Forbes

Everyone Wants You To Have Security, But Not From Them

Bruce Schneier

February 23, 2015

In December Google's Executive Chairman Eric Schmidt was interviewed at the CATO Institute Surveillance Conference. One of the things he said, after talking about some of the security measures his company has put in place post-Snowden, was: "If you have important information, the safest place to keep it is in Google. And I can assure you that the safest place to not keep it is anywhere else."

The surprised me, because Google collects all of your information to show you more targeted advertising. Surveillance is the business model of the Internet, and Google is one of the most successful companies at that. To claim that Google protects your privacy better than anyone else is to profoundly misunderstand why Google stores your data for free in the first place.

I was reminded of this last week when I appeared on Glenn Beck's show along with cryptography pioneer Whitfield Diffie. Diffie said:

> You can't have privacy without security, and I think we have glaring failures in computer security in problems that we've been working on for 40 years. You really should not live in fear of opening an attachment to a message. It ought to be confined; your computer ought to be able to handle it. And the fact that we have persisted for decades without solving these problems is partly because they're very difficult, but partly because there are lots of people who want you to be secure against everyone but them. And that includes all of the major computer manufacturers who, roughly speaking, want to manage your computer for you. The trouble is, I'm not sure of any practical alternative.

That neatly explains Google. Eric Schmidt does want your data to be secure. He wants Google to be the safest place for your data — as long as you don't mind the fact that Google has access to your data. Facebook wants the same thing: to protect your data from everyone except Facebook. Hardware companies are no different. Last week, we learned that Lenovo computers shipped with a piece of adware called Superfish that broke users' security to spy on them for advertising purposes.

Governments are no different. The FBI wants people to have strong encryption, but it wants backdoor access so it can get at your data. UK Prime Minister David Cameron wants you to have good security, just as long as it's not so strong as to keep the UK government out. And, of course, the NSA spends a lot of money ensuring that there's no security it can't break. Corporations want access to your data for profit; governments want it security purposes, be they benevolent or malevolent. But Diffie makes an even stronger point: we give lots of companies access to our data because it makes our lives easier.

I wrote about this in my latest book, *Data and Goliath*:

> Convenience is the other reason we willingly give highly personal data to corporate interests, and put up with becoming objects of their surveillance. As I keep saying, surveillance-based services are useful and valuable. We like it when we can access our address book, calendar, photographs, documents, and everything else on any device we happen to be near. We like services like Siri and Google Now, which work best when they know tons about you. Social networking apps make it easier to hang out with our friends. Cell phone apps like Google Maps, Yelp, Weather, and Uber work better and faster when they know our location. Letting apps like Pocket or Instapaper know what we're reading feels like a small price to pay for getting everything we want to read in one convenient place. We even like it when ads are targeted to exactly what we're interested in. The benefits of surveillance in these and other applications are real, and significant.

Like Diffie, I'm not sure there is any practical alternative. The reason the Internet is a worldwide mass-market phenomenon is that all the technological details are hidden from view. Someone else is taking care of it. We want strong security, but we also want companies to have access to our computers, smart devices, and data. We want someone else to manage our computers and smart phones, organize our e-mail and photos, and help us move data between our various devices.

Those "someones" will necessarily be able to violate our privacy, either by deliberately peeking at our data or by having such lax security that they're vulnerable to national intelligence agencies, cybercriminals, or both. Last week, we learned that the NSA broke into the Dutch company Gemalto andstole the encryption keys for billions — yes, billions — of cell phones worldwide. That was possible because we consumers don't want to do the work of securely generating those keys and setting up our own security when we get our phones; we want it done automatically by the phone manufacturers. We want our data to be secure, but we want someone to be able to recover it all when we forget our password.

We'll never solve these security problems as long as we're our own worst enemy. That's why I believe that any long-term security solution will not only be technological, but political as well. We need laws that will protect our privacy from those who obey the laws, and to punish those who break the laws. We need laws that require those entrusted with our data to protect our data. Yes, we need better security technologies, but we also need laws mandating the use of those technologies.