THE FUTURE OF PRIVACY

BRUCE SCHNEIER

Originally from New York City, Schneier currently lives in Minneapolis, Minnesota, USA. Schneier has a Master's degree in computer science from American University and a Bachelor of Science degree in physics from the University of Rochester.

Mr Schneier is an internationally renowned security technologist, cryptographer, computer security specialist and writer and is the founder and chief technologist officer of BT Counterpane. Before Counterpane, he worked at the United States Department of Defense and then AT&T Bell Labs.

Regularly quoted in the media, he has testified on security before the United States Congress on several occasions. He is the author of several books on computer security and cryptography and has written articles for many major publications, including The New York Times, The Guardian, Forbes, Wired, Nature, The Bulletin of the Atomic Scientists, The Sydney Morning Herald, The Boston Globe, The San Francisco Chronicle, and The Washington Post. *Schneier's* Applied Cryptography *is a popular reference work for cryptography. In 2000, Schneier published* Secrets and Lies: Digital Security in a Networked World. *In 2003, Schneier published* Beyond Fear: Thinking Sensibly About Security in an Uncertain World.

→| THE EXPERT

"As soon as questions of will or decision or reason or choice of action arise, human science is at lost."

NOAM CHOMSKY

OVER THE PAST TWENTY YEARS, there's been a sea change in the battle for personal privacy.

The pervasiveness of computers has resulted in the almost constant surveillance of everyone, with profound implications for our society and our freedoms. Corporations and the police are both using this new trove of surveillance data. We as a society need to understand the technological trends and discuss their implications. If we ignore the problem and leave it to the "market," we will all find that we have almost no privacy left.

Most people think of surveillance in terms of police procedure: Follow that car, watch that person, listen in on his phone conversations. This kind of surveillance still occurs. But today's surveillance is more like the NSA's model, recently turned against Americans: Eavesdrop on every phone call, listening for certain keywords. It's still surveillance, but it's wholesale surveillance.

Wholesale surveillance is a whole new world. It is not "follow that car," it is "follow every car." The National Security Agency can eavesdrop on every phone call, looking for patterns of communication or keywords that might indicate a conversation between terrorists. Many airports collect the license plates of every car in their parking lots, and can use that database to locate suspicious or abandoned cars. Several cities have stationary or car-mounted license-plate scanners that keep records of every car that passes, and save that data for later analysis.

More and more, we leave a trail of electronic footprints as we go through our daily lives. We used to walk into a bookstore, browse, and buy a book with cash. Now we visit Amazon, and all of our browsing and purchases are recorded. We used to throw a quarter in a toll booth; now EZ Pass records the date and time our car passed through the booth. Data about us are collected when we make a phone call, send an e-mail message, make a purchase with our credit card, or visit a website.

Much has been written about RFID chips and how they can be used to track people. People can also be tracked by their cell phones, their Bluetooth devices, and their WiFi-enabled computers. In some cities, video cameras capture our image hundreds of times a day.

The common thread here is computers. Computers are involved more and more in our transactions, and data are byproducts of these transactions. As computer memory becomes cheaper, more and more of these electronic footprints are being saved. And as processing becomes cheaper, more and more of it is being cross-indexed and correlated, and then used for secondary purposes.

Information about us has value. It has value to the police, but it also has value to corporations. The Justice Department wants details of Google searches, so they can look for patterns that might help find child pornographers. Google uses that same data so it can deliver context-sensitive advertising messages. The city of Baltimore uses aerial photography to surveil every house, looking for building permit violations. A national lawn-care company uses the same data to better market its services. The phone company keeps

detailed call records for billing purposes; the police use them to catch bad guys.

In the dot-com bust, the customer database was often the only salable asset a company had. Companies like Experian and Acxiom are in the business of buying and reselling this sort of data, and their customers are both corporate and government.

Computers are getting smaller and cheaper every year, and these trends will continue. Here's just one example of the digital footprints we leave:

It would take about 100 megabytes of storage to record everything the fastest typist input to his computer in a year.

That is a single flash memory chip today, and one could imagine computer manufacturers offering this as a reliability feature. Recording everything the average user does on the Internet requires more memory: 4 to 8 gigabytes a year. That's a lot, but «record everything» is GMail's model, and it's probably only a few years before ISPs offer this service.

The typical person uses 500 cell phone minutes a month; that translates to 5 gigabytes a year to save it all. My iPod can store 12 times that data. A "life recorder" you can wear on your lapel that constantly records is still a few generations off: 200 gigabytes/year for audio and 700 gigabytes/year for video. It will be sold as a security device, so that no one can attack you without being recorded. When that happens, will not wearing a life recorder be used as evidence that someone is up to no good, just as prosecutors today use the fact that someone left his cell phone at home as evidence that he didn't want to be tracked?

In a sense, we are living in a unique time in history. Identification checks are common, but they still require us to whip out our ID. Soon it will happen automatically, either through an RFID chip in our wallet or face-recognition from cameras. And those cameras, now visible, will shrink to the point where we won't even see them.

We are never going to stop the march of technology, but we can enact legislation to protect our privacy: comprehensive laws regulating what can be done with personal information about us, and more privacy protection from the police. Today, personal information about you is not yours; it's owned by the collector. There are laws protecting specific pieces of personal data – videotape rental records, health care information – but nothing like the broad privacy protection laws you find in European countries. That is really the only solution; leaving the market to sort this out will result in even more invasive wholesale surveillance.

Most of us are happy to give out personal information in exchange for specific services. What we object to is the surreptitious collection of personal information, and the secondary use of information once it's collected: the buying and selling of our information behind our back.

In some ways, this tidal wave of data is the pollution problem of the information age. All information processes produce it. If we ignore the problem, it will stay around forever. And the only way to successfully deal with it is to pass laws regulating its generation, use and eventual disposal. ▣