THE WALL STREET JOURNAL.

The Hard Questions

A mature democracy needs to carefully balance individual privacy, national security and business efficiency.

By Richard Epstein

March 16, 2015

New technologies are always a mixed blessing, their potential for good carrying with it the risk of evil. The deep challenge for a democracy is to develop legal rules, social practices and institutional arrangements that, at some reasonable cost, separate good from bad behavior. The exponential improvement in computation and communication technologies over the past few decades has posed this challenge in an acute form. Both large bureaucracies and determined individuals can now collect and organize huge amounts of information—and all of it, in one sense or another, is about all of us.

Protecting our privacy from the prying eyes and ears of government is the subject of Bruce Schneier's "Data and Goliath," whose title suggests an uneven struggle. Jacob Silverman's "Terms of Service" grapples with similar themes, though he focuses on commercial behemoths such as Amazon, Apple, Facebook, Google and Twitter, which relentlessly gather information about their customers. Both books, however, offer one-sided presentations.

It is not that these authors have nothing instructive to say about these problems. Mr. Silverman, a journalist, warns us to beware of "how companies try to embed pernicious language in their terms of service agreements," leading consumers to give away their privacy rights unknowingly. Mr. Schneier, a security technologist and fellow at the Berkman Center for Internet and Society at Harvard Law School, is attuned to the smallest potential dangers: He points out (rightly) how easy it is to use metadata to identify by name participants in any medical study, or to track cellphone usage near the site of a labor dispute without a warrant. But both authors are unable to make intelligent trade-offs among individual privacy, national security and business efficiency.

Let's start with Mr. Schneier. His book begins with a recounting of the well-known ways in which modern computational capacity allows the government to track emails, phone calls and movements in real time. He notes that the U.S. is not the only player: What it can do to collect information from concealed sources, other nations can do as well. He is thus quite correct to observe that building backdoors that allow American intelligence services secret access to private databases can create unintended openings for hostile governments to obtain that same data. All too often actions done in the name of security serve to undermine it.

Mr. Schneier is on thinner ice when he challenges not the means of surveillance but the value of the enterprise itself. Even post-9/11, he sees no great threat to American lives, no danger that might require special diligence and precision to thwart. In one astonishing passage he implicitly compares attacks like those on the World Trade Center with domestic mass killing like the one that took place in Aurora, Colo., in 2012. "Terrorists don't cause more damage or kill more people," he argues, "we just fear them more. We need to transfer the traditional law enforcement transparency principles to national security." Really? His view that operations that are now covert should be transparent in a manner similar to those of the police is unwise, considering the classified information that would be revealed—and then available to our enemies and to our peril.

No amount of technical expertise can excuse these fatal lapses in judgment or the unstinting and inexcusable praise that Mr. Schneier heaps on Edward Snowden for his leaks of highly classified American and British intelligence. (Mr. Schneier has written frequently for the Guardian newspaper, which has published much of the information that Snowden had illegally obtained from the National Security Agency.) Granted, it may be good for someone to tell the American population what it already knows, namely that our intelligence agencies work overtime to collect and organize sensitive information. But did Snowden really have to release these classified documents to the Guardian, or, as seems likely, share them with the Chinese and Russian governments? A unilateral transfer of confidential information to our enemies was surely not in the national interest.

Mr. Silverman, in "Terms of Service," is worried about how personal data about our buying habits and friendship patterns is all too freely given to online-services companies. "The Internet," he warns, "is being thoroughly socialized, which is to say thoroughly monitored." The key question is the extent to which these practices help or hurt the consumers, who flock to private networks by the millions. I am not that troubled that some private companies whose services I use know that I prefer wine to hard liquor, that they can determine my location by tracking my smartphone use, or that they are metering the services they supply so as to allow for constant readjustment of prices for hotels, apartments, flights or meals at restaurants. These and other activities generate enormous consumer benefits that dwarf the billions of dollars snapped up by the likes of Larry Page, Sergey Brin and Mark Zuckerberg.

In a complex world, we are wise to sometimes make compromises, in our personal lives as well as in public policy. The uncompromising stances of these two authors leave readers with the impression that not a single word of good sense could be said on behalf of either the national security establishment or the modern companies that created and drive social media. And so the hard questions remain.

Mr. Epstein is a professor of law at New York University, a senior fellow at the Hoover Institution, an adjunct scholar at the Cato Institute, and a senior lecturer at the University of Chicago Law School. His latest book is "The Classical Liberal Constitution."