NAKED SCANNERS, GPS TRACKING, AND PRIVATE CITIZENS: TECHNOLOGY'S ROLE IN BALANCING SECURITY AND PRIVACY

JEFFREY ROSEN†

Thank you so much, and it is a great pleasure to be here in Detroit, where my father was born eighty-five years ago. His father carved an inscription from the Skillman branch of the Detroit Public Library—"The Fountain of Wisdom Flows Through Books"—which remains one of my most cherished possessions.

You've asked me to discuss whether it is possible, after 9/11, to strike a sensible balance between privacy and security through law and technology. I will argue that it is indeed possible to strike a sensible balance. But often, the balance depends not on judges alone, but on legislators, regulators, technologists, and, ultimately, on an engaged citizenry, reflecting a national consensus about what sort of privacy invasions are reasonable and unreasonable. I will give specific examples of areas where the balance has been struck. I will suggest that it is easier to strike that balance when responding to government invasions of privacy, than when responding to invasions of privacy by the private sector—by companies like Google and Facebook, which today have more power over privacy and free speech than any King, President, or Supreme Court Justice.

To frame my remarks, I would like to use an example that has divided the nation since 9/11. The story took a surprising turn this week that I could never have predicted when the debate began. This is the story of the choice between the naked machine and the blob machine. In 2004, officials at Orlando airport began testing the three dimensional millimeter wave machines that have recently provoked a national controversy. When they were originally proposed to the government, federal officials faced a choice: either they could adopt the naked machine or the blob machine. The naked machine showed graphic images of the naked body, and the blob machine, proposed by the designers at the Pacific Northwest laboratories, took pictures of the naked body and scrambled them into a nondescript blob, a sexless avatar, with arrows pointing to areas where contraband was supposed to have

† Professor of Law, George Washington University Law School; Legal Affairs Editor, *The New Republic*. B.A., 1986, *summa cum laude*, Harvard University; B.A., 1988, Oxford University; J.D., 1991, Yale University.

been concealed. It was obvious in 2004, as it is now, that the choice between the naked machine and the blob machine is, from a privacy and security perspective, as they say, a "no-brainer." Both machines promised the same degree of security, except that one protected privacy, and the other gravely and grossly invaded it. I would have thought, therefore, that any sane attempt to balance privacy and security would choose the blob machine over the naked machine.

In Europe, that is just what happened. Most European airports refused to adopt millimeter wave machines at all because of concerns about their effectiveness. People who tested them in Britain concluded that they would not have detected the low-density contraband used by the Christmas trouser bomber. So for that reason, most European airports rejected the machines on the grounds that they were not worth the money. But the handful of European airports that did adopt these machines, such as Schiphol airport in Amsterdam, chose blob machine-like versions, partly under pressure from European privacy commissioners.

In America, the government made a different choice. The Homeland Security Department Privacy Office, several years ago during the Bush Administration, evaluated the technology and approved the naked machines without insisting on the blob machines. More recently, under President Obama, the new Homeland Security Department Privacy Office again endorsed the naked machine without insisting on the blob machine. This fall, the naked machines were rolled out at airports, and when they were combined with a new regulation requiring highly intrusive, degrading, and embarrassing pat downs of people who opted out, they provoked an unexpected national protest. We saw a dramatic example of grass roots activism. The man who unforgettably exclaimed, "don't touch my junk," became the Patrick Henry of the anti-naked machine movement.[1] His grass roots protest was combined with legal challenges of groups like the Electronic Privacy Information Center ("EPIC"), which filed lawsuits challenging the naked machines as unconstitutional. The James Madison of the anti-naked machine movement is sitting in this room—Marc Rotenberg of EPIC, who argued the case in the U.S. Court of Appeals for the D.C. Circuit.

There is a strong argument that naked machines are unconstitutional and unreasonable under the Fourth Amendment. The Supreme Court, in evaluating search technologies, has said that a reasonable search is one

1. *See generally* Andy Goldberg, *'Don't Touch My Junk' Case Sparks US Airport Revolt*, MONSTERS AND CRITICS (Nov. 21, 2010), http://www.monstersandcritics.com/news/usa/features/article_1600527.php/Don-t-Touch-My-Junk-case-sparks-US-airport-revolt.

that focuses on illicit information or contraband, without revealing innocent or embarrassing information. So the paradigm example of a reasonable search is a dog sniff, as the court said in the 1983 opinion, *U.S. v. Place*.[2] Justice O'Connor said that since the dog sniff reveals drugs but does not reveal any innocent but embarrassing information, it is quintessentially reasonable.[3] Under that analysis, the naked machine is the antithesis of a reasonable search: it reveals a great deal of innocent, but embarrassing information, and is ineffective at detecting contraband. Furthermore, there is a lower court opinion written by Judge Samuel Alito, before he joined the Supreme Court, stressing that screening procedures have to be minimally intrusive and effective.[4] In other words, they have to be well-tailored to protect personal privacy, and have to deliver on their promise of discovering serious threats.[5]

Under this analysis, a court might conclude that the naked machines are not minimally intrusive, since they could be designed in blob machine-like ways. In addition, they have the capacity to store and transmit information—the TSA claimed that that capacity was disabled, but later changed its story. When confronted with a Freedom of Information Act request filed by EPIC, it admitted that the capacity to transmit information could be turned back on, which further supports the claim that the machines do not involve a minimally intrusive process. So for all these reasons, it is possible that courts might strike down the naked machines as unreasonable under the Fourth Amendment.

Fortunately, the need for Rotenberg's lawsuit may have been diminished this week by a surprising and significant announcement. The TSA announced that it would begin testing blob machine software at selected airports.[6] In Las Vegas, Atlanta, and Washington, D.C., the TSA said it would implement filtering software that will essentially only reveal to screeners a blob-like nondescript generic outline of a person that will appear on a monitor attached to the screening unit.[7] The area identifying potential threats will require additional screening; if no potential threat items are detected, "OK" will appear on the monitor.

---

2. 462 U.S. 696 (1983).

3. *Id.* at 698.

4. United States v. Hartwell, 436 F.3d 174, 180-81 (3d Cir. 2006), *cert. denied*, 549 U.S. 945 (2006).

5. Jeffery Rosen, *Why the TSA pat-downs and body scans are unconstitutional*, WASH. POST (Nov. 28, 2010), *available at* http://www.washington.com/wp-dyn/content/article/2010/11/24/AR2010112404510.html.

6. Press Release, Transportation Security Administration, TSA Begins Testing New Advanced Imaging Technology Software (Feb. 1, 2011), *available at* http://www.tsa.gov/press/releases/2011/0201.shtm.

7. *Id.*

TSA officers will no longer be sitting in separate rooms remotely viewing naked images, and much of the objection to the naked machines on privacy grounds will evaporate. (The concerns about effectiveness remain.) This is big news. I never anticipated seven years ago that TSA would finally embrace the choice it should have made at the outset.

What is the moral of this story? It is that political protests and engagement are crucial. By itself, I do not think that the EPIC lawsuit would have been enough. Judges are generally reluctant to impose conceptions of privacy that they feel are not broadly supported by the people. It was not national majorities that rose up against the naked machines, but only an engaged minority, and that was enough to focus the attention of policy makers. The combination of engaged political protests and the threat of lawsuits ultimately led to regulatory action.

The same dynamic will be crucial as the country faces other technological choices involving national security over the coming decades. Are they more likely to lead to blob machines or naked machines? Part of the answer may depend on whether or not the threat that they pose can be grasped by citizens in a dramatic and personal way that is likely to inspire the sort of protest and demand for a sensible blob machine technology.

With that in mind, my second example involves a new screening and cyber security system called Perfect Citizen. In July 2010, the Wall Street Journal first reported the existence of Perfect Citizen, [8] which was formally rolled out recently in a speech by Secretary Napolitano in Washington.[9] Perfect Citizen is designed to identify cyber assaults on critical infrastructure controlled by the public and private sectors, including the electricity grid. The surveillance will rely on a set of sensors deployed in the computer network that will be triggered by unusual activities suggesting an impending cyber attack. Perfect Citizen seems to represent an extension into the private network of cyber attack detection and prevention systems currently in place on government computers. Jack Goldsmith describes this in a paper for the Brookings Project on Technology and the Constitution.[10] This system will use

---

8. Siobhan Gorman, *U.S. Plans Cyber Shield for Utilities, Companies*, WALL ST. J. (July 8, 2010), *available at* http://online.wsj.com/article/SB10001424052748704545004575352983850463108.html.

9. Janet Napolitano, Secretary, Department of Homeland Security, State of America's Homeland Security Address (Jan. 27, 2011), *available at* http://www.dhs.gov/ynews/speeches/sp_1296152572413.shtm.

10. Jack Goldsmith, *The Cyberthreat, Government Network Options, and the Fourth Amendment*, GOVERNANCE STUDIES AT BROOKINGS (Dec. 8, 2010), *available at* http://www.brookings.edu/~/media/Files/rc/papers/2010/1208_4th_amendment_goldsmith/1208_4th_amendment_goldsmith.pdf.

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.[11] Goldsmith imagines that Perfect Citizen may extend Einstein throughout public and private computer networks. He imagines that Perfect Citizen might be expanded to allow the NSA in "conjunction with private firms . . . to monitor the content of private internet communications, . . . store [them] temporarily, trace the source of malicious agents . . . all over the globe, . . . and take . . . steps to thwart malicious communications" in real time.[12]

Is Perfect Citizen a naked machine, a kind of privacy Chernobyl, which allows warrantless surveillance of all public and private communication without limits? Or could it be designed in a blob machine-like way that accurately and immediately identifies potential cyber threats without menacing innocent and harmless communications? Furthermore, would it be permissible under current law? Goldsmith argues that the government would probably, although not necessarily, need congressional authorization to implement Perfect Citizen in its more expansive form.[13] The Fourth Amendment, he notes, might not be viewed today to permit the unfathomably massive storage, copy, and analysis of private communications that Perfect Citizen calls for.[14] On the other hand, courts might approve the collection and analysis of the information on the grounds of the Third Party Doctrine,[15] which holds that when you disclose information to third parties you assume the risk that it may be disclosed to the government. Also, the courts could rely upon the Special Needs Doctrine, which makes an exception to the Fourth Amendment for reasonable government actions with purposes that go beyond routine law enforcement.[16]

But although it is possible that the courts might strike down Perfect Citizens in its current form, Goldsmith argues, and I agree, that to be reasonable, Perfect Citizen would have to have at least three privacy protecting mechanisms.[17] First, storage and viewing restrictions—in other words, the fact that only communications viewed by human beings are very suspicious would increase the reasonableness of the program.[18] Second and most important, use restrictions to ensure that only cyber

11. *Id.* at 4.
12. *Id.* at 9.
13. *Id.* at 15.
14. *Id.* at 11.
15. *See* U.S. v. Miller, 425 U.S. 435, 443 (1976).
16. Goldsmith, *supra* note 10, at 11-12. *See also* Bd. of Educ. of Indep. Sch. Dist. No. 92 v. Earls, 536 U.S. 822 (2002).
17. Goldsmith, *supra* note 10, at 15-16.
18. *Id.* at 15.

threats are targeted.[19] The government could place use restrictions on communications containing malicious signatures allowing them to be stopped or destroyed but not introduced in court as evidence in unrelated cases that do not involve national security, terrorism, or serious crimes.[20] The model here is the original Wiretapping Act, the Crime Control Bill of 1968, which originally allowed wire taps only for violent felonies, but not for low level crimes.[21] The problem with use restrictions is mission creep—today, most wire taps are allowed for non-violent felonies because of the political pressure to allow broad surveillance for non-violent, as well as violent, crimes. That is why the Germans, who allow their intelligence services broad authority to surveil without warrants, do not allow that information to be shared with the police unless it relates to violent crimes or terrorism. So that idea of use restrictions is the blob machine version that could make Perfect Citizen consistent with the Fourth Amendment. Goldsmith's third requirement is minimization requirements, to ensure that communications that do not prove to be threatening are destroyed, and that suspicious communications are examined in ways that reveal no more privacy than is necessary.[22]

It is hardly obvious, of course, that Perfect Citizen will be implemented in this blob machine way—including use restrictions, minimization requirements, and so forth. Citizens have more difficulty personalizing the threat posed by data mining than by naked machines. Because the threat is diffuse and abstract, rather than concrete and personal, Congress may well not require use restrictions. During the debate over the Patriot Act, Senator Feingold, the only Senator to vote against the Patriot Act, said that he might have accepted much of the expansion of police authority that the Patriot Act allowed as long as use restrictions were implemented and that the evidence discovered could only be introduced in terrorism cases, but not other cases.[23] But Feingold found no political constituency for these rules and restrictions. Even in post-9/11 Germany, the pressure to catch terrorists has caused use restrictions to be relaxed. So my second example points to the same

19. *Id.* at 15-16.

20. *Id.*

21. 18 U.S.C. §§ 2510-2522 (2006).

22. Goldsmith, *supra* note 10, at 16.

23. *USA Patriot Act*, ELECTRONIC PRIVACY INFORMATION CENTER, http://epic.org/privacy/terrorism/usapatriot/default.html#introduction (last visited Nov. 7, 2011). Senator Wyden made similar points during the debate over the reauthorization of the Patriot Act. *See* Ron Wyden, *Patriot Act: Congress Shouldn't Rush to Judgment (Again)* HUFFINGTON POST (Oct. 28, 2009), *available at* http://www.huffingtonpost.com/sen-ron-wyden/patriot-act-congress-shou_b_336504.html.

conclusion as the first—that in order to strike the sensible blob machine-like balance, you need privacy protections that the majority of citizens, or at least substantial and vocal minorities of engaged citizens, will actually demand.

My third example is Ubiquitous Surveillance, beginning with the possibility of global positioning system ("GPS") tracking. Already the police are trying to track suspects' moves with location-sensitive geopositioning devices. These efforts are already being challenged in court. The cases that have been decided recently arise out of efforts by the police to put GPS devices without a warrant on the bottom of suspects' cars and trace their movement twenty-four seven. Is this consistent with the Fourth Amendment? Courts have disagreed. Unsurprisingly, some courts have held that there is no expectation of privacy in public. Because any neighbor could theoretically tail you and trace your movements at all times, the cops can use low cost devices like GPS devices to achieve the same surveillance with much less effort. However, in a visionary decision, Judge Douglas Ginsburg on the U.S. Court of Appeals for the District of Columbia Circuit struck down warrantless GPS tracking.[24] "[U]nlike one's movements during a single journey," he noted persuasively, "the whole of one's movements over the course of a month is not actually exposed to the public because the likelihood that anyone would observe all these movements is effectively nil."[25] He cited the Overflight cases, such as *California v. Ciraolo*, where the government had hired a helicopter and saw someone growing pot in the backyard.[26] A majority of the Supreme Court said there is no constitutional problem because any ordinary member of the public could, in theory, rent a helicopter and fly over people's backyards; we have to assume the risk that our neighbors are doing so.[27] Justice O'Connor's concurring opinion took a more pragmatic approach. She said the question should be whether ordinary members of the public use technology in this way, or is this an unexpected use?[28] And applying that theory, Judge Ginsburg held that the fact that neighbors do not track us twenty-four seven shapes our expectations that the whole of our movements will not be tracked in public.[29] Moreover, Ginsberg argued that "[p]rolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly [or]

24. *See* U.S. v. Maynard, 615 F.3d 544 (D.C. Cir. 2010).
25. *Id.* at 558.
26. 476 U.S. 207 (1986).
27. *See generally* Florida v. Riley, 488 U.S. 445 (1989).
28. *Id.* at 454.
29. *Maynard*, 615 F.3d at 562.

does not do."[30] This information can "reveal more about a person than [just] any individual trip viewed in isolation."[31] Ginsburg was willing to translate the values of the Fourth Amendment into the technological age. He did not accept the wooden reasoning of the lower courts that there is no expectation of privacy in public, or the idea that if we surrender data to a third party we lose all expectation of privacy. He understood that ubiquitous surveillance of all one's movements is different in degree, not just in kind, from a snapshot that can only reveal one's movements at one brief and contained moment.

Will the Supreme Court agree? Again, I am not going to predict anything, but I think we would need some sort of national engagement and public consensus that ubiquitous surveillance is unreasonable in order to persuade the justices to impose restrictions on it. That is why I am impressed that as courts are wrestling with the Fourth Amendment status of this new monitoring, Senator Ron Wyden, the Oregon Democrat, along with Representative Jason Chaffetz, the Utah Republican, have drafted legislation to set standards for government access to geolocation data.[32] That interaction of legislation with political engagement will be necessary to create the consensus about Fourth Amendment reasonableness that is necessary to persuade the Supreme Court.

My final example is WikiLeaks,[33] which has emerged as a platform that has done some good in publishing whistleblowing documents, but has also needlessly invaded privacy with its unedited document dumps. It usefully published the Apache helicopter video last Spring, documenting the killing of several individuals in Baghdad,[34] but only a fraction of its leaks can be considered whistleblowing documents that expose serious wrongdoing—from criminal activity to the abuse of authority, and the waste of public resources. The vast majority involve the routine records of governmental operations—an attack on the entire notion of governmental secrecy. Unlike responsible publishers such as the New York Times, Wikileaks lacks editorial judgment and often abdicated the editorial function entirely, releasing tens of thousands of documents at a time relating to the Iraq and Afghan wars, few of which were actually newsworthy. The privacy implications are troubling. Wikileaks has

30. *Id.*

31. *Id.*

32. Press Release, Rep. Jason Chaffetz, *Chaffetz, Wyden Introduce GPS Act: Bipartisan Legislation Provides Needed Legal Clarity for Use of Geolocation Information,* (June 15, 2011), *available at* http://chaffetz.house.gov/press-releases/2011/06/chaffetz-wyden-introduce-gps-act.shtml.

33. WIKILEAKS, http://www.wikileaks.org (last visited Nov. 7, 2011).

34. *Collateral Murder*, WIKILEAKS (April 5, 2010), http://www.collateralmurder.com.

published the raw police file of a Belgian politician who allegedly associated with a pedophile who was jailed for murdering children,[35] but, in fact, the accusations were false. So, document dumps can threaten privacy as well as national security—people in Afghanistan will be deterred from cooperating with the U.S. government if they are not confident that their identities will be kept confidential.

What is the correct regulatory response? Certainly not espionage and prosecutions, which are being threatened by Senator Joe Lieberman, who has emerged as a kind of A. Mitchell Palmer of the digital age.[36] Lieberman proposed to amend the Espionage Act to allow the prosecution of publishers, as well as leakers. This would be a grave error. As a constitutional matter, it is impossible to distinguish between the New York Times and WikiLeaks. Here is a case where a legal response, to protect privacy and secrecy, would gravely threaten free speech.

But as an editorial matter, there is a big difference between Wikileaks and the New York Times, namely that the New York Times exercises editorial judgment, and only publishes those documents it believes to be in the public interest. That is why I think the better response to the privacy threats of WikiLeaks is technological. A disgruntled WikiLeaks staffer, Julian Assange's former deputy, Daniel Domscheit-Berg, has created an alternative site called OpenLeaks,[37] which will not publish any documents, but instead will serve as a conduit that allows anonymous sources to deposit leaked information in a secure drop box and then designate the news organizations or NGOs of their choice to receive the information, determine whether or not it is newsworthy, and engage in fact-checking and redaction.[38] OpenLeaks would preserve the benefits of WikiLeaks, while avoiding the dangers. But, as in the case of the blob machine, the choice of OpenLeaks over WikiLeaks requires newspapers, editors, and citizens to make voluntary

---

35. *New WikiLeaks Row Over Pedophile Dossier*, THE AUSTRALIAN (Aug. 28, 2010), *available at* http://www.theaustralian.com.au/news/world/new-wikileaks-row-over-pedophile-dossier/story-e6frg6so-1225911056437. *See also* Jeffrey Rosen, *The New York Times vs. WikiLeaks*, THE NEW REPUBLIC (Apr. 27, 2011), *available at* http://www.tnr.com/article/politics/87443/wikileaks-guantanamo-new-york-times-journalism.

36. Jeffrey Rosen, *The Deciders: Facebook, Google, and the Future of Privacy and Free Speech*, THE BROOKINGS INSTITUTE (May 2, 2011), *available at* http://www.brookings.edu/papers/2011/0502_free_speech_rosen.aspx.

37. OPENLEAKS, http://www.openleaks.org (last visited Nov. 7, 2011).

38. *See* About Open Leaks, OPENLEAKS, http://www.openleaks.org/content/about.shtml (last visited Nov. 7, 2011). *See also* Rosen, *supra* note 35.

choices to work with technologies that preserve privacy and security rather than threaten them.

I take from all four of these examples the following lesson, namely that in efforts to balance privacy, security, and liberty, there is often a blob machine-like solution—a sensible way of designing or regulating the technologies that strikes a reasonable balance between competing values. From the blob machine itself to use restrictions on Perfect Citizen, the warrant requirement for GPS tracking, and OpenLeaks rather than WikiLeaks, it is possible to protect liberty, privacy, and security at the same time. In all four cases, the good balance was often achieved by a combination of political protests and legal threats, which led to a transformation in norms and the adoption of better technologies that protect privacy by design. In every case, in other words, the right answer comes not just from judges or statutes or constitutional doctrine alone, but from the actual norms of an engaged public. And that is why, although the challenges that confront us are complicated, the courts alone cannot save us, laws alone cannot save us, and regulators alone cannot save us. The only thing that can save us is engaged activism by people like you.