Privacy and Surveillance with New Technologies

By Peter B. Swire and Kenesa Ahmad, editors
Price $24.95, pp. 376

Reviewed by Lloyd Chebaclo
Journal of High Technology Law
Suffolk University Law School

Privacy and Surveillance with New Technologies is an anthology including articles published in the Economist, the Atlantic, and other online and print sources and statements from Congressional hearings and conference forums, dealing with issues of privacy arising out of changing surveillance technology. The legal issues at stake deal with the Fourth Amendment right of the people to be secure in their persons, houses, papers, and affects against unreasonable search and seizure without a warrant supported by probable cause. The publisher, the International Debate Education Association, is geared toward sparking debates among high school students. The book’s editors are Peter P. Swire, C. William O’Neill Professor of Law at the Moritz college of Law of the Ohio State University and senior fellow at the Center for American Progress and the Future of Privacy Forum, and Kenesa Ahmad, is an attorney for the Washington, D.C.-based global financial consulting firm Promontory Financial Group’s working on their global privacy practice. Ms. Ahmad was also a fellow at the Future of Privacy Forum in D.C., and Professor Swire was the Clinton administration’s Chief Counselor for Privacy from 1999 to early 2001. Professor Swire also wrote A Reasonableness Approach to Searches After the Jones GPS Tracking Case,¹ and co-wrote U.S. Private-sector Privacy: Law and Practice for Information Privacy Professionals² with Ms. Ahmad.

The views express experience and opinions from policy professionals, privacy advocates from the American Civil Liberties Union, government officials, academics, journalists, and more on various applications of surveillance technology and methods used including video surveillance, border searches of

¹ 64 Stan. L. Rev. Online 57, Feb. 2, 2012, archived at www.webcitation.org/6EX8gZ5RX (interpreting a recent case of GPS surveillance via a tracker secretly attached to a defendant’s automobile).
electronic devices, locational tracking, issues of online privacy, backdoor surveillance through wiretapping. Glenn Greenwald\(^3\) is a recurring voice calling for greater privacy protections who discusses cases in which post 9/11 border searches appear to have gone too far, and appear to have been without cause. For example, Laura Poitras, an academy award-winning filmmaker has been detained and interviewed extensively while traveling in and out of the U.S. as part of her work on films like “My Country, My Country” about a Sunni physician and 2005 candidate for the Iraqi Congress who protested the imprisonment of a nine-year-old boy by the U.S. military. Her other works include “The Oath” about two Yemenis and America’s War on Terror one of which Hamdan of the 2006 Supreme Court case.\(^4\)

Poitras is described as having been “hampered, and continues to be hampered, by the constant harassment, invasive searches, and intimidation tactics to which she is routinely subjected whenever she enters her own country.” Her laptop, camera, and cellphone have been seized for weeks and her reporters’ notebooks have been copied despite her objections and invocation of reporters’ privilege to protect her confidential sources.\(^5\) At one point a Department of Homeland Security (DHS) agent told she could not take notes (though her attorney advised her to do so) while she was being questioned because her pen could be used as a weapon, and that it was suspicious that she was unwilling to help her country by answering certain questions about who she contacted during her trips when she asserted her journalistic privilege, and she was accused of refusing to cooperate with an investigation, a statement later clarified to say there was no investigation per se, only questioning.\(^6\) She has since resorted to not bringing electronics with her when she travels for fear of seizure of raw footage, exposure of sources, the confidentiality of which is critical to retaining sources. Greenwald also notes that documents obtained

---

\(^3\) Currently a columnist at the Guardian on security and liberty, Greenwald was contributing writer at Salon.com at publication, and is a former constitutional and civil rights litigator.

\(^4\) Hamdan v. Rumsfeld, 548 U.S. 557 (2006) (addressing whether rights under the Geneva Convention could be enforced in federal court through habeas corpus petitions and whether the military commission established to try Hamdan and others for alleged war crimes in the War on Terror was authorized by Congress or inherent powers of the President). See Peter B. Swire and Kenesa Ahmad, Privacy and Surveillance with New Technologies 180 (International Debate Education Association 2012) (discussing Poitras’s documentary work).


\(^6\) See Swire & Ahmad, supra note 4 at 182, 184 (discussing Poitras’s experience during questioning by DHS agents).
from a Freedom of Information Act (FOIA) request show that DHS has repeatedly concluded that nothing incriminating was found from its border searches and interrogations of Poitras who has had to travel frequently abroad for her documentaries and has been subject to intensive searches upon every return.\(^7\)

Thematically, Greenwald’s article seems to speak directly to David Brin’s earlier 1996 *Wired* article about video surveillance in the book, *The Transparent Society*, in which he essentially says the antidote to an Orwellian nightmare where law enforcement surveillance is entirely unfettered by government and corporate interests in the form of privatized security is criticism and the freedom to dissent to keep liberty and privacy from being subsumed.\(^8\) Greenwald points out that the harassment has had a chilling effect on journalists and people like Poitras, who has been reluctant to speak more publicly about her treatment in travel searches and seizures for fear of it further impeding her work, and who endures much difficulty but still is in a better position because she is a known filmmaker. Brin takes a different approach by describing hypothetical cities in a more novelistic style filled with cameras constantly watching its citizens at traffic lights, anticipating much of what can commonly be seen today including the growing use of drone surveillance by the military, and even some civilian drone use.\(^9\)

Greenwald sharply criticizes federal courts as having

> “become extremely submissive to assertions of Executive authority in the post 9/11 era, particularly when justified in the name of security. It’s also in part because anyone with a record of antiauthoritarianism or a willingness to oppose unrestrained government power, with very rare exception, can no longer get appointed to the federal bench; instead it’s an increasingly homogeneous lot with demonstrated fealty to institutional authority.”\(^{10}\)

Perhaps there is something to this, but this portion of the book might have benefited from some citations to a number of specific cases in support.\(^{11}\) He also goes on to say that many “life-tenured

---

\(^7\) See id. at 183 (addressing Poitras’s response and lack of DHS findings).

\(^8\) See id. at 81 (pointing to the importance of criticism by the people to create accountability for policies should they fail to protect citizen privacy as surveillance technology becomes ubiquitous).

\(^9\) See id. at 76, 77 (anticipating expansive surveillance technology including military drones and possible civilian drones).

\(^10\) Id. at 185 (criticizing courts in the post-9/11 era for not deference to the Executive in security matters).

\(^11\) In fairness to Greenwald, however, the version on Salon.com does include a link to http://lawprofessors.typepad.com/crimprof_blog/2008/04/ninth-circuit-u.html which discusses a Ninth Circuit holding that does not require individualized suspicion for border laptop searches, and references a similar Fourth Circuit holding, which are not in the book’s footnotes. See Brooks Holland, Ninth Circuit Upholds Border Laptop
federal judges have been cloistered on the bench for decades, are technologically illiterate, and thus
cannot apprehend the basic difference between having your suitcase searched at the airport and having
the contents of your laptop and cellphone copied and stored by the U.S. Government.”

One of the criticisms that privacy advocates in the book put forth is that the approach taken in
current surveillance modes is overbroad, that it casts too wide a net yielding too much data without
enough analysts to process it. The current approach is said to spend too much of its resources on
monitoring innocent behavior, leaving ignored some data that actually leads to something actionable.
For example, there was ample information on the Ft. Hood shooter Nidal Harran and attempted
Christmas Day bomber Umar Abdulmutallab that was collected but went unrecognized. The
argument is that information overload clogged the surveillance system and prevented it from being
processed.

Other approaches taken in the realm of online and electronic privacy involve recommending
greater use of encryption technology and anonymizing data and limiting the ability of companies not only
in how they use the data they collect as in selling to third party applications for advertising, but further
what they can collect at all. The authors do not include too much technical detail, but make the
arguments accessible to the reader and provide footnotes to the research and recommendations of
supporting experts that discuss the particulars. Rather than having the data be attributed to the
individual user, the author points to methods that allow data generated to be anonymous, even where for
instance a user’s friends post on social networking that is relevant to the users’ location without requiring
any of the parties to be specifically identified. On the other hand, it is argued that even with encryption
and segmented data trails, it is not so difficult for individuals to aggregate the data and make it
attributable to an individual. A senior editor of the Atlantic, Alexis Madrigal discusses the shortcomings

Searches without Individualized Suspicion, CrimProf Blog, Apr. 23, 2008, archived at
www.webcitation.org/6EX958Sqo.
12 See Swire & Ahmad, supra note 4 at 185 (criticizing courts as being out of touch with technology).
13 See Swire & Ahmad, supra note 4 at 42 (criticizing the excessiveness of collected data as hindering its ineffective
implementation in security outcomes).
14 See id. at 328 (citing more technically detailed sources about encryption such as how to use secure multi-party
computation).
of efforts like the Do Not Track\textsuperscript{15} legislation towards stopping data collection by companies of internet usage, and how you can combine multiple databases to put together a fleshed-out digital portrait.\textsuperscript{16}

On the other hand, proponents of expanding surveillance technology discuss the successes of surveillance by enabling law enforcement to stop terrorist attacks in advance or stem them by allowing quicker identification and arrests of bombers who have already struck, as in London. Nathan Sales, assistant professor of law at George Mason University School of Law, notes that Zacarias Moussaoui, a convicted 9/11 conspirator and al Qaeda operative’s connections to that organization might have been discovered sooner had investigators found data on his laptop computer, which evidently had information about crop-dusting aircraft an wing patterns.\textsuperscript{17} Further important advantages to the laptop searches at borders and airports include apprehending those in possession of child pornography and those with connections to child exploitation.\textsuperscript{18} Arguably this has been made possible by more permissive use of suspicionless searches and precedent allowing for “routine” border searches of property without requiring individualized suspicion.\textsuperscript{19} Stewart Baker\textsuperscript{20} argues we should not treat the assembling of data as though it were a search of physical property, stating that “as technology makes it easier and easier to collect data, the analogy between doing that and conducting a search of a truly private space will become less and less persuasive.”\textsuperscript{21} He contends that requiring reasonable suspicion before a laptop search will open every border search to litigation, and reasonable arguments for searches may be difficult to defend in court, where the focus will be on the motives of border officials.\textsuperscript{22}

\textsuperscript{15} See id. at 348-349 (discussing how Do Not Track tools allows internet users to “opt-out” of targeted advertising online but fails to meet expectations of being able to opt out of their data being collected entirely).

\textsuperscript{16} See id. at 351 (addressing the potential for aggregation of data created by internet user about sites visited and purchases made among other activities).

\textsuperscript{17} See id. at 127 (considering interests at stake in laptop searches).

\textsuperscript{18} See id. at 128 (discussing the dangers prevented by border searches).

\textsuperscript{19} See id. at 126, 130-131 (recognizing plenary authority in government to conduct routine searches at border without probable cause or a warrant to prevent entry of contraband).

\textsuperscript{20} Stewart Baker is a partner at the law firm of Steptoe & Johnson in Washington, D.C. and was first assistant secretary for policy at the Department of Homeland Security, and formerly general counsel of the National Security Agency from 1992-1994.

\textsuperscript{21} See Swire & Ahmad, supra note 4 at 145 (arguing against a probable cause requirement for laptop searches).

\textsuperscript{22} See id. (discussing that the focus of litigation will lead defense counsel to scrutinize searches for whether a disproportionate amount is done on certain groups like minorities, Saudis, or other patterns that may get the case dismissed).
The proponents of the use of cameras at the Police Executive Research Forum also suggested that all staff should be trained to be competent with using and interpreting information the technology yields including responding officers and lab technicians, which intends to address the analytic lags that can attend the vast body of information collected. These observations present important policy issues as to what policies should be set for training regarding effective and appropriate use of surveillance. One Texan police chief mentioned that the use of personal body cameras will become standard for every officer soon, and he noted that the department did not have a policy about retaining video footage from body cameras so it was working with lawyers to draft one. That is somewhat indicative of what privacy advocates take issue with—the lag of policy behind technology advances which is probably inevitable, but is often the source of concern. Also, this police chief argued that this technology can help reduce mistrust in the government, which privacy advocates might agree with to the extent that the usage is regulated to prevent inappropriate tampering and addressing the policies behind retention and release are transparent as well.

The issues of video surveillance are also viewed in the different context of school security, which gave rise to some cases such as Robbins v. Lower Merion School District (2010) in which a student was unwittingly remotely monitored through a webcam on a school-issued laptop, including at his home, which a plaintiff in the original complaint claimed the school initiated as part of an investigation into alleged drug use.

The book includes the editors’ co-authored article “ ‘Going Dark’ Versus a ‘Golden Age for Surveillance’ ” which argues that law enforcement currently has unprecedented surveillance technology at its disposal. Their piece is a response to proponents of Going Dark proposals which, as Valerie Caproni addresses in her statement to the House Judiciary Committee’s Subcommittee on Crime, Terrorism and Homeland Security, is about the government’s practical difficulties in intercepting communications and

---
23 See id. at 113-114 (discussing the critical role of cameras in identifying bombers).
24 See id. at 120 (outlining the use of body cameras by police).
25 See id.
26 The case was settled out of court. See Swire & Ahmad, supra note 4 at 18. See also Brannum v Overton County School Board, 516 F.3d 489 (6th Cir. 2008) (holding that videotaping of middle school students while they changed clothes in school locker room was unreasonable search and Fourth Amendment violation).
related data that courts have authorized it to collect---the lagging capability in accessing real or near-real time electronic communications and related data. This lag might be addressed, it is argued, by expanding legislation like the 1994 Communications Assistance for Law Enforcement Act (CALEA), which required telecommunications carriers to equip their networks with an intercept capability that would allow law enforcement to readily access those communications when legally authorized to do so. They hope to expand CALEA to cover internet-based communications that do not use public telephone networks, such as Voice over Internet Protocol (VoIP) services, Skype, Gmail video chat, and beyond.

Swire and Ahmad respond that such arguments are based on framing the state of surveillance technology in a way that overstates law enforcement’s ability to exploit it effectively. Instead they argue law enforcement has gained much more at its disposal to more than offset the loss of capability in older technology, since they now have the ability to use data-mining, analytics on stored data to predict behavior, and locational tracking, information about contacts and confederates, and an array of new databases that create “digital dossiers” about individuals’ lives. Thus they contend it is more of a golden age than a dark one for law enforcement’s surveillance capabilities, and with this policies must address issues like the disparate retention policies permitted for communications providers across jurisdictions for location information like cell site historical data generated by signals sent to and from a cell phone.

This book can play a significant role in shaping the concerns of younger generations who are born into unprecedented integration of technology in daily life, at work and in their personal lives, and can perhaps influence them as future policymakers. The book can be useful as a secondary source to law and policy students, and professionals seeking an accessible background on privacy and technology issues, with the footnoted articles and congressional testimony being perhaps most useful as a trail towards more
detailed research. For those purposes and for any reader seeking some perspective on the competing interests involved with changing surveillance technology across different media, I would recommend a purchase if the book is not readily available for borrowing from a local library—its circulation overall appears fairly limited. The discussion it presents addresses timely issues in an area of law and societal interests in both security and privacy that are complex and seemingly always in flux.