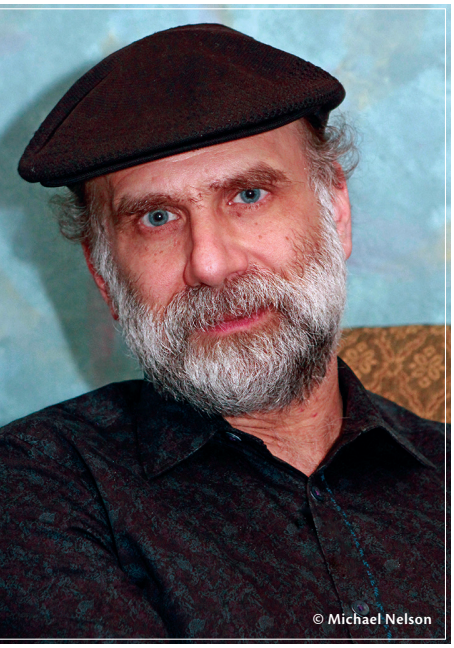

Bruce Schneier
Co3 Systems

Metadata = Surveillance

Ever since reporters began publishing stories about NSA activities, based on documents provided by Edward Snowden, we've been repeatedly assured by government officials that it's "only metadata." This might fool the average person, but it shouldn't fool those of us in the security field. Metadata equals surveillance data, and collecting metadata on people means putting them under surveillance.

An easy thought experiment demonstrates this. Imagine that you hired a private detective to eavesdrop on a subject. That detective would plant a bug in that subject's home, office, and car. He would eavesdrop on his computer. He would listen in on that subject's conversations, both face to face and remotely, and you would get a report on what was said in those conversations. (This is what President Obama repeatedly reassures us isn't happening with our phone calls. But am I the only one who finds it suspicious that he always uses very specific words? "The NSA is not listening in on your phone calls." This leaves open the possibility that the NSA is recording, transcribing, and analyzing your phone calls—and very occasionally reading them. This is far more likely to be true, and something a pedantically minded president could claim he wasn't lying about.)

Now imagine that you asked that same private detective to put a subject under constant surveillance. You would get a different report, one that included things like where he went, what he did, who he spoke to—and for how long—who he wrote to, what he read, and what he purchased. This is all metadata, data we know the NSA is collecting. So when the president says that it's only metadata, what you should really hear is that we're all under constant and ubiquitous surveillance.

What's missing from much of the discussion about the NSA's activities is what they're doing with all of this surveillance data. The newspapers focus on what's being collected, not on how it's being analyzed—with the singular exception of the *Washington Post* story on cell phone location collection. By their nature, cell phones are tracking devices. For a network to connect calls, it needs to know which cell the phone is located in. In an urban area, this narrows a phone's location to a few blocks. GPS data, transmitted across the network by far too many apps, locates a phone even more precisely. Collecting this data in bulk, which is what the NSA does, effectively puts everyone under physical surveillance.

This is new. Police could always tail a suspect, but now they can tail everyone—suspect or not. And once they're able to do that, they can perform analyses that weren't otherwise possible. The *Washington Post* reported two examples. One, you can look for pairs of phones that move toward each other, turn off for an hour or so, and then turn themselves back on while moving away from each other. In other words, you can look for secret meetings. Two, you can locate specific phones of interest and then look for other phones that move geographically in synch with those phones. In other words, you can look for someone physically tailing someone else. I'm sure there are dozens of other clever analyses you can perform with a database like this. We need more researchers thinking about the possibilities. I can assure you that the world's intelligence agencies are conducting this research.

How could a secret police use other surveillance databases: everyone's calling records, everyone's purchasing habits, everyone's browsing history, everyone's Facebook and Twitter history? How could these databases be combined in interesting ways? We need more research on the emergent properties of ubiquitous electronic surveillance.

We can't protect against what we don't understand. And whatever you think of the NSA or the other 5-Eyes countries, these techniques aren't solely theirs. They're being used by many countries to intimidate and control their populations. In a few years, they'll be used by corporations for psychological manipulation—persuasion or advertising—and even sooner by cybercriminals for more illicit purposes. ■

Bruce Schneier is the CTO of Co3 Systems. You can find him online at www.schneier.com.

Copublished by the IEEE Computer and Reliability Societies