

Social Network Privacy

Overcoming Facebook policies that put users at risk

By CW3 Elbert Peak

Facing the Facebook Privacy Dilemma

On-line social networking has benefits but also risks to be considered when using such sites as Facebook.

Internet privacy threats are a challenge that is impossible to completely mitigate on every social network, but there are steps one can take to significantly reduce the risks.

The Rise of Facebook

Facebook is one of the largest web sites in the world. The site was started in 2004 by Mark Zuckerberg when he was an undergraduate student at Harvard. The site grew rapidly to include hundreds of millions of users.

Since September 2006, anyone over the age of 13 with a valid e-mail address can join Facebook as a user. Users can add friends and send messages and announcements, and update their personal profiles to notify friends about themselves. Social networking giant Facebook registered its 500 millionth member, the firm announced in July 2009.

Its millions of users around the world have reason to limit visibility of their personal information from the total World Wide Web but still want to be able to share that information with trusted contacts. Facebook became a huge success on that premise and ought to be able to continue thriving without doing an about face on privacy.

Humans are social beings and most seek some engagement with others. Facebook uses a social graph, which is the global mapping of people and how they're connected. Sociologists have been studying these graphs for decades. Fa-



mously, the social networks have a Small World Property--more widely known as the Six Degrees of Separation. This is both an anecdotal and scientific observation that we all are connected to each other--no more than six people away. What is the secret? It's because this is how human networks form. Dense clusters are interconnected by shortcuts.

There is a social networking privacy premise that people have the right to control their "private space."

The argument is generally upheld that "private space" is presumptuous and a user's right to control. You have privacy to the extent you control who is allowed into your "zone of inaccessibility." Discussions about privacy revolve around the notion of access, where access means either physical proximity to a person or knowledge about that person. The lack of privacy often makes individuals vulnerable to having their behavior controlled by others. Social networking is built on the ideology of sharing information and personal data. Users share a variety of information about themselves on their Facebook profiles, including photos, contact information, and tastes in movies and books. It's meant to be social.

(Continued on page 42)

The rise of Facebook

Active users, millions

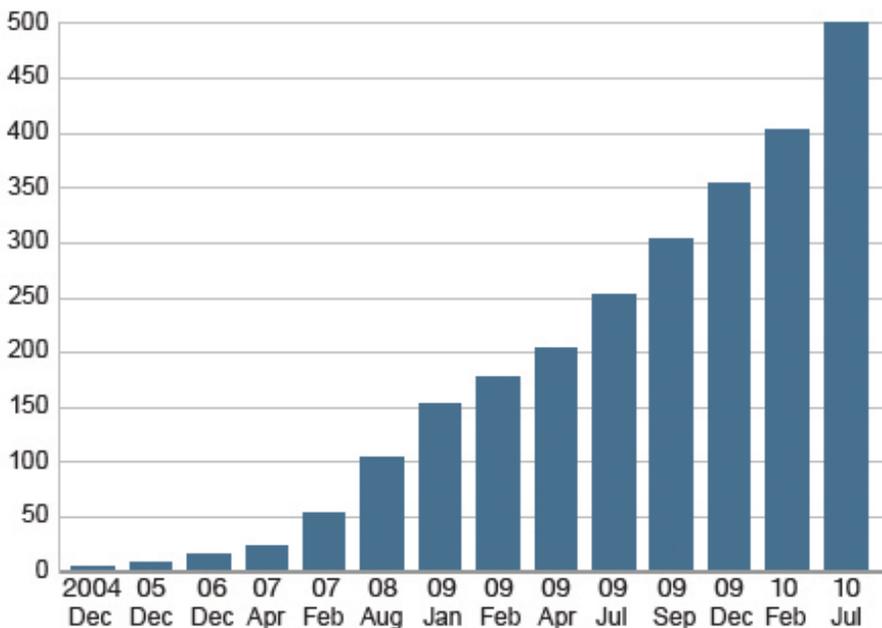


Diagram 1

(Continued from page 41)

Facebook: Threats to Privacy

End-users share a wide variety of information on Facebook, but a discussion of the privacy implications of doing so has yet to emerge widely. I examined how Facebook affects privacy, and found serious flaws in the system.

Privacy on Facebook is undermined by three principal factors: users disclose too much, Facebook does not take adequate steps to protect user privacy, and third parties are actively seeking out end-user information using Facebook.

With this much detailed information arranged uniformly and aggregated into one place, there are bound to be risks to privacy. Users may submit their data without being aware that it may be shared with advertisers. Third parties may build a database of Facebook data to sell. Intruders may steal passwords, or entire databases, from Facebook. Although many Facebook features empower users to control their private information, there are still significant shortcomings.

Facebook's privacy features give users a good deal of flexibility in who is allowed to see their information. The privacy settings page allows a user to specify who can see them in searches, which can see their profile, which can see their contact info, and which fields other users can see. In addition, the privacy settings page allows users to block specific people from seeing their profile. In the usage agreement, a user can request Facebook to not share information with third parties, though the method of specifying this is not located on the privacy settings page.

There are a number of systems changes that can be made, to give the user a reasonable perception of the level of privacy protection available, and to protect against disclosure to intruders.

Brief Technical Description of Facebook

Facebook uses server-side hypertext preprocessor scripts and applications to host and format the content available on the service. Content is stored centrally on Facebook servers. Scripts and applications at Facebook acquire, process, and filter information on-demand, and deliver it to users in real time, to a Web browser over the Internet. Users begin their Facebook session at the service's top level site, <http://www.facebook.com/>.

At the main Facebook page, a user can log in to



the service, or browse the small amount of information available to the general public. The main page of the service is simple, and does not provide any personally identifiable information or technical insight. During the login process, the service provides the user's web browser with some information, which is stored in the form of a cookie. Some of this information, such as the user's e-mail address, is written to a file so the user does not have to enter his or her e-mail at the next login.

Facebook's service creates and gives a user a unique checksum at every login, which the browser stores as a session cookie and generally does not write to a file. This checksum varies from login to login, but other parameters do not. Once logged in to the service, a user is free to interact with Facebook. The user may edit their profile, look at others' profiles, add or change their friends list or personally identifiable information, and explore the service.

The core of the Facebook platform is the open graph application programming interface, which enables read and write data to Facebook. The open graph API allows applications, pages, Websites, and other software services to add Facebook features, like the "Like" button, to their own sites. Taking actions on other sites results in those actions being shared with your friends on Facebook, and may allow friends on those sites to see what you're doing also.

Every object in the social graph has a unique ID. You can fetch data associated with an object by fetching <https://graph.facebook.com/ID>. Alternatively, people and pages with usernames can be fetched using their username as an ID. All responses are JavaScript Object Notation objects. JSON is a lightweight text-based standard designed for human readable data interchange.

It's derived from the JavaScript programming language for representing simple data structures and associative arrays, called objects.

Metadata in Facebook

Society spawns one gigantic social graph. In this graph, each one of us is a node. There is an explicit connection, if we know each other. For example, two people can be connected because they work together or because they went to school together or because they are married. Everything has an array of likes, friends, and recommendations stored within a social graph. User-contributed (or generated) metadata is the high value, structured matter that allows ads, and the overall user experience, to be more personalized. As the social Web evolves, privacy and metadata ownership issues will continue to produce friction in the system.

In effect, Facebook is building an identity graph, not just a social graph out of an individual's metadata. A key issue going forward is whether and how users become the control point for their online identities, including all the metadata that sites collect.

Aggregation of Facebook Data

Could a more sophisticated aggregation of Facebook data allow privacy to be exposed? Facebook CEO Mark Zuckerberg says he is providing "the power to share in order to make the world more open..."

Facebook's advanced search allows one to query the database of users via any of the fields in a profile. The problem is compounded by



a security hole that multiple people have discovered. The likebutton.me (<http://likebutton.me>) site created by Zachary Allia and itstrending.com (<http://itstrending.com>) site created by Matt Schlicht aggregates shared objects from Facebook's recommendation plug-ins (plug-in to make website content socially relevant) across online media web-

sites. Both show the same data just in similar interfaces, displaying what your friends are "liking" and otherwise sharing on different sites. These sites aggregate data and displays in real time feed of most shared content on Facebook (vid

(Continued on page 44)



"I realized that this is a scary privacy issue," Boves wrote. "I can find the name of pretty much every person on Facebook."

Boves said Facebook users can change their settings so they do not appear in the public directory going forward, but even people who do that now will have their information available via Boves' torrent file available on the file-sharing site Pirate Bay. There have been more than 10,000 downloads of the file.

"Once I have the name and URL of a user, I can view, by default, their picture, friends, information about them, and some other details," he wrote. "If the user has set their privacy higher, at the very least I can view their name and

(Continued from page 43)

eos, news, images, entertainment, gaming, etc). This is all possible by using publicly-shared data by users and their friends, based on each user's social graph. You must be logged into Facebook to see personalized results on these widgets.

Apparently two developers, Will Moffat and Peter Burns, (and possibly a third, James Home used for designing) built the site Youopenbook (<http://youopenbook.org>) to demonstrate how public our Facebook information really is.

One person stated online that "I'm willing to put myself out there on Facebook and other social networks and online sites, so to me, social media privacy can be a bit of an oxymoron no matter how many privacy settings I activate on Facebook."

The website Youopenbook is a demonstration of lack of privacy in Facebook.

With this site you can search public Facebook updates using Facebook's own search service. By using the Open Graph API, developers can make searches of public timeline information without logging into Facebook. Developer Timo Paloheimo did just that by creating the Open Facebook Search at <http://openfacebooksearch.com>. This website opens up new possibilities for developers to create totally new services on top of Facebook's data. Now you can embed Facebook searches to any website.

Another tool for searching public data on Facebook can be accessed at <http://zesty.ca/facebook>. This site was created by another developer, Ka-Ping Yee, using the Open Graph API. Try entering your name or e-mail address, your friends' names or e-mail addresses, or any keywords. Use the button to search for users, posts, events, groups, or pages. You might be surprised at what is publically available. Many users allow their status updates, likes, and other activity to be public without knowing. Developers are using the available documentation from Facebook to make this happen. See <http://developers.facebook.com/docs/api>.

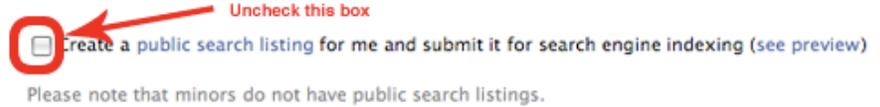
Facebook Data Found on Pirate Bay

Last summer Ron Bowes, a Canadian security consultant and Nmap developer, used a piece of code to scan Facebook profiles, collecting data not hidden by user's privacy settings.

To figure out if your name is on the list released by Bowes you can either download the file or check your settings on Facebook. To do that, click on the

Public Search Listing

Use this setting to control whether your search result is available outside of Facebook.



"Account" pull down menu on the upper right of your Facebook page and click on "Privacy Settings." Then select "Basic Directory Information" and "View Settings." If "Search for me on Facebook" is marked for "Everyone," your information might be on the list.

Avoid Facebook Account Hacks

Hackers are enticing Facebook users to install an application pitched as a "Dislike" button that jokingly notifies contacts at the social networking service "now I can dislike all of your dumb posts." Once granted permission to access a Facebook user's profile, the application pumps out spam from the account and spreads itself by inviting the person's friends to get the button, according to Sophos. Beyond tricking a user into completing a survey, and hence gaining access to your profile and the ability to spam your friends, there doesn't appear to be much about the scam that's dangerous.

Eventually, after the user completes the survey, it does redirect to FaceMod, the maker of a Facebook-based "dislike" button that takes the form of a Firefox browser plug-in. Sophos points out that the scam does not appear to have any direct connection to FaceMod.

Many of the malware applications reported spam by Facebook users have been taken down by Facebook. But still the thing to worry about is that the Facebook profile spying spam is not spreading through apps only, in fact it is spreading with the help of Facebook Events, Pages and groups too. So Facebook needs to filter out those spam pages, groups and events too.

Most of the profile spying groups, pages and app take you to a page that's completely filled with advertisements and affiliate links. Quite often they ask users to complete certain offers or surveys (see screenshot above) after which users end up passing their important information to the spammers or downloading infected files to their PC.

You will find a large number of Facebook pages, groups and apps that claim to tell users about who checked/viewed their profile. Actually they all are spam. Their sole purpose is to get a large user following by tricking people and then directing them all to pages heavily loaded with advertisements which in turn generates revenue for them. Facebook itself says that there is no way at all with which you can see/check who is visiting your Facebook profile. This is

what Facebook's recent status updates state about this rapidly growing spam.

Another attack that is trending is the clickjacking attack. This Facebook attack uses iFrames, which essentially places an invisible button over an entire web page, so that wherever the user clicks, they end up hitting the button - in this case a hidden Facebook "like" button. Many types of operations can take place from this type of attack hidden from the user, sometimes resulting in a cross-site scripting attack. Usually this type of XSS attack will bypass client-side security and malicious scripts on web pages can be executed on the end-user's computer.

Tag... You're It!

This is the classic Facebook problem. You let loose for a few hours one night and photos or videos of the moment are suddenly posted for all to view, not just your close friends who shared the moment with you. The result can be devastating. Some have been fired from work after incriminating photos/videos were posted for the boss to see. For others, randomly tagged photos/videos have ended relation-

ships. You should have to approve a tagged picture before it goes up rather than having to check periodically to see if any pictures are something you do not want posted. In which case you have to "un-tag" the photo and possibly report it.

You control who can see the photos and videos you tagged to appear on your profile. Remember, the owner of a photo can still share that photo with people who are not your friends.

If you don't want your tag to appear, remove it from the photo or video itself. This will also prevent it from appearing on your profile. The "My Photos" service allows users to upload, store and view photos.

Users can append metadata to the photographs that allows other users to see who is in the photographs, and where in the photograph they are located. These tags can be cross-linked to user profiles, and searched from a search dialog. The only recourse a user has against an unwelcome Facebook photo posted by someone else, aside from asking them to remove it, is to manually remove the metadata tag of their name, individually, from each photograph. Users may disable



others' access to their Wall, but not to the Photos feature.

Check-in Versus Tagging

So, since check-ins is also presumably mobile posts, wouldn't that also mean they exist outside a user's privacy settings? If so, this could be a big issue for Places; and defensible territory for Foursquare and Gowalla. The difference between being checked-in and being tagged can be confusing. If you're checked-in by yourself or by a friend, your presence at the location is visible to anyone that either you or your friend allows, based on your friend's and your privacy settings. Your name will show up on the location's Places page, if there is one, so everyone at the location can see that you're there. If you are tagged by a friend, your presence at the location is seen by your friends or whoever they allow to see their posts, subject to their (not your) privacy settings. Your friends' apps may be able to access information about your most recent check-in by default.

Recommended Facebook Privacy Settings

Currently the information displayed in the search profile is limited to: your profile picture, a list of your friends, a link to add you as a friend, a link to send you a message, and a list of up to approximately 20 fan pages on which you are a member. To increase your privacy settings, it is necessary to select the custom settings and modify each setting individually. If you want to

(Continued on page 46)

SEE WHO VIEWED YOUR PROFILE!!





(Continued on page 45)

have full control over who sees your profile, meaning that only people you have chosen will be able to see any part of your profile, choose "Friends only." Towards the bottom of the settings, uncheck the box that states "Let friends of people tagged in my photos and posts see them." Then click on "Apply These Settings."

Many open source tools are available for use to help alleviate these problems in Facebook settings. Developer Matt Pizzimenti, cofounder of Olark.com, created an independent and open tool (Reclaim Privacy Scanner) for scanning your Facebook privacy settings. To keep the privacy scanner up-to-date, all development will remain open and transparent. Source code is maintained at <http://github.com/mjpizz/reclaimprivacy> and uses a JavaScript file named "privacyscanner.js" about 8,167 lines of code as of today. The tool is used for scanning Facebook privacy settings and fixing unexpected privacy holes. This scanner is not fully compatible with the latest Facebook privacy settings, so be sure you check your privacy settings manually yourself. The tool can be downloaded from <http://www.reclaimprivacy.org>.

Another open source tool named SaveFace, provided by Untangle is a simple to install bookmark utility that automatically resets Facebook settings to restore your privacy. SaveFace sets your privacy settings back to Friends only, for all the following: contact information, search settings, friends' tags and comments, personal information and posts. Best of all, it's free. Untangle collects no personal information from you or your Facebook when you use this bookmark utility. SaveFace can be downloaded from <http://www3.untangle.com/saveface>.

Here are some tips for using any social network:

- Set appropriate privacy and security controls; use complex passwords; separate e-mails
- Don't install third party applications from



You can be outed, if you don't disable friends' ability to check you in



sources you don't trust

- Only accept friend requests from people you know directly
- Read and understand privacy policy and terms of service carefully
- Consider everything public; be careful what you post
- More at: <http://socialmediasecurity.com>

For a more in-depth reference on Facebook privacy settings, one should visit <http://www.wikihow.com/Manage-Facebook-Privacy-Options> and <http://www.facebook.com/fbprivacy>.

Conclusion

In an environment of growing Facebook information misuse,

Facebook would do its users a great service to explain the dangers of security breaches and outside monitoring. Until the societal norms regarding this new use of computers become well-established, Facebook could clearly state that they can provide no guarantees regarding the security of their data, and that if users make their profiles public, all information contained therein may be viewed by anyone. Ultimately, lasting change in online privacy will only come from a gradual development of common sense regarding what is appropriate to post in social networking forums. Unfortunately, this is not an easy fix.

CW3 Elbert Peak is assigned as a cyber security instructor at the School of Information Technology, Fort Gordon, Ga. He recently completed a 10 month train-the-trainer program for the new Warrant Officer 255S Information Protection Technician MOS course. Since joining the Army in 1988, CW3 Peak has worked in many areas of information technology including networking, systems administration, and information assurance. He holds a Bachelor's degree in Computer Science from University of Maryland, a Master's degree in Computer Information Systems from Florida Institute of Technology, and a Master's degree in Software Engineering from California State University, Fullerton.



Bio, family, photos, posts & relationships default: everyone

