the weekly Standard

Protecting Privacy

Matthew Feeney

August 25, 2017

The Fourth Amendment is in a sorry state. The constitutional provision intended to protect us and our property from unreasonable searches and seizures has been weakened over decades—a fact that ought to be of acute concern at a time when surveillance technology is increasingly intrusive and secretive. A modernization of Fourth Amendment doctrines is long overdue.

In his new book, *The Fourth Amendment in an Age of Surveillance*, David Gray, a professor at the University of Maryland's Francis King Carey School of Law, attempts to outline what such a modernization might look like. To establish why reform is necessary, he offers a historical account. Gray traces the concepts embodied in the amendment back to mid-18th-century concerns in both England and the American colonies about overly broad permissions for executive agents. In England, the focus of the controversy was general warrants, which were vague in purpose and almost unlimited in scope.

In the colonies, the controversy focused on writs of assistance, a specialized kind of general warrant, ripe for abuse. In a five-hour-long speech before the Massachusetts Superior Court in 1761, the lawyer James Otis Jr. condemned writs of assistance, declaring them "the worst instrument of arbitrary power, the most destructive of English liberty." John Adams, who witnessed Otis's oration, decades later described it as the moment when "the Child Independence was born." A distaste for needless and indiscriminate intrusions into homes and other property is thus baked into America's revolutionary DNA. It was eventually codified in the Fourth Amendment, with its prohibition of "unreasonable searches and seizures" and guarantee that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

The doctrines used in interpreting the amendment have evolved over time. The rise of modern police forces prompted the judiciary to develop the exclusionary rule (which ensures that evidence collected via Fourth Amendment violations is inadmissible), the *Miranda* warning (which, as anyone who has seen a TV cop show in the last four decades can tell you, holds that once you're in police custody officers must tell you that you have the right to remain silent and the right to an attorney), and the warrant requirement (which holds that searches are per se unreasonable if they're conducted without prior approval from a judge or magistrate).

The interpretation of the Fourth Amendment has also evolved in response to technological development. Notably, the advent of eavesdropping devices gave rise to the "reasonable expectation of privacy" test, first formulated in Supreme Court Justice John Harlan's concurrence in *Katz* v. *United States* (1967) and subsequently adopted by the Court. According

to the test, government agents have conducted what the law considers a "search" if they have violated an individual's subjective expectation of privacy and if that expectation is one that society is prepared to accept as reasonable.

"Unfortunately," Gray writes, "the *Katz* test has proven inadequate to the task of regulating the means, methods, and technologies that have come to define our contemporary age of surveillance." Gray puts in his crosshairs three post-*Katz*doctrines that have had the effect of leaving some of the most intrusive surveillance technologies outside the purview of Fourth Amendment challenge.

First, thanks to the "public observation doctrine," police do not necessarily need a warrant to peek into your backyard with a drone. (Some states have passed legislation mandating warrants for drone surveillance, but these requirements go beyond what is required by current Fourth Amendment interpretation.) Nor do police need a warrant to track your public activities for days at a time. As Gray points out, there wouldn't even seem to be a Fourth Amendment issue if the government were to install GPS trackers in *every* car or computer and then use those trackers to keep an eye on all citizens' public movements. After all, as the *Katz* Court held, "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."

The "third-party doctrine" likewise offers little reassurance. According to this doctrine, you have no reasonable expectation of privacy in information you voluntarily surrender to third parties, such as Internet providers and banks.

In an era of Big Data and ubiquitous electronic communication, the implications of the third-party doctrine are significant. For example, police today can deploy devices called "stingrays" that mimic cellular towers. Each cell phone is constantly playing a game of Marco Polo with nearby cell towers, seeking a connection. A stingray emits a boosted signal, forcing all nearby phones to connect to it. This allows police to monitor the location of a target's cell phone. Using a stingray, law enforcement can also uncover information about a target's communications, such as the number of texts sent, the recipients of texts, the phone numbers dialed, and the duration of calls. But stingrays can also collect all of this information about the communications of innocent people. Thanks to the third-party doctrine, there is no clear Fourth Amendment remedy to this invasion of privacy.

Finally, the rules about legal "standing" in Fourth Amendment cases have, according to Gray, also weakened the remedies available to citizens. Under the rules that emerged after *Katz*, plaintiffs must demonstrate that they have suffered a violation of their reasonable expectation of privacy. So, for example, citizens outraged about the National Security Agency's metadata collection program lack the standing to file their own Fourth Amendment suits; they have to be able to explain how the program violated their reasonable expectations of privacy. Or, in another instance, when Amnesty International challenged the FISA Amendments Act of 2008, a law giving the federal government broad power to snoop on U.S. citizens' international communications, the Supreme Court ruled in 2013 that the organization lacked standing to challenge the law, even though Amnesty works with many international partners. As Justice Samuel Alito wrote for the Court, "respondents cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending."

With its citations from old dictionaries and other contemporary texts, Gray's exhaustive word-by-word and clause-by-clause dissection of the Fourth Amendment should appeal to originalists. His take on standing may raise a few eyebrows, but he does a noble job of defending his claim that an original public understanding of the Fourth Amendment reveals that it protects a collective right to prospective relief, not just relief for past individual harms. The amendment does protect individuals, Gray believes, but its individual protections are derived from the collective right.

Gray proposes several ways to improve Fourth Amendment protections in light of the high-tech surveillance techniques that are now available to authorities. Surveillance conducted by drones and stingrays could, he argues, be curtailed via a remedy modeled on the Wiretap Act. Under that 1968 legislation, passed in the wake of the *Katz* ruling, officers seeking a wiretap order must establish probable cause, exhaust other investigative methods, and ensure that the wiretap is time-limited. The act also requires that officers regularly report back to the court that issued the wiretap warrant.

When it comes to Big Data, Gray proposes a range of constraints governing the aggregation, collection, analysis, and storage of data.

Perhaps Gray's most interesting proposal flows from his collective-right theory of the Fourth Amendment. He would allow individuals and organizations to have standing to challenge programs that threaten the people as a whole. This would allow, say, the American Civil Liberties Union to challenge the legality of New York City's stop-and-frisk program. Such other programs and technologies as persistent aerial surveillance, metadata surveillance, and license-plate readers would be open to challenge under Gray's understanding of the Fourth Amendment.

Not everyone will be convinced by Gray's analysis. Some critics will undoubtedly dispute his collective-right theory of the Fourth Amendment and quibble with his Wiretap Act-like remedies. However, these disagreements will not detract from the fact that his book is a welcome and informative contribution to the public debate about surveillance—a debate that will lastingly shape how we live together and how we understand privacy and liberty.

Matthew Feeney is a policy analyst at the Cato Institute.