The Ends of Privacy

By Jack Goldsmith

Review of Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*

W. W. Norton & Company, 2015

"Over the past twenty years," complained *Newsweek*, the United States has become "one of the snoopiest and most data-conscious nations in the history of the world." Part of the problem is that "the average American trails data behind him like spoor through the length of his life." Another part of the problem is that the government and private firms "have been chasing down, storing, and putting to use every scrap of information they can find." These "vast reservoirs of personal information" are "poured into huge computers" and "swapped with mountains of other data from other sources" with "miraculous speed and capacity." As a result of these forces, "Americans have begun to surrender both the sense and the reality of their own right to privacy – and their reaction to their loss has been slow and piecemeal."

The *Newsweek* article – published in 1970, and entitled *The Assault on Privacy* – nicely captures the thesis of Bruce Schneier's new book, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. That doesn't mean that Schneier's book isn't valuable – it is. It just means that there is something to be learned about Schneier's argument from the fact that it was made 45 years ago. (Disclosure: I gave Schneier comments on a draft of his book and he and I are teaching a class together on Internet power and governance.)

Data and Goliath is an informed, well-written, accessible, and opinionated critique of "ubiquitous mass surveillance" by governments and corporations – how it happens, its costs, and what to do about it. Mass surveillance is made possible because "everything is turning into a computer." The average individual interacts with hundreds (and soon thousands) of computers everyday – smartphones, laptops, web pages, social media, automobiles, cameras and recorders and others sensors, payment mechanisms, and so on. Soon pets, food containers, and appliances will all have chips and sensors – this is the Internet of things, where everything is computerized. These computers collect, record, store, generate, and emit an astounding amount and variety of data about us: what we say and write and like and want and do (including our vices and secrets); where we are, who we are with, and who we communicate with; the state of our health and finances and personal lives; and much more.

This "exhaust of the information age" is growing fast. An exabyte of data is a billion billion bytes, the equivalent of 500 billion pages of text. Schneier says that 76 exabytes of data will travel across the Internet this year. A thousand exabytes is a zettabyte (1,000 000,000,000,000,000,000 bytes). A recent presidential report on big data noted that computers worldwide generated 4 zettabytes of information in 2013. According to IBM, 90% of the data in the world today has been created in the last two years. And this is all before the Internet of things

really gets going. This incomprehensibly huge mass of information – "big data" – is easy to retain. "[C]omputer storage has become cheap enough to make it feasible to indefinitely save all of the data we churn out," Schneier says. And because the cost of computing is also quite cheap, the data is easy to "mine" – that is, to process, transfer, correlate, and analyze in ways that uncover an astounding amount of information about our lives.

The first third of *Data and Goliath* is a terrific tutorial on how firms use big data to data mine. Building on the Snowden documents, Schneier also explains how governments work with these firms in a vast "public-private surveillance partnership" to gather this data for intelligence purposes, and sometimes to steal it from them as well. Schneier's story about the out-of-control U.S. government is exaggerated. But even those who trust the government and are disinclined to worry about private data mining will pause over the scale of public and private watching that Schneier describes. "We're all open books to both governments and corporations," he says.

Schneier nods to the benefits of mass surveillance, but the second and third parts of the book focus almost exclusively on what he sees as its many extreme dangers. Mass surveillance, he argues, is "the enemy of democracy" because it enables "perfect" law enforcement and social control which inhibit legal and social change. It is "dehumanizing" because it destroys anonymity, disables how we present ourselves to the world, and makes it very hard "to be ephemeral" (because everything is recorded). Constant government and private observance also chills free speech and thought. And it promotes invidious discrimination because all of the characteristics that might matter to governments and firms – race, wealth, health, age, and really any distinguishing trait – can be easily discerned and used as a basis for action.

Schneier matches these alarmist conclusions with a long list of needed reforms. For government, he wants less secrecy and more transparency, more and better oversight, better protection for whistleblowers, elimination of bulk surveillance, disclosure and patching (as opposed to hoarding) of computer vulnerabilities that enable offensive cyber operations, a sharp limit on the military's role in cyberspace, and a break-up of the National Security Agency. For corporations, he proposes liability for data breaches, extensive regulation of the collection and use of data, greater data transparency, stronger consumer rights to data, and creation of information fiduciaries.

This program will please the powerful groups of anti-surveillance civil libertarians that Reihan Salam dubs "Snowdenites." (Schneier has worked with Edward Snowden and Glenn Greenwald in analyzing the Snowden documents, and he writes about them with insight on his blog.) But Schneier realizes that most of his proposals are unrealistic. "I'm not yet living in a country where the majority of people want these changes," he says. "Most people don't seem to care whether their intimate details are collected and used by corporations; they think that surveillance by the governments they trust is a necessary prerequisite to keeping them safe."

This is the central issue. The government gets most of its big data from firms, and firms collect most of their data from individuals who give the information away. "The bargain you

make, again and again, with various companies is surveillance in exchange for free service." Another bargain we make is letting the government surveil us in order to "relieve [our] fear." Schneier thinks these "aren't good or fair bargains." We are about to find out if he is right, for we are in the midst of informed public debates about the proper regulation of big data.

Just last month the Obama administration proposed a comprehensive consumer data privacy bill, and the Federal Trade Commission and state governments are well aware of the corporate dangers Schneier describes and taking steps to mitigate them. Similar reforms are afoot on government surveillance. Modern surveillance tools empower the government. But they also weaken it. As Snowden and Chelsea Manning have shown, the mechanisms of mass surveillance – digitalization, bulk data storage, instant copying and transfer, powerful computer analysis, and the like – can be turned on the government to extract the deep secrets that are central to its power. The cascade of revelations, in turn, has sparked unprecedented scrutiny of the Surveillance State by politicians, courts, and journalists, and an organized reform movement. It has also incentivized the mass distribution of easy-to-use encryption tools and other "privacy-enhancing technologies" that, as Schneier explains, make government surveillance harder. These technological and political forces have a good chance to balance the power between the State, firms, and individuals roughly where most Americans want it, though almost certainly not where Schneier wants it.

One reason Schneier's case for reform falls short is that he does not fully articulate its costs for the private sector, or the current benefits of private-sector surveillance. Schneier wants computer- and Internet-related firms to be heavily regulated industries. He fails to explain convincingly why such regulation would not (as Internet- and computer-related firms insist) destroy innovation and degrade the consumer-friendliness of digital products. Nor does he explain why the government he distrusts would regulate wisely and would not misuse the heaps of yet-more-data needed to make its new regulations efficacious.

The truth is that consumers love the benefits of digital goods and are willing to give up traditionally private information in exchange for the manifold miracles that the Internet and big data bring. Apple and Android each offer more than a million apps, most of which are built upon this model, as are countless other Internet services. More generally, big data promises huge improvements in economic efficiency and productivity, and in health care and safety. Absent abuses on a scale we have not yet seen, the public's attitude toward giving away personal information in exchange for these benefits will likely persist, even if the government requires firms to make more transparent how they collect and use our data. One piece of evidence for this is that privacy-respecting search engines and email services do not capture large market shares. In general these services are not as easy to use, not as robust, and not as efficacious as their personal-data-heavy competitors.

Schneier understands and discusses all this. In the end his position seems to be that we should deny ourselves some (and perhaps a lot) of the benefits big data because the costs to privacy and related values are just too high. We "have to stop the slide" away from privacy, he

says, not because privacy is "profitable or efficient, but because it is moral." But as Schneier also recognizes, privacy is not a static moral concept. "Our personal definitions of privacy are both cultural and situational," he acknowledges. Consumers are voting with their computer mice and smartphones for more digital goods in exchange for more personal data. The culture increasingly accepts the giveaway of personal information for the benefits of modern computerized life.

This trend is not new. "The idea that privacy can't be invaded at all is utopian," says Professor Charles Fried of Harvard Law School. "There are amounts and kinds of information which previously were not given out and suddenly they have to be given out. People adjust their behavior and conceptions accordingly." That is Fried in the 1970 *Newsweek* story, responding to an earlier generation's panic about big data and data mining. The same point applies today, and will apply as well when the Internet of things makes today's data mining seem as quaint as 1970s-era computation.

JACK GOLDSMITH is the Henry L. Shattuck Professor at Harvard Law School, a Senior Fellow at the Hoover Institution at Stanford University, and co-founder of Lawfareblog.com. He teaches and writes about national security law, presidential power, cybersecurity, international law, internet law, foreign relations law, and conflict of laws. Before coming to Harvard, Professor Goldsmith served as Assistant Attorney General, Office of Legal Counsel from 2003-2004, and Special Counsel to the Department of Defense from 2002-2003.