

Another ugly reminder to check your Facebook settings — NOW!

Latest privacy brouhaha comes with a lesson we should have already learned



Duane Hoffmann / msnbc.com

Hey you! Don't be blind to your Facebook privacy settings! Adjust them now! Do it! Do as I say! Obey me!



by Helen A.S. Popkin

You know that guy who just posted the personal details of 100 million Facebook profiles in an online downloadable file? He ain't Matthew Broderick in "War Games," Keanu Reeves as "Neo" or "The Girl with the Dragon Tattoo."

Sure, the dude wrote some code to [access and aggregate user information through Facebook's directory](#), but he isn't a "cracker." He didn't even need to be a "hacker" to do it. Ron Bowes is just a security researcher who used a tool to quickly access all the profile info made readily available by Facebook users who — by either choice or chance — didn't lock it down.

If we take any lesson from this latest Facebook privacy brouhaha, it's one we should have already learned: Facebook isn't for people who don't wish to be known. Because here's the deal: Facebook has not now, nor will it ever, protect your information for you.

The thing to remember is that on Facebook, your wishes (or privacy settings, whatever) are by default, indexed for search engines. That's how Bowes was able to access and aggregate the 2.80 gigabyte file he uploaded to file-sharing website Pirate Bay. As in the Facebook statement, the information on this file "already exists in Google, Bing, other search engines, as well as on Facebook."

If users haven't properly understood and changed the default settings, information is available to be collected and aggregated by a security researcher like Bowes, or any unsavory character that may have already done the same and didn't bother mentioning it to the press.

"Facebook has been making so many changes, and every time those changes are made, the information is by default publicly available," said Nicole Ozer, technology and civil liberties policy director for the ACLU of Northern California.

"The 100 million people on that file make up one-fifth of Facebook. How many of those people haven't made a conscious choice, misunderstood a setting or even knew where to find it to change the default?" Failing to [understand and change settings](#) means people can inadvertently share private information that can be used in a way most users can't predict, Ozer says.

"How many of those 100 million users anticipated that a security researcher was going to aggregate and leak their information on a peer-to-peer sharing site?"

It's not like Facebook provides worst-case scenarios. Though, it's hardly surprising that a bunch of huge corporations may be downloading all that info posted on Pirate Bay, as [Gizmodo reported today](#).

Using a peer block-like program, the tech blog was able to identify a cavalcade of IP addresses accessing the BitTorrent data, including Disney, Church of Scientology, Halliburton, Lucasfilm, Procter & Gamble, Sega, the United Nations and [a whole heck of a lot more](#). (To be fair, it could just be some guy at work who's downloading for kicks and giggles, plus the fact that IP addresses do fluctuate.)

What's more, Facebook might very well be incapable as an organization to protect your stuff because at its very core, Facebook wants to spread your information, not protect it. They may say they will protect it, [but you should bet that they won't](#). Facebook in its very DNA is about spreading information and is repulsed by the idea of locking it down. They may say they care about privacy, but they hold their nose every time they add another privacy setting.

Spreading your information is what makes Facebook valuable to users who want to connect with others. Sharing your information with marketers who want to aggregate your personal information so they can better sell you stuff is how Facebook makes money.

Make no mistake. For all its recent grandstanding about not being in it for the money, Facebook wants to get paid.

"Facebook is in it for the money, wants to make a lot of money, is in fact fiduciarily obligated to its investors to be 'doing this for the money,' " Ryan Tate of Silicon Alley gossip blog Valley Wag [wrote in May](#). "Facebook is not a hippie collective of open-source do-gooders paid in massages, pot brownies and gratitude."

For all the recent privacy upgrades and simplified privacy settings, users are still fairly exposed. Take applications. If you haven't locked down your profile, every time your Facebook friend allows an application (FarmVille, etc.) to access his or her profile, that application is accessing your profile too.

If you're on Facebook, you need to stay on top of your privacy settings. The [Electronic Frontier Foundation, a digital advocacy group](#), is also wary of Facebook's pattern of ever-changing privacy policies. "Facebook takes one step forward, and two steps back," says EFF spokesperson Eva Galperin. "They'll start to erode the privacy of users, roll it back when there are complaints, but in the end you'll have less privacy than you did before."

Here's a nice agriculture analogy for all you FarmVille fans. You don't ask the fox to guard the henhouse. You may be able to yell at the fox and shame him long enough to make him say that he's going to protect it, but you have to remember that he will always be a fox and will do fox things and the best thing for you to do, if you care about your chickens, is to put a padlock on their pens or switch them to another damned cage.

For tips on protecting your chickens — er — privacy, check out the [EFF's settings tutorial](#) embedded in this story.

Helen A.S. Popkin rants about online privacy, then begs you to friend her on [Facebook](#) or follow her on [Twitter](#) ... because that's how she rolls.

© 2010 msnbc.com [Reprints](#)