**The Digital Person: Technology and Privacy in the Information Age**
Daniel J. Solove
New York: New York University Press, 2004, 283 pp.

There is no better survey of the privacy landscape than Daniel Solove's *The Digital Person*. The book proceeds thoughtfully but briskly through the major elements of the privacy debate. With important qualifications, this book is a recommended read for people concerned with the threats wrought by increasingly data-heavy modern business processes.

*The Digital Person* examines the growth of databases and dossiers, assesses the varied laws that protect privacy, explores the privacy consequences of public records and open government, exposes the growing scope of data use by governments, and surveys relevant Fourth Amendment law. It is thoroughly researched and footnoted, giving readers entrée to further sources of reading.

Solove's discussion of the privacy torts is a highlight. It is particularly welcome because other scholars and advocates have ignored this baseline privacy protection, acting as if federal statute and bureaucratic regulation were the only influence on individuals and institutions. Indeed, Solove recognizes that contract law and markets, tort law, statutes, and constitutional rights all provide privacy protections one way or another.

On Fourth Amendment law, *The Digital Person* is particularly good. Solove's analogy between *Olmstead v. United States*, 277 U.S. 438 (1928), and *United States v. Miller*, 425 U.S. 435 (1976), is delightful. In *Olmstead*, the Supreme Court found that tapping a phone line outside a person's house was not a Fourth Amendment violation because there was no entry into the home; it was rightly overruled in the landmark decision in *Katz v. United States*, 389 US 347 (1967).

*Miller* is one of several cases in which the Court has failed to recognize that Americans' reasonable privacy expectations extend to information that they place with third parties, such as banks, telephone and (now) Internet service providers, and medical practitioners. This case and its kin must also be overruled.

As a survey of the privacy landscape, *The Digital Person* is quite good. It does not, however, break much new ground and it has important weaknesses of which readers should be wary.

Rather than George Orwell's *1984*, Solove proposes to organize privacy thinking around a new metaphor: Franz Kafka's *The Trial*. In that story, the hapless Joseph K. is declared under arrest by a group of bureaucrats, though they do not imprison him. Joseph K. struggles against a remote, faceless, and arbitrary bureaucracy that ultimately seizes him in the middle of the night and executes him. Far lesser versions of Joseph K.'s struggle can and do happen in the world of databases, obviously.

Invoking Kafka may whet an otherwise dry topic, but the metaphor is ultimately just as prone to misuse as Orwell and *1984*. It is probably a disservice to the careful, reasoned thinking about privacy that Solove otherwise uses and seeks.

*The Digital Person* does attempt fair consideration of all the angles, including the role of markets in protecting privacy. Again, this is refreshing because most academics and privacy activists ignore market processes or dismiss them as inherently coercive, unfair, or insufficient.

Though he takes more care, Solove ends up rejecting markets on essentially these same grounds. Current markets do not offer the privacy choices that he (and they) deem most appropriate. Rather, consumers are faced with take-it-or-leave-it offers that require them to trade privacy for convenience and other goods. Solove (and the others) ignore consumers' power to exit markets entirely—a power they exercise consistently, using cash selectively or entirely in place of credit and bank cards, shopping in stores rather than online, and communicating by phone or letter rather than e-mail.

By withholding patronage, these consumers sap profit from corporations and products that offer unsatisfactory privacy protection, while

holding a carrot out before those that would win their trust. If they do not represent a large enough market, they are outliers, no more entitled to the privacy terms they want than milk-drinkers are entitled to have dairies offer home delivery by a man in a crisp white uniform.

Data-centric businesses provide easy payment methods with fraud and anti-theft protections far superior to cash. They amass reputation information that allows consumers fast access to credit at favorable rates. They shave down prices and buff up the quality of products to win consumer favor. And they constantly study how they can please consumers more, using personal information as an essential tool. Solove and his colleagues tend to ignore these benefits and seek default legal rules against them, adopting a privacy-centric myopia that neglects other dimensions of consumer welfare.

There are things wrong in the world of consumer data, of course. Witness the recent spate of data breaches. Many institutions have obviously failed to recognize the value of data they hold or the risks to themselves, other businesses, and consumers created by casual handling of sensitive personal information. The public debate over these incidents post-dates publication of *The Digital Person*, but Solove has promoted the solutions in his book using the heightened attention to data security.

Solove's response is to override the "invasion conception" of privacy with something else. The "invasion conception" is that privacy is something individuals enjoy, the loss of which individuals suffer as a harm. Though the invasion conception can continue, what Solove calls for is a society-wide privacy "architecture."

The heart of this privacy "architecture" is the weakest part of the book. Solove advocates the "fair information principles" (FIPs) that have been floating around for decades. FIPs are bundles of policies designed to solve the variety of concerns that surround data collection, aggregation, sharing, and use. Many of these policies are meritorious. Some are not. And some are in tension with one another. They probably apply better in the governmental context but have seen only mixed success even there. The Privacy Act of 1974, for example, is one FIP statute that is plainly not equipped to address modern problems.

And, ironically, Solove does not recognize that the Fair Credit Reporting Act (FCRA)—another FIP statute—is probably responsible for the credit reporting industry being so . . . well, Kafkaesque. Under the FCRA, an intricate set of regulatory procedures dictates how consumers can dispute items in their credit reports and what responsibilities credit bureaus have to respond or to change consumers' files. It sets low hurdles for the credit bureaus and, most important, insulates them from tort liability for defamation, invasion of privacy, or negligence.

Accordingly, ever since the FCRA was passed in 1970, the credit reporting industry has served two masters: the financial institutions that furnish information and buy information products and the government regulators that enforce the FCRA. Consumers—who could be partners

in maintaining the data that typically serves them so well—are an afterthought. The "architecture" created by the FCRA should act as a warning against the adoption of FIP statutes.

One interesting proposal Solove puts forward is to place data collectors in a fiduciary relationship to the subjects of that data. This high a duty, based solely on the collection of personal information, is far-fetched and Solove does not spend a lot of time defending it. However, a lower duty on the part of data holders, a duty to protect data subjects from harm, has been recognized at common law in some states. Adopted widely, this could do much of what Solove seeks.

These are quibbles that will have to be hashed out in other, narrower forums. They do not undermine the quality of *The Digital Person* as a survey of the privacy issues we all face as we sit on the cusp of the Information Age.

Jim Harper
Cato Institute