Schneier on Security

← How to Design—And Defend Against—The Perfect Security Backdoor

Why the NSA's Defense of Mass Data Collection Makes No Sense →

Your Life, Under Constant Surveillance

Bruce Schneier
CNN
October 16, 2013

Historically, surveillance was difficult and expensive.

Over the decades, as technology advanced, surveillance became easier and easier. Today, we find ourselves in a world of ubiquitous surveillance, where everything is collected, saved, searched, correlated and analyzed.

But while technology allowed for an increase in both corporate and government surveillance, the private and public sectors took very different paths to get there. The former always collected information about everyone, but over time, collected more and more of it, while the latter always collected maximal information, but over time, collected it on more and more people.

Corporate surveillance has been on a path from minimal to maximal information. Corporations always collected information on everyone they could, but in the past they didn't collect very much of it and only held it as long as necessary. When surveillance information was expensive to collect and store, companies made do with as little as possible.

Telephone companies collected long-distance calling information because they needed it for billing purposes. Credit cards collected only the information about their customers' transactions that they needed for billing. Stores hardly ever collected information about their customers, maybe some personal preferences, or name-and-address for advertising purposes. Even Google, back in the beginning, collected far less information about its users than it does today.

As technology improved, corporations were able to collect more. As the cost of data storage became cheaper, they were able to save more data and for a longer time. And as big data analysis tools became more powerful, it became profitable to save more. Today, almost everything is being saved by someone—probably forever.

Examples are everywhere. Internet companies like Google, Facebook, Amazon and Apple collect everything we do online at their sites. Third-party cookies allow those companies, and others, to collect data on us wherever we are on the Internet. Store affinity cards allow merchants to track our purchases. CCTV and aerial surveillance combined with automatic face recognition allow

companies to track our movements; so does your cell phone. The Internet will facilitate even more surveillance, by more corporations for more purposes.

On the government side, surveillance has been on a path from individually targeted to broadly collected. When surveillance was manual and expensive, it could only be justified in extreme cases. The warrant process limited police surveillance, and resource restraints and the risk of discovery limited national intelligence surveillance. Specific individuals were targeted for surveillance, and maximal information was collected on them alone.

As technology improved, the government was able to implement ever-broadening surveillance. The National Security Agency could surveil groups—the Soviet government, the Chinese diplomatic corps, etc.—not just individuals. Eventually, they could spy on entire communications trunks.

Now, instead of watching one person, the NSA can monitor "three hops" away from that person—an ever widening network of people not directly connected to the person under surveillance. Using sophisticated tools, the NSA can surveil broad swaths of the Internet and phone network.

Governments have always used their authority to piggyback on corporate surveillance. Why should they go through the trouble of developing their own surveillance programs when they could just ask corporations for the data? For example we just learned that the NSA collects e-mail, IM and social networking contact lists for millions of Internet users worldwide.

But as corporations started collecting more information on populations, governments started demanding that data. Through National Security Letters, the FBI can surveil huge groups of people without obtaining a warrant. Through secret agreements, the NSA can monitor the entire Internet and telephone networks.

This is a huge part of the public-private surveillance partnership.

The result of all this is we're now living in a world where both corporations and governments have us all under pretty much constant surveillance.

Data is a byproduct of the information society. Every interaction we have with a computer creates a transaction record, and we interact with computers hundreds of times a day. Even if we don't use a computer—buying something in person with cash, say—the merchant uses a computer, and the data flows into the same system. Everything we do leaves a data shadow, and that shadow is constantly under surveillance.

Data is also a byproduct of information society socialization, whether it be e-mail, instant messages or conversations on Facebook. Conversations that used to be ephemeral are now recorded, and we are all leaving digital footprints wherever we go.

Moore's law has made computing cheaper. All of us have made computing ubiquitous. And because computing produces data, and that data equals surveillance, we have created a world of ubiquitous surveillance.

Now we need to figure out what to do about it. This is more than reining in the NSA or fining a corporation for the occasional data abuse. We need to decide whether our data is a shared societal resource, a part of us that is inherently ours by right, or a private good to be bought and sold.

Writing in The Guardian, Chris Huhn said that "information is power, and the necessary corollary is that privacy is freedom." How this interplay between power and freedom play out in the information age is still to be determined.

Categories: National Security Policy, Privacy and Surveillance

Tags: CNN

← How to Design—And Defend Against—The Perfect Security Backdoor

Why the NSA's Defense of Mass Data Collection Makes No Sense →