Steven M. Bellovin
Columbia University

Unnoticed Consent

For more than 45 years, the root of privacy policy has been transparency and agreement: the subject must be told what is being collected and stored and then can assent or decline. This has generally been called *notice and consent*. The root is a 1973 U.S. government advisory committee report, which held, among other things, that people had the right to know what was being collected about them and to limit or prevent secondary uses of the data. These notions, the fair information practice principles (FIPPs), are the basis for laws around the world, up to and including the European Union's General Data Protection Regulation. These ideas have been with us for so long that they sound obviously correct. Perhaps they were, at the dawn of the web 25 years ago, but they no longer fit the modern world. The FIPPs no longer work, and, if we are to retain (or regain) privacy, we need a different basic structure.

There are a number of reasons that the FIPPs have failed, but the fundamental issue is simple: the world of data is far more complex today than it was in 1973. To use Alan Westin's term, our *data shadow*, the information that is created by our daily activities, is much larger. Worse yet, the very concept of secondary use is becoming meaningless. Let's take these points one at a time.

> **It is all but impossible to participate in the modern world without creating and relying on this data shadow.**

One of the reasons for the growth of the data shadow is the existence of new technologies. It was incomprehensible in 1967 that, when someone asked for directions, the provider could see whether those directions were actually followed and how fast the person walked or drove. But every time you follow turn-by-turn directions on your smartphone, that's exactly what is happening. Similarly, the notion that people's houses would contain devices that listen to every word spoken was the stuff of dystopian fiction. Today, Alexa, Siri, Cortana, and their friends are ubiquitous—and, at least in principle, these gadgets can populate far-off databases with what you say. Even dolls can collect conversations.

The last few decades have also witnessed the dramatic growth of the commercial data collection industry. Westin saw this coming, but the vastly increased sources of information (e.g., auto mechanics routinely upload odometer data at every oil change, and some chain food outlets have stopped accepting cash in favor of the credit cards that produce so much data about us) have amounted to a change in kind rather than a change in scale. In the United States, data brokers now have an average of 1,500 pieces of information on every adult. This is a far cry from the credit bureaus of the early 1900s, whose records were often merely a collection of gossip.

The third big change is what some have called the *original sin* of the web: the advertising-supported business model. Advertising may or may not be evil per se, but, today, it relies on a vast array of trackers monitoring your every click.

Few, if any, of these databases are secret. Our gadgets, apps, and web pages are chock-full of privacy policies. But the policies are too long and complex, and there are too many of them. Virtually no one reads them or heeds their warnings. The data broker industry doesn't hide its existence, but few (apart from privacy specialists and the businesses

Digital Object Identifier 10.1109/MSEC.2018.2882121
Date of publication: 21 January 2019

continued on p. 79

 Copublished by the IEEE Computer and Reliability Societies 1540-7993/18©2018IEEE

continued from p. 80

that buy from them) are aware of what they store and aggregate.

We also can't really control what happens to our data. If our phones have deduced our work and home addresses from our map queries, is it a second use for a phone to spontaneously suggest a different commuting pattern? What about ads for businesses along those routes? And all of these data go to train machine learning models, so it's impossible to tell which items are important to ads and which to answering our requests. Finally, it is all but impossible to participate in the modern world without creating and relying on this data shadow. If you can't live without it, is your consent voluntary?

So people do not (cannot) understand what is being collected about them, do not (cannot) understand when there are secondary uses, and do not (cannot) effectively withhold consent. But, as these are the heart of the FIPPs, the FIPPs are dead. What, then, should replace them? What is a new paradigm for privacy protection, one that works in the modern world?

Steven M. Bellovin is a professor of computer science and affiliate law faculty at Columbia University. Contact him via https://www.cs.columbia.edu/~smb.