The Costs of Privacy

Author : Christopher Slobogin

Date : September 6, 2021

Ric Simmons, **Smart Surveillance: How to Interpret the Fourth Amendment in the Twenty-First Century** (2019).

Most scholarship about the impact of technology on policing has been of the sky-is-falling variety. The typical author recites a litany of technological advances, points out how those advances have made policing much more intrusive and pervasive, and then calls for a warrant requirement, some version of "privacy by design," or perhaps even a prohibition on whatever surveillance technique is at issue. Maintenance of privacy is the main, if the not the dominant, goal.

In *Smart Surveillance*, Ric Simmons takes a completely different view. Adopting a cost-benefit analysis, he embraces technology that can make policing more efficient. The common scholarly refrain is that maximum Fourth Amendment protection must be imposed whenever technology gives the police a leg up—whenever, as the Supreme Court's opinion in *Carpenter v. United States* put it when explaining why a warrant is required to obtain cell site tracking information, new technology makes enforcement efforts "remarkably easy, cheap, and efficient compared to traditional investigative tools." To Professor Simmons, this stance makes no sense. Such thinking, he says, "turns the cost-benefit analysis on its head by seeking to deter some of the most productive searches available to law enforcement." (P. 121.)

Professor Simmons plays this idea out in four different settings: reactive searches, binary searches, mosaic searches, and hyper-intrusive searches. Reactive searches are those that use technology to counteract privacy-enhancing technology, such as encryption, high-powered heat lamps (of the type the defendant in *Kyllo v. United States* used to grow marijuana indoors), and third-party services that enable would-be criminals to carry out their activities under cover of the Internet. Binary searches rely on technology that can discover criminal activity and nothing else, as the Supreme Court has assumed drug-sniffing dogs can do. Mosaic searches are those that use technology to accumulate information from numerous public sources much more cheaply and quickly than through traditional means—for instance, cell phone tracking rather than tailing, or buying information from data brokers rather than tromping from one records office to another. In contrast to reactive searches, hyper-intrusive searches "over-react" to privacy enhancing developments by, for instance, enabling continuous surveillance of phone and email conversations, covert surveillance of the home, and interceptions of computer and phone communications.

In each of these scenarios, Professor Simmons argues that courts need to do a much better job gauging the security benefits and the privacy costs. Ideally, this benefit-cost analysis would be carried out in as quantified a manner as possible. For instance, on the benefits side, Professor Simmons argues that big data can help generate statistics on the efficacy of various techniques—ranging from hit rates for stops and frisks in "high crime" neighborhoods to arrest rates resulting from CCTV cameras and cellphone tracking. On the cost side, he envisions greater use of surveys measuring community views of intrusiveness as a means of calibrating privacy interests.

This methodology is then applied throughout the book. Although he does not reach definitive conclusions on the matter, Professor Simmons suggests that, based on the available data, the stop and frisk practices of many cities cannot be justified, but that predictive policing using algorithms could be,

at least when they incorporate or are combined with conduct that gives the police some reason to believe criminal activity is afoot. Additional possible benefits of this data-driven policing—assuming the decision-making algorithms are disclosed and used even-handedly—include more transparent decision-making, a redistribution of privacy toward the disadvantaged, and less racially-based policing.

More confidently, Professor Simmons argues that binary searches will virtually always be justified on a cost-benefit rationale, as long as the technology is accurate most of the time (and thus does not generate a large number of false positives) and does not require suspicionless seizures to operate. He also suggests that some reactive searches (e.g. thermal imaging of the home) and mosaic searches (e.g., tracking of public travels) might be justified on much less than probable cause, give their efficiency and their relative unintrusiveness (compared to, for instance, full searches of the home). Hyper-intrusive searches, on the other hand, might require, as Title III does for electronic surveillance, not only ex ante review and probable cause, but a showing that no less intrusive technique will be productive. However, in contrast to much academic commentary, Professor Simmons agrees with *Maryland v. King's* conclusion that suspicionless collection of DNA is permissible, and even gestures toward approval of a universal DNA database, given the ability of junk DNA to identify perpetrators without revealing other intimate facts.

Leaving no controversy untouched, Professor Simmons also argues in favor of the third party doctrine, which allows police to obtain data in the hands of banks, phone companies, Internet service providers and the like with a mere subpoena, and sometimes a simple request. If *Carpenter* is any guide, at least six justices, along with most Fourth Amendment scholars, have serious reservations about the doctrine. But Professor Simmons points out that the personal data maintained by modern companies can be extremely useful to law enforcement and that "millions of individuals already knowingly—and at times, willingly—share this information with third-party companies." (P. 154.) To Professor Simmons, these high security benefits and low privacy costs weigh in favor of the current regime. He also notes that, increasingly in the past decade, some third parties (e.g., Google, Apple and some DNA companies) have been willing for their own business-related purposes to resist law enforcement investigations, a development that allows those individuals who are concerned about privacy to pay for it.

I do not agree with every point made in this book. But Professor Simmons has provided a very useful counter-point to much of the scholarship about police use of surveillance techniques. His insights cannot be ignored as we race headlong into a new era of policing.

Cite as: Christopher Slobogin, *The Costs of Privacy*, JOTWELL (September 6, 2021) (reviewing Ric Simmons, **Smart Surveillance: How to Interpret the Fourth Amendment in the Twenty-First Century** (2019)), https://crim.jotwell.com/the-costs-of-privacy/.