Hard National Security Choices LAWFARE

SUPPORT

Sunday, February 21, 2016

CYBERSECURITY

Security or Surveillance?

By **Bruce Schneier** Monday, February 1, 2016, 1:01 PM

Harvard's Berkman Center for Internet & Society convened an interdisciplinary group to take on vexing questions of surveillance and cybersecurity. The group has now released the report "Don't Panic." Here, its authors share some individual reflections.

***

Both the "going dark" metaphor of FBI Director James Comey and the contrasting "golden age of surveillance" metaphor of privacy law professor Peter Swire focus on the value of data to law enforcement. As framed in the media, encryption debates are about whether law enforcement should have surreptitious access to data, or whether companies should be allowed to provide strong encryption to their customers.

It's a myopic framing that focuses only on one threat — criminals, including domestic terrorists

Bruce Schneier is an internationally renowned security technologist, called a "security guru" by The Economist. He is the author of 12 books — including "Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World" — as well as hundreds of articles, essays, and academic papers. His influential newsletter "Crypto-Gram" and blog "Schneier on Security" are read by over 250,000 people. Schneier is a fellow at the Berkman Center for Internet and Society at Harvard Law School, a program fellow at the New America Foundation's Open Technology Institute, a board member of the Electronic Frontier Foundation, and an

— and the demands of law enforcement and national intelligence. This obscures the most important aspects of the encryption issue: the security it provides against a much wider variety of threats.

Encryption secures our data and communications against eavesdroppers like criminals, foreign governments, and terrorists. We use it every day to hide our cell phone conversations from eavesdroppers, and to hide our Internet purchasing from credit card thieves. Dissidents in China and many other countries use it to avoid arrest. It's a vital tool for journalists to communicate with their sources, for NGOs to protect their work in repressive countries, and for attorneys to communicate with their clients.

Many technological security failures of today can be traced to failures of encryption. In 2014 and 2015, unnamed hackers — probably the Chinese government — stole 21.5 million personal files of U.S. government employees and others. They wouldn't have obtained this data if it had been encrypted. Many large-scale criminal data thefts were made either easier or more damaging because data wasn't encrypted: Target, TJ Maxx, Heartland Payment Systems, and so on. Many countries are eavesdropping on the unencrypted communications of their own citizens, looking for dissidents and other voices

Advisory Board member of the Electronic Privacy Information Center. He is also the Chief Technology Officer of Resilient Systems, Inc.

MORE ARTICLES >

RELATED ARTICLES

Apple's Challenge to Magistrate's Order for Assisting the FBI
Herb Lin Wed, Feb 17, 2016, 7:52 PM

Not a Slippery Slope, but a Jump off the Cliff
Nicholas Weaver Wed, Feb 17, 2016, 4:51 PM

Apple vs FBI: The Going Dark Dispute Moves from Congress to the Courtroom
Robert Chesney Wed, Feb 17, 2016, 12:58 PM

Cyber (In)security in India
Samir Saran, Bedavyasa Mohanty Tue, Feb 16, 2016, 9:34 AM

How Concerned Should We Be about IoT Vulnerability?
Paul Rosenzweig Fri, Feb 12, 2016, 4:14 PM

SUPPORT LAWFARE

they want to silence.

Adding backdoors will only exacerbate the risks. As technologists, we can't build an access system that only works for people of a certain citizenship, or with a particular morality, or only in the presence of a specified legal document. If the FBI can eavesdrop on your text messages or get at your computer's hard drive, so can other governments. So can criminals. So can terrorists. This is not theoretical; again and again, backdoor accesses built for one purpose have been surreptitiously used for another. Vodafone built backdoor access into Greece's cell phone network for the Greek government; it was used against the Greek government in 2004-2005. Google kept a database of backdoor accesses provided to the U.S. government under CALEA; the Chinese breached that database in 2009.

We're not being asked to choose between security and privacy. We're being asked to choose between less security and more security.

This trade-off isn't new. In the mid-1990s, cryptographers argued that escrowing encryption keys with central authorities would weaken security. In 2013, cybersecurity researcher Susan Landau published her excellent book *Surveillance or Security?*, which deftly parsed the details of this trade-off and concluded that security is far more important.

Ubiquitous encryption protects us much more from bulk surveillance than from targeted surveillance. For a variety of technical reasons, computer security is extraordinarily weak. If a sufficiently skilled, funded, and motivated attacker wants in to your computer, they're in. If they're not, it's because you're not high enough on their priority list to bother with. Widespread encryption forces the listener — whether a foreign government, criminal, or terrorist — to target. And this hurts repressive governments much more than it hurts terrorists and criminals.

Of course, criminals and terrorists have used, are using, and will use encryption to hide their planning from the authorities, just as they will use many aspects of society's capabilities and infrastructure: cars, restaurants, telecommunications. In general, we recognize that such things can be used by both honest and dishonest people. Society thrives nonetheless because the honest so outnumber the dishonest. Compare this with the tactic of secretly poisoning all the food at a restaurant. Yes, we might get lucky and poison a terrorist before he strikes, but we'll harm all the innocent customers in the process. Weakening encryption for everyone is harmful in exactly the same way.

Topics: Cybersecurity, Surveillance, Encryption, Going Dark

Tags: Cybersecurity, Harvard Berkman Center for Internet & Society, going dark