New Scientist

David and Goliath: What do we do about surveillance?

30 March 2015 by **Douglas Heaven**
Magazine issue 3014
For similar stories, visit the **Books and Art** Topic Guide

From spyware designed to catch students misbehaving to police tracking rioters by phone, we are spied on as never before, reveals a book by Bruce Schneier

Book information
Data and Goliath: The hidden battles to collect your data and control your world by Bruce Schneier
Published by: W. W. Norton
Price: $27.95/£17.99

Police worldwide are trying to link specific phones to specific events *(Image: Gleb Garanich/Reuters)*

"DEAR subscriber, you have been registered as a participant in a mass disturbance." This text was sent by the Ukrainian government last year to everyone with a cellphone known to have been near a protest in the capital, Kiev.

Just what you'd expect from an ex-Soviet country? Not so fast. In the US and Europe, police are also seeking information on phones linked to specific places and times – and always without a warrant. We're all spied on. Our phones are bugged, our laptops inveterate informants. Reports on activities that define you – where you go, who you meet, what you buy – are sold to the highest bidder. But do we notice? And do we care?

Bruce Schneier does his best to make us do both. But it's tough: as it fades into the background, surveillance gets easier to ignore. For Schneier, this is a unique time to take a good look at the leviathan before it submerges forever.

So what is surveillance? The US military defines it as "systematic observation". It controls "what we see, what we can do... ultimately, what we say", says Schneier. A director of the Electronic Frontier Foundation in San Francisco, Schneier has been a go-to expert for years. He helped analyse some of the more technical documents leaked by Edward Snowden. But he wears his expertise lightly: the book moves fast and references are relegated to pages of notes.

There are brilliantly creepy examples. Take Cobham, a UK company that sells a system which allows "blind" calls to be sent to your phone. It won't ring, so you won't know you received it, but it makes your phone send a signal so callers can track it within a metre. Then there's Lower Merion School District in Ardmore, Pennsylvania, which installed spyware on laptops for its pupils. School administrators could secretly record chat logs, monitor web use and photograph the kids. This was exposed when a student was shown a picture of himself taking drugs. It turned out to be candy.

And image-based surveillance is poised to make things worse. Researchers at Carnegie Mellon University in Pittsburgh, Pennsylvania, set up a camera in a public space and identified people by combining face-recognition software with Facebook's publicly tagged database. By correlating names with other databases, they displayed data about individuals in the time it took them to pass by.

Many dismiss all this. Schneier cites a Google executive who told him that worrying about a computer reading your email was like worrying about your dog seeing you naked. It's not, Schneier rejoins: your dog won't base decisions on what they see, and will certainly never tell anyone.

Another common justification is that we're only giving up our metadata: the "to" and "from" of emails, not their contents; and the time and duration of calls, not what was said. It can still be highly revealing information and is the equivalent of someone tailing you and reporting who you spoke to and for how long, he says. And whatever's collected is stored indefinitely, often because it's cheaper and easier than filtering out the juicy bits.

Worse, what doesn't bubble to the surface today could do so tomorrow with new techniques. Take Alfred Kinsey's sex research subjects, who participated in the 1940s and 1950s only under the strictest anonymity. In 2013, a study showed that in principle it would be possible to identify 97 per cent of them.

Snooping that once required a warrant and was subject to tight regulations is now routine. At one time, recounts Schneier, an FBI agent listening to a mobster on a bugged phone was required to stop listening when a spouse or child came on the line – quaint niceties compared to the practices of the US National Security Agency and the UK's GCHQ.

How did we get here? Fear – of terrorism in particular, says Schneier. But anti-terrorism laws suffer from mission creep and create a culture that normalises surveillance. How to get out of this is one of the big questions of our time, he adds.

So what can we do? Here, the impish anarchist in Schneier gets loose. Use the anonymising, ad-blocking, cookie-munching solutions available, he says, but also mess with the system: put stickers over laptop cameras, add noise to the data by searching for random names on Facebook, wear masks or face paint to confuse CCTV. He's only half joking. If data is the pollution problem of the information age, then protecting privacy is the environmental challenge. Can we make a difference?

Schneier calls himself a short-term pessimist but a long-term optimist. In 50 years, he says, people will look at today's data practices much as we now view practices like tenant farming or child labour. I'm not so sure. It may well be a generational issue, but not the way Schneier thinks. Few people under 30 worry where the data on their phone goes. Your feelings about Venmo, say – an app combining a digital-payment service with social-media updates on who you're paying – will also depend on age. And sexting is as common among teens as texting a decade ago. What if we look back at surveillance angst as a hang-up we had to overcome?

This article appeared in print under the headline "Got you in our sights"