The Internet is a surveillance state

By Bruce Schneier , Special to CNN
updated 2:04 PM EDT, Sat March 16, 2013

CNN.com

Editor's note: Bruce Schneier is a security technologist and author of "Liars and Outliers: Enabling the Trust Society Needs to Survive."

(CNN) -- I'm going to start with three data points.

One: Some of the Chinese military hackers who were implicated in a broad set of attacks against the U.S. government and corporations were identified because they accessed Facebook from the same network infrastructure they used to carry out their attacks.

Two: Hector Monsegur, one of the leaders of the LulzSac hacker movement, was identified and arrested last year by the FBI. Although he practiced good computer security and used an anonymous relay service to protect his identity, he slipped up.

And three: Paula Broadwell,who had an affair with CIA director David Petraeus, similarly took extensive precautions to hide her identity. She never logged in to her anonymous e-mail service from her home network. Instead, she used hotel and other public networks when she e-mailed him. The FBI correlated hotel registration data from several different hotels -- and hers was the common name.

The Internet is a surveillance state. Whether we admit it to ourselves or not, and whether we like it or not, we're being tracked all the time. Google tracks us, both on its pages and on other pages it has access to. Facebook does the same; it even tracks non-Facebook users. Apple tracks us on our iPhones and iPads. One reporter used a tool called Collusion to track who was tracking him; 105 companies tracked his Internet use during one 36-hour period.

Increasingly, what we do on the Internet is being combined with other data about us. Unmasking Broadwell's identity involved correlating her Internet activity with her hotel stays. Everything we do now involves computers, and computers produce data as a natural by-product. Everything is now being saved and correlated, and many big-data companies make money by building up intimate profiles of our lives from a variety of sources.

News: Cyberthreats getting worse, House intelligence officials warn

Facebook, for example, correlates your online behavior with your purchasing habits offline. And there's more. There's location data from your cell phone, there's a record of your movements from closed-circuit TVs.

This is ubiquitous surveillance: All of us being watched, all the time, and that data being stored forever. This is what a surveillance state looks like, and it's efficient beyond the wildest dreams of George Orwell.

Sure, we can take measures to prevent this. We can limit what we search on Google from our iPhones, and instead use computer web browsers that allow us to delete cookies. We can use an alias on Facebook. We can turn our cell phones off and spend cash. But increasingly, none of it matters.

There are simply too many ways to be tracked. The Internet, e-mail, cell phones, web browsers, social networking sites, search engines: these have become necessities, and it's fanciful to expect people to simply refuse to use them just because they don't like the spying, especially since the full extent of such spying is deliberately hidden from us and there are few alternatives being marketed by companies that don't spy.

This isn't something the free market can fix. We consumers have no choice in the matter. All the major companies that provide us with Internet services are interested in tracking us. Visit a website and it will almost certainly know who you are; there are lots of ways to be tracked without cookies. Cellphone companies routinely undo the web's privacy protection. One experiment at Carnegie Mellon took real-time videos of students on campus and was able to identify one-third of them by comparing their photos with publicly available tagged Facebook photos.

Maintaining privacy on the Internet is nearly impossible. If you forget even once to enable your protections, or click on the wrong link, or type the wrong thing, and you've permanently attached your name to whatever anonymous service you're using. Monsegur slipped up once, and the FBI got him. If the director of the CIA can't maintain his privacy on the Internet, we've got no hope.

In today's world, governments and corporations are working together to keep things that way. Governments are happy to use the data corporations collect -- occasionally demanding that they collect more and save it longer -- to spy on us. And corporations are happy to buy data from governments. Together the powerful spy on the powerless, and they're not going to give up their positions of power, despite what the people want.

Fixing this requires strong government will, but they're just as punch-drunk on data as the corporations. Slap-on-the-wrist fines notwithstanding, no one is agitating for better privacy laws.

So, we're done. Welcome to a world where Google knows exactly what sort of porn you all like, and more about your interests than your spouse does. Welcome to a world where your cell phone company knows exactly where you are all the time. Welcome to the end of private conversations, because increasingly your conversations are conducted by e-mail, text, or social networking sites.

And welcome to a world where all of this, and everything else that you do or is done on a computer, is saved, correlated, studied, passed around from company to company without your knowledge or consent; and where the government accesses it at will without a warrant.

Welcome to an Internet without privacy, and we've ended up here with hardly a fight.

Follow.

Join us at.

The opinions expressed in this commentary are solely those of Bruce Schneier.