elements of your profile. Each of these pieces of content has a drop-down box next to it for inline privacy controls. You can also use the *View As...* button on your profile to see how your profile is visible to others.

Google+ Privacy Recommendations

Google+'s inline controls and Circles give it a competitive advantage in social-networking privacy. For even more information in Google+ privacy, you can access the Privacy Center from the Profile and Privacy section of your Account Settings page. Privacy Center centralizes privacy features for many of Google's products and services. One significant difference with Google+ is that anyone using the service can add you to his or her circles; there is no request process as with Facebook. But just because someone has added you does not mean they can see any of your information if you are using the inline controls appropriately, although they, and everyone else, will see anything you designate as Public. Google+ users should be aware of the following privacy settings and best practices—

- ▶ **Circles**—Google+ privacy is built on Circles—groups of people you share content with. The names of your Circles and those you add to them are visible only to you. Build Circles such as friends, family, and professional colleagues to enable the granular privacy capabilities.
- ▶ **Profile Privacy**—When editing your profile, each element has a drop-down menu associated with it to allow you to share that element with specific Circles. Your Full Name is the only required element in the profile, and is visible to anyone on the Web. You can customize your privacy for each element to reflect what you are comfortable sharing. You can also use the *View Profile As...* check box on your profile to see how your profile is visible to others.

- ▶ **Profile Discovery**—By default, your name and any other fields you make public in your profile are searchable on the Web. If you are concerned about your profile showing up in search engines, you can disable this by editing the Profile Discovery in your Profile and clearing the Help others discover my profile in search results check box. This will block search engines from indexing your profile.
- ▶ **Circle Visibility**—By default, anyone on the Web can see whom you have added to your Circles (but not which specific Circle) and who has added you to their Circles. To change this, on the left side of your profile, click the *Change who is visible here* link. You can choose to hide both of these elements from everyone, or to make them available only to certain Circles.
- ▶ **Geo Location**—By default, Google+ shows geo-location tagging for photos. You can limit the use of geo-tagging by disabling photo geo-tagging in the Google+ section of your Account Settings page. Clear the *Show photo geo-location information in newly uploaded albums and photos* check box.
- ▶ **Tagging**—You can disable or pre-approve individuals or Circles to tag you in photos and link to your profile. You can also limit the use of photo tagging by selecting or removing those individuals or Circles that you automatically approve to link to your profile by editing the Photos permissions in the Google+ section of your Account Settings page, or by selecting the Photos tab while editing your profile.
- ▶ **Post Privacy**—You can use the inline privacy settings to select individuals and Circles with which to share any post you write. For each new post, Google+ remembers the individuals or Circles you shared with last, so it is wise to

check this setting each time you post. You can also disable comments and lock the post from sharing before submitting. Note that your comments on other people's posts are shared with the same privacy as that post; therefore, if you...if you comment on a publicly shared post, your comment will be public and searchable on the Web. Check to see if the post privacy setting is Limited or Public to gauge who will be able to read it.

- ▶ **Understand +1's**—The Google +1 feature allows you to share information publicly, but is also recorded for Google and its partners. This information may also appear to others as an annotation with your profile name and photo in Google services and on the Web. You can view the list of items that you have designated as +1 on the +1 tab of your profile. You can also remove items from the list. While editing your profile, clicking the +1 tab will allow you the option to hide the tab from others viewing your profile.

The long-term significance of online social networking remains to be seen as technological advancements are continuously revolutionizing the way we interact. We have only just begun to understand how these new means of collaboration and communication will shape our daily lives or even the world. Events like the recent uprisings in Iran and Egypt demonstrate how social networking platforms are being used to challenge authoritarianism, while the London riots in the summer of 2011 highlight the dangers of an idle population empowered by Twitter and Blackberry Messenger. The next generation, which will have grown up with the likes of Facebook and Google+, will face the task of determining how these technologies evolve and affect the right to privacy.

▷ ▷ *continued on page 50*

USSTRATCOM Cyber and Space Symposium



The United States Strategic Command (USSTRATCOM) Cyber and Space Symposium took place November 15-17, 2011, in Omaha, NE. The conference provided an opportunity for leaders to discuss cyber innovations and ways for industry and government organizations to more effectively collaborate. It featured speakers from across the Department of Defense, U.S. government, industry, academia, and allied governments.

Some of the featured speakers included General C. Robert Kehler, USSTRATCOM Commander; General

Keith Alexander, U.S. Cyber Command Commander; Admiral James Winnefeld, Jr., Vice Chairman of the Joint Chiefs of Staff; and The Honorable Howard Schmidt, White House Cybersecurity Coordinator.

This conference featured 16 different panel discussions that focused on a variety of critical information assurance (IA) and cybersecurity (CS) topics. These topics included managing risk across networks; international cyber issues and how to collaborate across borders; space and cyber solutions; and industry innovations in both cyber and

space. The symposium also held academic sessions for high school students to interact with IA/CS professionals, learn more about the challenges that the field will face in the future, and gain insight into the opportunities they will have to contribute to the advancement of IA/CS in the future. [1] ■

References

1. <http://www.afcea.org/events/stratcom/11/introduction.asp>

▷ continued from page 43

SOCIAL NETWORKING AND PRIVACY

About the Authors

Dillon Friedman | currently works in privacy and information management and is focused on privacy and security issues concerning mobile and wireless technology as well as social media. Mr. Friedman holds a B.A. from the University of San Diego. He can be contacted at friedman_dillon@bah.com.

Angela Orebaugh | is a technologist, researcher, and cybersecurity executive, who is passionate about helping clients embrace tomorrow's technology today. Ms. Orebaugh was recently selected as Booz Allen Hamilton's first and

currently only Cyber Fellow, a distinction reserved for an elite group of the firm's most noted authorities. She evangelizes social media and mobile technologies by highlighting the powerful ways in which these technologies are changing business, communications, and information sharing. Ms. Orebaugh is also the Information Assurance Technology Analysis Center Director of Research and Academic Integration. She is an international author and invited speaker for technology and security events. Follow her on Twitter @AngelaOrebaugh and connect with her on Google+ at <http://gplus.to/angelaorebaugh>. She can be contacted at iatac@dtic.com.

References

1. <https://www.facebook.com/press/info.php?statistics> [2]http://www.boston.com/business/technology/articles/2011/09/15/will_google_strike_out_of_the_social_networking_market/
2. <http://www.bbc.co.uk/news/technology-14859813>
3. <http://www.pcmag.com/article2/0,2817,2390440,00.asp>
4. <http://notwithoutawarrant.com/>