Journal of Privacy and Confidentiality (2010) **2**, Number 1, pp. 3–4

Schneier on Security: Privacy and Control

Bruce Schneier*

In January, Facebook Chief Executive Mark Zuckerberg declared the age of privacy to be over. A month earlier, Google Chief Eric Schmidt expressed a similar sentiment. Add Scott McNealy's and Larry Ellison's comments from a few years earlier, and you've got a whole lot of tech CEOs proclaiming the death of privacy—especially when it comes to young people.

It's just not true. People, including the younger generation, still care about privacy. Yes, they're far more public on the Internet than their parents: writing personal details on Facebook, posting embarrassing photos on Flickr and having intimate conversations on Twitter. But they take steps to protect their privacy and vociferously complain when they feel it violated. They're not technically sophisticated about privacy and make mistakes all the time, but that's mostly the fault of companies and Web sites that try to manipulate them for financial gain.

To the older generation, privacy is about secrecy. And, as the Supreme Court said, once something is no longer secret, it's no longer private. But that's not how privacy works, and it's not how the younger generation thinks about it. Privacy is about control. When your health records are sold to a pharmaceutical company without your permission; when a social-networking site changes your privacy settings to make what used to be visible only to your friends visible to everyone; when the NSA eavesdrops on everyone's e-mail conversations—your loss of control over that information is the issue. We may not mind sharing our personal lives and thoughts, but we want to control how, where, and with whom. A privacy failure is a control failure.

People's relationship with privacy is socially complicated. Salience matters: People are more likely to protect their privacy if they're thinking about it, and less likely to if they're thinking about something else. Social-networking sites know this, constantly reminding people about how much fun it is to share photos and comments and conversations while downplaying the privacy risks. Some sites go even further, deliberately hiding information about how little control—and privacy—users have over their data. We all give up our privacy when we're not thinking about it.

Group behavior matters; we're more likely to expose personal information when our peers are doing it. We object more to losing privacy than we value its return once it's gone. Even if we don't have control over our data, an illusion of control reassures us. And we are poor judges of risk. All sorts of academic research backs up these findings.

Here's the problem: The very companies whose CEOs eulogize privacy make their money by controlling vast amounts of their users' information. Whether through targeted advertising, cross-selling, or simply convincing their users to spend more time on their site and sign up their friends, more information shared in more ways, more publicly, means more profits. This means these companies are motivated to continually

*Chief Security Technology Officer, BT Group, London, UK, mailto:schneier@schneier.com

ratchet down the privacy of their services, while at the same time pronouncing privacy erosions as inevitable and giving users the illusion of control.

You can see these forces in play with Google's launch of Buzz. Buzz is a Twitter-like chatting service, and when Google launched it in February, the defaults were set so people would follow the people they corresponded with frequently in Gmail, with the list publicly available. Yes, users could change these options, but—and Google knew this—changing options is hard and most people accept the defaults, especially when they're trying out something new. People were upset that their previously private e-mail contacts list was suddenly public. A Federal Trade Commission commissioner even threatened penalties. And though Google changed its defaults, resentment remained.

Facebook tried a similar control grab when it changed people's default privacy settings last December to make them more public. While users could, in theory, keep their previous settings, it took an effort. Many people just wanted to chat with their friends and clicked through the new defaults without realizing it.

Facebook has a history of this sort of thing. In 2006 it introduced News Feeds, which changed the way people viewed information about their friends. There was no true privacy change in that users could not see more information than before; the change was in control—or arguably, just in the illusion of control. Still, there was a large uproar. And Facebook is doing it again; last month, the company announced new privacy changes that will make it easier for it to collect location data on users and sell that data to third parties.

With all this privacy erosion, those CEOs may actually be right—but only because they're working to kill privacy. On the Internet, our privacy options are limited to the options those companies give us and how easy they are to find. We have Gmail and Facebook accounts because that's where we socialize these days, and it's hard—especially for the younger generation—to opt out. As long as privacy isn't salient, and as long as these companies are allowed to forcibly change social norms by limiting options, people will increasingly get used to less and less privacy. There's no malice on anyone's part here; it's just market forces in action. If we believe privacy is a social good, something necessary for democracy, liberty, and human dignity, then we can't rely on market forces to maintain it. Broad legislation protecting personal privacy by giving people control over their personal data is the only solution.

This essay originally appeared on Forbes.com, April 6th, 2010.

Reprinted with the permission of the author from *Schneier on Security* (`www.schneier.com`, a blog covering security and security technology.