From Perfect Citizen to Naked Bodyscanners: When is Surveillance Reasonable?

Jeffrey Rosen

Report GW-CSPRI-2010-2

December 14, 2010

Abstract

The federal government recently launched a project called "Perfect Citizen" that plans to detect cyber assaults on private companies and government agencies by using sensors to identify unusual activity in privately owned computer systems. In the future, unregulated surveillance of private sector data in the name of security is likely to become even more widespread: using Face Recognition software, for example, the government might identify anonymous citizens at a protest rally by plugging cellphone pictures of them into a Facebook database equipped with facial recognition software. And yet the Fourth Amendment, as currently interpreted, does not provide clear limits on government monitoring of private communications in the name of cyber-security. This paper gives a very brief summary of the constitutional issues raised by "Perfect Citizen" and other forms of government surveillance using technologies owned by the private sector, and proposes a variety of responses.

Work supported by the Office of the Vice President for Academic Affairs and the School of Engineering and Applied Science of The George Washington University

From Perfect Citizen to Naked Bodyscanners: When is Surveillance Reasonable?

A Talk to the Cyber Security Policy and Research Institute

George Washington University

September 22, 2010

Jeffrey Rosen

Professor of Law

George Washington University Law School

In July 2010, the Wall Street Journal reported that "The federal government is launching "Perfect Citizen," a program designed to identify cyber assaults on critical infrastructure controlled by the private and public sectors, including the electricity grid. Run by the National Security Agency, the surveillance "would rely on a set of sensors deployed in computer networks for critical infrastructure that would be triggered by unusual activity suggesting an impending cyber attack."[1]

Defenders of Perfect Citizen say that it's necessary to subject the private sector to the same detection systems that could prevent cyber attacks that might bring the entire communications network to its knees. Critics say that by surveiling millions of private communications without a warrant, private citizen represents precisely the kind of general search that the Framers of the Fourth Amendment to the Constitution meant to forbid.

Is Perfect Citizen a troubling and unconstitutional intrusion of military surveillance into

[1] http://online.wsj.com/article/SB10001424052748704545004575352983850463108.html

domestic affairs or is it a reasonable response to a grave security threat that only NSA can provide?

In my talk today, I'd like to argue that Perfect Citizen is an emblem for the difficulty of translating constitutional values in light of new technologies that ensure that the greatest threats to privacy in the twenty first century will come not from the government acting alone, but from private companies, such as Internet Service Providers, Facebook, and Google, acting in conjunction with the government. I'd like to argue that in order to satisfy the Fourth Amendment, Perfect Citizen would have to be implemented with a series of privacy protections to guarantee its legality, to ensure that it focuses on detecting and preventing serious threats, not low level wrongdoing. And then I'd like to use those privacy protections as a model for regulating a range of surveillance technologies in the twenty-first century – from airport scanners to ubiquitous surveillance by GPS devices -- in order to protect the constitutional values in the twenty-first century.

How does Perfect Citizen work? It appears to represent an extension into private networks of cyber attack detection and prevention systems currently in place on government computers. As Jack Goldsmith describes in a paper for the Brookings Project on Technology and the Constitution, the current intrusion detection system, known as EINSTEIN 2, is being supplanted by an intrusion prevention system, known as EINSTEIN 3, which will use sensors to detect malicious attacks on privately owned computer networks and Internet Service Providers to stop them in real time before they can reach government computers.[2]

Goldsmith imagines that Perfect Citizen might extend EINSTEIN throughout public and private computer networks, and that the government might require a threat detection system to monitor all communications, public and private, without a warrant. He imagines that Perfect Citizen might be expanded to allow the NSA, in conjunction with private firms, "to (a) suck up and monitor the content of private Internet communications,

[2] http://www.brookings.edu/~/media/Files/rc/papers/2010/1208_4th_amendment_goldsmith/1208_4th_amendment_goldsmith.pdf

(b) store those communications, at least temporarily, (c) trace the source of malicious agents in these communications all over the globe, including inside the United States, and (d) take steps to thwart malicious communications, even when they originate in or use computers in, the United States." [3]

Would such a system be legal under current law? In his Brookings paper, Goldsmith argues that an extension of Perfect Citizen along these lines would require Congressional authorization. But if Congress authorized the extension of Perfect Citizen, would it violate the Fourth Amendment? According to Goldsmith, "The Fourth Amendment might not be viewed today to permit the unfathomably massive copying, storage, and analysis of private communications." Courts have held that there's no reasonable expectation of privacy in this information and thus that the government collection and analysis of such information does not implicate the Fourth Amendment, although it might have to be authorized by statute.

Goldsmith concludes that the collection (or copying) and analysis of bulk communication content is another matter, although some Courts might be inclined to approve it under two existing doctrines – the third party doctrine, which holds that when you disclose information to third parties you assume the risk that the information may be disclosed to the government; and the special needs doctrine, which makes an exception to the Fourth Amendment warrant requirement for reasonable governmental actions with a purpose that goes "beyond routine law enforcement." Still, to be reasonable under the totality of the circumstances, Goldsmith concludes that Perfect Citizen would have to be implemented with at least three privacy-protecting mechanisms:

First, storage and viewing. The fact that the only communications viewed by human beings (rather than computers) are extremely suspicious increases the reasonableness of the program: courts have held that searches (like dog sniffs) that only reveal contraband and don't reveal innocent information are quintessentially reasonable.

[3] Ibid, p 9.

Second, use restrictions. To ensure that only cyber threats are targeted, the government could place use restrictions on communications that contain malicious signatures, allowing them to be stopped or destroyed but not introduced as evidence in unrelated cases that don't involve national security or computer related crimes or especially serious crimes. For models of use restrictions, the government could look to the original title III of the crime control bill of 1968, which was originally limited to violent felonies but, as a result of mission creep, has now been extended to non-violent felonies.

Third, minimization. Goldsmith suggests a variety of minimization procedures to ensure that communications that don't prove to be threatening are destroyed and that suspicious communications are examined in ways that reveal no more privacy than necessary to meet the threat. [4]A model here is the original Carnivore system, where data was traceable but not personally identifiable unless there was a high probability that it revealed as serious threat.

I'd like to argue that Goldsmith's model can be generalized to many of the surveillance technologies that have been proposed after 9/11. To the degree that they rely on suspicionless searches, all can be designed in ways that make them more or less reasonable, depending the legal and technological constraints imposed on them, such as viewing, storage, minimization requirements, and use restrictions.

Consider the body scanners recently deployed at American airports that have created a national uproar. Eight years ago, when officials at Orlando International airport first began testing the millimeter wave body scanners that have now caused a national uproar, the designers of the scanners at Pacific Northwest Laboratories made clear that U.S. officials faced a choice. They could deploy "naked machines," that display graphic images of the human body, or they could deploy "blob" machines, developed by the same researchers, that were just as effective at identifying contraband but scrambled the images of the naked body into a nondescript blob.

[4] Ibid, pp. 15-16.

Since both versions of the body scanners promise the same amount of security, any sane attempt to balance privacy and security would seem to favor the blob machines over the naked machines. And that's what European governments chose: although most European airport authorities have declined to adopt body scanners at all, because of evidence that they're not effective at detecting low density contraband, the handful of European airports that have adopted body scanners, such as Schiphol airport in Amsterdam, have chosen the blob machine over the naked machine.

The Schiphol blob machines contain another important privacy protection: images cannot be stored and transmitted. These choices reflects principled opposition to the naked machines, voiced by European privacy commissioners like Germany's Peter Schaar, who have emphasized the importance of designing body scanners in ways that protect privacy. "So far I have not seen a machine that protects personal rights," [5] Schaar said earlier this year.

In the U.S., the Department of Homeland Security made a very different choice, deploying the body scanners without any opportunity for public comment, and then appearing surprised by the backlash. The U.S. has implemented naked machines, not blob machines, and the Department of Homeland security required vendors to offer machines that were capable of storing and transmitting images, although a DHS privacy analysis emphasized that DHS has chosen to disable this capability after it was revealed by a Freedom of Information Act suit by the Electronic Privacy Information Center.[6] The Chief Privacy Officer of DHS did not insist on the two privacy features that European regulators have found crucial – namely blobbed images and no storage capacity of the machines. If both of these features were mandatory, they would address many of the privacy concerns and would shore up the argument that the machines are not unreasonable strip searches prohibited by the Fourth Amendment.[7]

[5] http://www.thelocal.de/national/20100105-24357.html
[6] http://epic.org/privacy/body_scanners/DHS_PIA_07_23_09.pdf
[7] For an argument that the naked machines are unconstitutional, see http://www.washingtonpost.com/wp-dyn/content/article/2010/11/24/AR2010112404510.html

A range of other surveillance technologies might be reasonable or unreasonable depending on whether they implemented with similar constraints – from warrantless 24/7 GPS searches placed secretly by the police under a suspect's car to the warrantless data mining that hopes to identify suspicious patterns of behavior that might prevent terrorism.

The model for all these acts of constitutional translation is the great prophet of the need for the Constitution to adopt in light of new technologies: Louis Brandeis. In his visionary dissenting opinion in the Olmstead case (1928), Brandies objected that a majority of the Court had approved the warrantless wiretapping of a suspected bootlegger. As private life had begun to be conducted over the wires in the age of radio, Brandeis observed, telephone conversations contained even more intimate information than sealed letters, which the Supreme Court had held in the nineteenth century couldn't be opened without a warrant. To protect the same amount of privacy that the framers of the Fourth and Fifth Amendments intended to protect, Brandeis concluded, it had become necessary to translate those amendments into the twentieth century, extending them to prohibit warrantless searches and seizures of conversations over the wires, even if the invasions occurred without physical invasions.

In a remarkably prescient passage, Brandeis then looked forward to the age of cyberspace, predicting that technologies of surveillance were likely to progress far beyond wiretapping. "Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home," he wrote. In anticipation of those future innovations, Brandeis challenged his colleagues to translate the Constitution once again to take account of the new technologies, or else risk protecting less privacy and freedom in the twenty-first century than the framers of the Constitution expected in the eighteenth century.

In evaluating technologies from Perfect Citizen to the naked machines, Brandeis would never have tolerated arid abstractions about how we lose all expectations of privacy when we walk in public places, or enter the airport, to expose our data to third parties, which have the effect of giving citizens less privacy in the age of cloud computing than they had

during the founding era. Brandeis might hold instead, like some states, that government intrusions must be no greater than necessary, encouraging judges to balance the intrusiveness of the search against the seriousness of the crime being prevented, as juries used to do during the Founding era. Or he might attempt to define how much privacy citizens in a free society should be entitled to expect, regardless of society's expectations. What's clear is that Brandeis would have considered it a duty actively to engage in the project of constitutional translation in order to preserve the Framers' values in a very different technological world. As Brandeis put it, "If we would guide by the light of reason, we must let our minds be bold."

Jeffrey Rosen

Title: Professor of Law

Email: jrosen@law.gwu.edu

Education
B.A., Harvard University; B.A., Oxford University; J.D., Yale University

Jeffrey Rosen is a professor of law at The George Washington University and the legal affairs editor of The New Republic. His most recent book is The Supreme Court: The Personalities and Rivalries that Defined America. He also is the author of The Most Democratic Branch, The Naked Crowd, and The Unwanted Gaze. Rosen is a graduate of Harvard College, summa cum laude; Oxford University, where he was a Marshall Scholar; and Yale Law School.

Professor Rosen's essays and commentaries have appeared in the New York Times Magazine, The Atlantic Monthly, on National Public Radio, and in The New Yorker, where he has been a staff writer. The Chicago Tribune named him one of the 10 best magazine journalists in America and the L.A. Times called him, "the nation's most widely read and influential legal commentator." Professor Rosen lives in Washington, D.C., with his wife Christine Rosen and two sons.