Facebook Privacy: 5 Most Ignored Mistakes

A Consumer Reports survey of Facebook users reveals many people still ignore privacy controls and sharing risks. Do you understand the common mistakes that could bite back?

By **Thomas Claburn** ✉ InformationWeek
May 04, 2012 09:05 AM

6 Social Sites Sitting On The Cutting Edge

Facebook no longer represents that it offers privacy as a matter of policy, like some other companies do. It states outright that it will use your data. It has a Data Use Policy instead of a Privacy Policy.

But consider the dictionary definition of privacy: *1) The state or condition of being free from being observed or disturbed by other people; 2) The state of being free from public attention.* If that's your gold standard, then you cannot use Facebook or any other online service for that matter, at least not without privacy-protecting technology. Once you venture online, once you share, you're talking about something less than privacy. Online services may talk about how they respect privacy, but they should really be talking about data usage and sharing.

Facebook's privacy settings would be better referred to as sharing settings. That might encourage more people to use them. According to *Consumer Reports*, 13 million out of 150 million U.S. Facebook users don't use, or are not aware of, Facebook's privacy settings.

Consumer Reports' data comes from a survey of 2,002 online households, 1,340 of which are active on Facebook. From this limited data set, the magazine has projected nationwide Facebook usage trends. The magazine's findings reveal some surprising privacy blind spots.

1. Privacy Settings

The fact that only 13 million, or 8.6%, of U.S. Facebook users, don't use, or don't know about, Facebook's privacy settings can be seen as encouraging because it's a relatively small percentage. Its high compared to the rate of illiteracy in the United States, which is about 1% or less if you accept a very lax definition of literacy. But it's about what you'd expect if you consider functional illiteracy, which suggests some 23 million U.S. adults have very low reading skills. If you use Facebook, Facebook literacy is a must.

2. Location Sharing

Consumer Reports estimates that 4.8 million people have published posts that contain details about their whereabouts during the day. The magazine calls this "a potential tip-off to burglars." While there have been reports of burglaries linked to online posts about being away from home, you have to wonder whether other methods of location broadcasting--such as leaving home, when anyone might observe your absence without leaving an online data trail--might not present more of a risk. Even so, it's probably best to think twice about saying too much about one's travel plans.

3. "Liking" Things That Could Be Used Against You

Some 4.7 million people have "liked" a Facebook page about a health condition or treatment. *Consumer Reports* suggests insurers could use this information against you. That may sound far-fetched, but there have already been documented cases of insurers scouring Facebook to fight fraud. And as *Consumer Reports* notes, the IRS and other government agencies are allowed to comb Facebook, and in some instances friend people, to fight fraud.

4. Betraying Family Privacy

Consumer Reports says that some 39.3 million U.S. Facebook users identified a family member in their profile. Not a big deal in most cases, but how many times was permission sought? Not everyone wants to be tagged in a photo or posted about. That's an issue of user thoughtfulness. But Facebook could help out here by making it easier for people to avoid involvement in sharing. Making Tag Suggest opt-in rather than opt-out would be a step in the right direction.

5. Telling Apps Too Much

Only 37% of Facebook users bother to use the site's privacy controls to limit the data apps can see about them, according to *Consumer Reports'* survey. And anyone can create a Facebook app. Take a good look at the information requested by Facebook apps. You might be surprised.

Sophos security researcher Chet Wisniewski in a phone interview called *Consumer Reports'* findings "disappointing but not surprising." As to whether or not the risks mentioned by the magazine are realistic, he said there's a lot of hype, but that doesn't mean the risks should be ignored. He said one problem with sharing he's seen has been stalking.

"A lot of young women post their movements on Facebook and don't realize their photos have GPS coordinates," Wisniewski said. He also pointed to the website pleaserobme.com as a way to underscore the risks presented by sharing location information.

Online services, Wisniewski said, could do a better job with providing privacy by default instead of as something that has to be chosen.

"Unfortunately, it's a race to the bottom when some new feature or service is introduced," he said. "It's a race to zero privacy."

As companies increase their use of cloud-based applications, IT and security professionals must make some tough and far-reaching decisions about how to provision, deprovision, and otherwise manage user access. This Dark Reading report, How To Manage Identity In The Public Cloud, examines the options and provides recommendations for determining which one is right for your organization. (Free registration required.)