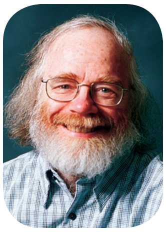
The Puzzle of Privacy



Steven M. Bellovin
Columbia University

Several recent news stories have made me wonder more about privacy. It's not just that threats to privacy are increasing; rather, the problem is that the countervailing forces are becoming so much stronger. Was Scott McNealy right when he told us that we had no privacy and that we should just "get over it"?

To overgeneralize, in the past, companies have violated privacy by exploiting data they collected. Today, privacy violations occur by exploiting deliberate (though often unwitting) choices individuals make. This change makes it harder to combat the loss of privacy because the benefits of the action accrue directly to the individual.

Years ago, for example, you could only buy music by purchasing a physical object containing it: a record, a tape, a CD. The purchase might be traceable, but only if the buyer used a traceable payment system, such as a check. Today, though, music can be leased online. Lease renewals *inherently* provide tracking data. Digital video recorders provide an even more striking example: the "record similar shows" feature often requires informing a central site of what you've watched.

Sometimes, financial inducements persuade people to use traceable technologies. The penalty for using cash ranges from 33 percent on New York's George Washington Bridge to 267 percent on the London Tube.

Another new phenomenon is that privacy-invading technologies are moving to the physical world. In several countries, toll highways work by cameras that read license plates and bill the vehicle owners. New York City is planning to use license plate cameras and OCR as part of an antiterrorist initiative. The *New York Times* reports that "Data on each vehicle—its time-stamped image, license plate imprint and radiological signature—would be sent to a command center in Lower Manhattan, where it would be indexed and stored for at least a month." Fighting terrorism is a good idea, but what else will this data be used for? Will it be available via subpoena to, say, divorce lawyers? (E-ZPass toll transponders records already are.)

In a post on a cryptography mailing list, Perry Metzger made the following observations:

> "The time for focusing on the privacy implications of payment transponders and fare cards is over. … Digital cash toll collection systems will not avoid records being kept of your car's movements when cameras are reading and recording license plates anyway.
>
> "Unfortunately, I don't see anything technological that people can reasonably do here to provide more privacy, at least short of everyone going everywhere on foot while wearing a burqa and periodically attempting to confuse the cameras. The solutions, if any exist at all, appear to be non-technical."

Traditionally, three methods preserve privacy: technology, market incentives, and regulation. It's harder to use these for physical privacy invasions. There are no onion routing networks or digital cash systems that let us evade networked surveillance cameras. The market incentives appear to be working against privacy. That leaves regulation.

It's hard to argue with the benefits from the primary uses of all this collected data. E-ZPasses are faster than cash tolls, fighting terrorism is a fine idea, and so on. As is frequently the case, the danger comes from the secondary uses of the data—and the only solution is to legislate against it. Tell me about the movies I might like—but don't use that information for advertising. Let me speed my way through the tunnels—but don't tell any lawyers where I've been. Fight real terrorists, but don't use their existence as an excuse to build an omnipresent surveillance system. In short, we need laws and regulations—and we need them to apply to government as well as to the private sector. □

***Steven M. Bellovin** is a professor of computer science at Columbia University. Contact him via www.cs.columbia.edu/~smb.*