Isaac Marks Memorial Lecture

THE NAKED CROWD: BALANCING PRIVACY AND SECURITY IN AN AGE OF TERROR

Jeffrey Rosen*

It is a great pleasure and honor to come to Tucson as the twenty-fourth annual Marks lecturer. I have been looking forward to coming here for several reasons: first, because of the weather—I am told it never rains; second, because of your distinguished faculty; and third, because the roster of past lecturers includes not only one of my greatest teachers, Bruce Ackerman, who taught me to revere the study of the Constitution; but also my judge, Abner Mikva. To be a member of their company is a high honor indeed.

Yesterday evening, I had the pleasure of meeting Selma Marks, the woman who has kindly given me the chance to talk today. During our brief conversation, I could tell that she is a force of nature. Her intelligence, liveliness, and interest in ideas are palpable. She has honored the University of Arizona by creating this lectureship, and I hope to justify that honor by talking today about the subject that engages me more than any other: the balance of privacy and security after September 11.

When I was invited to speak here two years ago, I had just written about the destruction of privacy in America in the Internet age.[1] Now, two years later, we are told that everything has changed. I am not convinced. I will try to persuade you of a thesis, which you may or may not find too optimistic. My thesis is that it is possible through law and technology to strike a reasonable balance between privacy and security.

I will describe what the technologies and legal arrangements might look like if they were modified to achieve this balance between privacy and security;

---

* Jeffrey Rosen is a law professor at George Washington University and the legal affairs editor of *The New Republic*. This lecture is transcribed from his spoken remarks at the Twenty-Fourth Annual Isaac Marks Memorial Lecture on Mar. 4, 2004.

1. JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA (Random House, Inc. 2000).

and then I will ask us to think together about who is most likely to guarantee this effective balance. Is it the public, the courts, the Executive, or Congress? Perhaps heretically, standing here as a Marks lecturer, I will argue that if we are to be saved, we should not expect judges to be our saviors. Instead, salvation must come from a combination of Congressional resistance and Executive leadership. But the question of how to achieve the right balance is complicated.

What is an example of the kind of balance that I have in mind? Consider a technology that is being tried out now at airports, in particular Orlando International Airport.[2] It is a technology that we might call, for the sake of argument, the naked machine. It is an electronic, three-dimensional holographic imaging machine that uses a high-beam X-ray to bounce off the human body.[3] It reveals not only metal, but also plastics, ceramics, and any objects concealed under clothing. In addition to the extremely accurate vision of any contraband, it reveals the human body completely naked. It is an electronic strip search.

Given the choice between waiting for five minutes in line and being naked, many people are happy that there is a naked machine. Some say they are exhibitionists, others say that they have a low expectation of privacy in airports, and still others say that they are so afraid of flying now that they would do anything to ritualistically prove their own innocence. They want to strip themselves bare as a demonstration of their own trustworthiness.

But the naked machine does not have to be designed in ways that invade privacy while protecting security. The people who designed it at the Pacific Northwest National Laboratories also came up with a simple program shift that enables images of contraband to be projected onto a sexless mannequin, while the images of the naked body are scrambled so that they resemble a nondescript blob.[4] This wonderful machine—call it the blob machine—is obviously for most of us an act of mercy.

The blob machine is a vivid example of a silver bullet technology. It promises complete protection for both security and privacy by revealing guilty information, while scrambling and concealing innocent information. As a paradigm, the blob machine could be a model for future technological and legal choices that have emerged following September 11. The range of technologies—identification cards, data line systems, surveillance cameras—can all be designed in ways to look more like the blob machine than the naked machine. In addition,

---

2. The Greater Orlando Aviation Authority announced its involvement in the Advanced Technology Checkpoint Project on Mar. 14, 2002. Press Release, Greater Orlando Aviation Authority, Advanced Technology Checkpoint Project Begins at Orlando International Airport (Mar. 14, 2002), http://www.orlandoairports.net/goaa/press/20020314.htm.

3. Kevin Maney, *The Naked Truth About Possible Airport Screening Device*, USA TODAY, Aug. 7, 2002.

4. Mick Hamer, *All-Seeing Scan Spares Your Blushes*, NEW SCIENTIST, Aug. 17, 2002.

the Patriot Act[5] could also be refined in ways to look more like the blob machine than the naked machine.

Let me now provide a few examples of the blob-like technologies and laws that I have in mind, and then we can think through how they might be adopted.

First, let us begin with a cautionary tale, a technology that might in theory be designed in a blob-like way, but instead was deployed in a manner that makes it closely resemble the naked machine. This is the example of surveillance cameras in Britain. I had not been to Britain for ten years, but I went right before September 11. I was struck by the fact that in the course of a decade, the cradle of the Magna Carta, the birth of American liberties, had wired itself up to so many surveillance cameras that it resembled the set of the Truman Show.[6] It has been an extraordinary sociological phenomenon. There are over 4.2 million cameras in the country, although people have stopped counting.[7] The average Brit is said to be photographed 300 times a day.[8] One is struck getting off the airplane by the proliferation of cameras. They follow you through the airport, down the metro, inside the metro station, as you take the escalator to the street, in the taxicabs, and in the hospitals. All over are warning signs, "CC-TV Surveillance" or "CC-TV Watching."

Britain began using surveillance cameras in the 1990s in response to fears of terrorism.[9] A series of IRA bombings led the Government to create a ring of steel that combined cameras on each of the thirteen gates to London and promised to provide an invisible shield against threats of terror.[10] However, the cameras were quickly deployed for very different purposes. When I asked the chief in charge of deploying the cameras whether they caught any terrorists, he replied, "No, not using this system." Well then, what is their use? They are now used to charge a five-pound car-tax for every car that comes into the city and an extra tax if the car does not leave on time.

There was also the hope that these cameras might be deployed with biometric databases that would contain the faces of known terrorists. In London, the Borough of Newham actually implemented this system,[11] but the Borough did not enter the faces of known terrorists—because if the terrorists are known, of course, we could catch them—but instead entered the faces of a few thugs who acted up in shopping malls and were wanted for minor crimes of disorder.[12] In addition, the biometrics are very inaccurate. They cannot tell the difference

---

5. The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001, Pub. L. No. 107-56, 115 Stat. 272.

6. THE TRUMAN SHOW (Paramount Pictures 1998).

7. JEFFREY ROSEN, THE NAKED CROWD: RECLAIMING SECURITY AND FREEDOM IN AN ANXIOUS AGE 36 (Random House, Inc. 2004).

8. *Id.* at 37.

9. *Id.* at 34–35.

10. *Id.* at 35.

11. *Id.* at 42.

12. *Id.* at 43.

between a man and a woman[13] and are easily defeated by disguises.[14] In fact, the cameras are often turned off.[15] They are designed to make people feel like they are being watched even though they are not.[16] They are a form of panoptic-like surveillance.

These cameras are designed to make people feel safe even if they do not actually make people safer. The British public, it turns out, faced with the British Government's own study suggesting that there was no connection between the proliferation of the cameras and the decline of violent crime or terrorism, was indignant. They viewed the cameras not as big brother, but as a kindly, watchful uncle or aunt. John Major and Tony Blair spent more money on cameras than any other device for crime control, and the cameras continue to proliferate. Now, it is possible to imagine a blob machine-like version of the cameras if the biometric database were limited to known terrorists, and the images were not to be stored. This would avoid the specter of ubiquitous surveillance, by which it might be technologically possible in the near future to flip or click on a picture of people in the London metro, backward click on them to see where they came from, and forward click on them to see their destination

Britain, unlike America, is a country with a strong deference to authority, with a greater tolerance of hierarchy, without constitutional checks and balances, without a separation of the Executive and Legislature, and without a strong libertarian anti-government tradition. The British public eagerly embraces a feel-good technology in the face of empirical evidence suggesting its ineffectiveness as a deterrent for crime or for terrorism. We should heed the warnings of the British surveillance cameras and the Orlando airport naked machine, and acknowledge what the unchecked public, inflamed by fears of terror, may precipitously demand.

Let me now focus on America. The current most controversial technologies involve data mining systems, which analyze a great degree of electronic data: public databases that contain our criminal history and private databases that contain our browsing purchases, our magazine subscriptions, and our consumer habits. Based on the consolidation of this public and private information, it was proposed after September 11 to engage in ambitious forms of what Roger Clarke has called "mass dataveillance" to consolidate and analyze public and private data in the hope of unearthing unusual patterns that might predict suspicious activity.[17] The most ambitious form of mass dataveillance proposed after September 11 was the "total information awareness system." Total information awareness, in its unregulated form, was the naked machine version of general dataveillance. It proposed to combine databases held by state and federal governments with private data held by companies like ChoicePoint and Axiom and, using a technology called neural network analysis, look for suspicious behavior.[18]

---

13. Jeffrey Rosen, *A Watchful State*, N.Y. TIMES MAG., Oct. 7, 2001.
14. *Id.*
15. ROSEN, *supra* note 7, at 42.
16. *Id.* at 42–43.
17. *See* Privacy Act of 1974: System of Records, Notice to Amend a System of Records, 68 Fed. Reg. 2,101, 2,102 (Jan. 15, 2003).
18. *Id.*

So, for example, if a traveler bought fertilizer and a one-way ticket and took flight lessons in Florida, he or she might be tagged for special searches. The possibility that this traveler might be a retired businessperson who was a gardening aficionado would not be evidently detectable by the system. The premise of mass dataveillance was that these sorts of predictive patterns could in fact identify bad people and target them for special searches.

What is the danger of mass dataveillance in its unregulated form? Why does it strike me as a naked machine rather than a blob machine? In many ways, it possesses some of the same dangers that the framers of the Fourth Amendment intended to prohibit. Recall that the paradigmatic example of an unreasonable search under the Fourth Amendment was the general warrant, which allowed the king to break into the homes of any number of citizens in search of suspicious information without particularized suspicion and without limitations on its use. Searching for the author of the seditious pamphlet, *The North Briton*, No. 45, written by the British rogue patriot John Wilkes, which criticized King George's mother for having an affair with a foreign secretary, King George dispatched Lord Halifax, his Ken Starr figure, to search the desk drawers of thousands of citizens.[19] Based on this general search—this fishing expedition—the King identified Wilkes as the author and prosecuted him.[20] Wilkes objected that his most intimate secrets had been exposed to the world, that this was an unreasonable search.[21] In those days, the remedy for an unreasonable search was a trespass action, not exclusion. Wilkes won his suit in a ruinous verdict of a thousand pounds, the McDonald's verdict of its day.[22] He persuaded a jury that paper searches, at least for low-level crimes, like seditious libel, were inherently unreasonable. Lord Camden vindicated this principle in an opinion that Justice Louis Brandeis would later praise as a high watermark of American liberties.[23]

The principle of the Fourth Amendment is that unregulated paper searches threaten us with discriminatory prosecution that allows the king to retaliate against his political enemies. It is a version of the Nixon effect; the modern version of the general search is President Nixon's effort to scan the tax returns of Vietnam protestors and threaten them with prosecution.

Could total information awareness in its unregulated form be a version of the general search that might lead to the Nixon effect? It might indeed. Given unregulated access to reading and browsing habits of law professors who criticize the government, an unscrupulous administration could easily scour consumer data searching for low-level forms of wrongdoing or for embarrassing Internet information, and then threaten us with prosecution or exposure.

This is the theoretical harm that we are trying to avoid. And it can be avoided. There is no reason to design total information awareness data systems that threaten the Nixon effect. We can imagine a blob machine version of a general

---

19. ROSEN, *supra* note 1, at 27–28.
20. *Id.* at 28.
21. *Id.*
22. *Id.* at 29.
23. Olmstead v. United States, 277 U.S. 438, 474–75 (1928) (Brandeis, J., dissenting) (citing Boyd v. United States, 116 U.S. 616, 630 (1886)).

dataveillance search. Such a version is more or less being arrived at in the current version of the data-mining project, which may be employed at airports later this year, and is called Computer Assisted Passenger Pre-Screening System (CAPPS-II).

The CAPPS-II architecture resembles the general dataveillance proposed by total information awareness. It proposes integrating public databases with the private and consumer data held by folks such as Lexis-Nexis, Choice Point, and Axiom and sorting travelers into different categories based on perceived local risks that they pose. Most travelers will be code green and sent through without distress, some will be yellow and taken on the side for more extensive searches, and some will be assigned red and taken into back rooms for bludgeoning and so forth.

But CAPPS-II, although originally structured to operate as a naked machine, has been refined in two ways. First, it is no longer designed for general predictive profiling.[24] It is not designed to ask whether individuals look like the September 11 terrorists; it is only designed for purposes of authentication or verification.[25] It is supposed to confirm the individual traveler's identity, rather than classifying him or her based on dangerousness.[26] Second, and even more important, in response to the criticisms of privacy advocates, CAPPS-II embraced an important limitation on the use of data. The government may not forward to law enforcement evidence of any low-level wrongdoing that it discovers and can only forward evidence of outstanding warrants for violent state or federal crimes.[27]

The use-limitation strikes me as a central insight, a tremendous victory for privacy, and a model for the blob machine versions that we might think about across the range of surveillance technologies. It is a version of the use-limitations embraced by the Germans, who, based on their unfortunate experience with Nazism and Fascism, devised some of the most effective and sensitive protections for privacy in a national security state. The German Intelligence Service has broad surveillance powers, but the intelligence officers are not allowed to forward to their law enforcement officers evidence of low-level crimes that they find in the course of their investigation and can only forward evidence of violent crime or terrorism.[28] For example, when applying this rule, German courts have excluded evidence from diaries in adultery prosecutions found in intelligence investigations because the invasiveness of the search is disproportionate to the seriousness of the crime.[29]

I want to suggest other use-limitations that might inform our thoughts about other forms of surveillance, and this leads me to the Patriot Act. After having looked at the Patriot Act and taught it for the past two years, I find some of the criticisms overstated. For example, the criticisms of new uses of roving

---

24. Privacy Act of 1974: System of Records, Notice of Status of System Records, 68 Fed. Reg. 45,265, 45,266 (Aug. 1, 2003).

25. *Id.*

26. *Id.*

27. *Id.*

28. *See* Craig M. Bradley, *The Exclusionary Rule in Germany*, 96 HARV. L. REV. 1032, 1042–43 (1983).

29. *See id.*

wiretaps appear unjustified, because the act fills technical holes in the law and allows certain forms of electronic communications to be treated under the same rules that have been used for snail-mail and non-electronic forms of communication. However, some aspects of the Patriot Act are indeed troubling. Perhaps most troubling is the section that so inflamed America's librarians, who are our greatest civil libertarians, and this is Section 215.

Before we address Section 215, consider the broad surveillance authority authorized by the Foreign Intelligence Surveillance Act (FISA).[30] Before Section 215, FISA allowed searches without particularized suspicion of wrongdoing and allowed these searches to take place in secret without notice to the individual concerned.[31] However, it only suspended the ordinary Fourth Amendment requirements of particularity and individualized suspicions after an individual had been identified in advance as unusually suspicious.[32] Before Section 215, the government had to prove that there was probable cause to believe the individual was an agent of a foreign power or a suspected spy or terrorist before engaging in this broad form of surveillance.

Section 215 of the Patriot Act, along with the National Security letters that it authorizes, broadens the government's surveillance authority in two ways. First, it removes the requirement that an individual be identified in advance as a suspected spy or terrorist.[33] It allows for secret searches of databases held by third parties without notice to the individual, as long as the government merely certifies that the information is relevant to a terrorism investigation.[34] Second, the Patriot Act broadens the category of the data that may be searched. Before, only certain categories of information, such as bank records, could be searched. Now, any tangible data can be searched.[35]

Section 215 of the Patriot Act resurrects some of the dangers of general searches or the vindictive Nixon-effect retaliatory prosecution that the framers of the Fourth Amendment feared. The Attorney General could, in theory, decide to silence the law professors who criticize him and go to all the Internet service providers without notice to us, discover our data, and prosecute or embarrass us based on low-level crimes.

Restoring the particularity requirement would refine the Patriot Act. Indeed, the SAFE Act, proposed by a bipartisan coalition in Congress, would revive the pre-Patriot Act requirement that an individual be a suspected spy or

---

30. Foreign Intelligence Surveillance Act (FISA), Pub. L. No. 95-511, 92 Stat. 1783 (1978) (codified as amended at 50 U.S.C. §§ 1801–1862).

31. *See id.*

32. Intelligence Authorization Act of Fiscal Year 1999, Pub. L. No. 105-272 § 601, 112 Stat. 2396, 2405 (amending FISA).

33. USA PATRIOT Act, Pub. L. No. 107-56 § 214(a)(3), 115 Stat. 272, 286 (striking 50 U.S.C. § 1842(c)(3)).

34. USA PATRIOT Act, § 214(a)(2), 115 Stat. at 286 (amending 50 U.S.C. § 1842(c)(2)).

35. *Compare* Intelligence Authorization Act, § 602, 112 Stat. at 2411 (amending FISA) *with* USA PATRIOT Act, § 215, 115 Stat. at 287.

terrorist before any searches can take place.[36] Whether or not it passes, the principle of the SAFE Act joined with the controlled-use model embodies the constitutional values that the Fourth Amendment was designed to protect. Personal dataveillance, searches of a specific individual, is only authorized when you identify an individual in advance as unusually suspicious. General dataveillance, searches of everyone without individualized suspicion, is only authorized with strong controls on the data's use. These two limitations might assuage many of the concerns of civil libertarians about the Patriot Act.

Who is most likely to embrace these use limitations? Is it the public, the courts, Congress, or the Executive? I am not putting my faith in the public. There is an informative poll that the Attorney General cited during his tour defending the Patriot Act. The poll says that half the public thinks the Patriot Act strikes a reasonable balance between privacy, liberty, and security. Twenty percent think it does not go far enough and twenty percent think it goes too far.[37] Regardless of the inaccuracies of polling and the difficulty of expressing an opinion about the complicated Patriot Act, this poll is instructive. It suggests that opponents of the Patriot Act are indeed, as the Attorney General says, a distinct and vocal minority. They are a bipartisan minority—a combination of civil libertarian liberals with libertarian conservatives. For example, Representative Butch Otter, one of the heroes of privacy in the recent Congress, proposed the Otter Amendment.[38] The Otter Amendment would deny funding for the enforcement of the sneak-and-peek provisions of the Patriot Act, which allow for searches without notice to individuals under the circumstances that had been allowed before.[39]

But the political reality is that the majority of the public, as the British example shows, faced with a choice between an immediate promise of security and illusory loss of privacy, will favor often security above privacy. And there is powerful evidence in the psychology of fear that supports this reality. The public tends to make decisions about security based on emotions rather than arguments.

Professor Paul Slovic, a behavioral psychologist at the University of Oregon, describes the psychology of fear in illuminating ways.[40] However, behavioral psychologists are reluctant to use the word "irrational"; they prefer "quasi-rationality." When faced with a transfixing and memorable image of a highly terrifying event such as the World Trade Center falling, a quasi-rational public will exaggerate the degree to which they are likely to be personally victimized.[41] People believe they are more likely to be killed in terrorist attacks than car accidents because they can remember the pictures of the terrorist attacks, whereas behind the wheel of a car they have an illusion of control.

After September 11, twenty percent of the public believed that they would be personally victimized by terrorist attacks in the next year, and fifty percent

---

36. Safety and Freedom Ensured Act (SAFE Act), S. 1709, 108th Cong. § 4 (2003).
37. USA Today/CNN/Gallup Poll (Aug. 25–26, 2003).
38. H.R. Amdt. 292, 108th Cong. (2003), *amending* H.R. 2799.
39. USA PATRIOT Act, § 213, 115 Stat. at 286 (amending 18 U.S.C. § 3103a).
40. PAUL SLOVIC, THE PERCEPTION OF RISK (Earthscan Ltd. 2000).
41. *See* ROSEN, *supra* note 7, at 71–75.

thought that their neighbors would be victimized.[42] Thankfully, these erroneous predictions turned out false. For the predictions to be true, a terrorist attack of the magnitude of September 11 would have needed to occur each of the 365 days after the initial attack. Behavioral psychologists and economists have many other examples of heuristics. The public has difficulty processing remote probabilities of highly terrifying fears, which might make them impatient with the complicated technological and legal choices outlined here and favor feel-good choices rather than ones that might strike a more thoughtful balance between privacy and security.

Who then will save us from ourselves? That question has confronted us since September 11. The excesses of public opinion and of a democracy present an old question that has been venerably described by my distinguished predecessors behind the podium. The place that lawyers tend to look for salvation from the excesses of the crowd is usually the courts. However, the American constitutional doctrine provides no obvious traditional remedy. There are many reasons for this. Let us think through a couple of the problems.

Surveillance cameras and database searches are generally unregulated by American constitutional law because American courts have held repeatedly that once I have surrendered privacy for one purpose, I have surrendered it for all purposes.[43] So, for example, if I turn over my personal data to ChoicePoint or LexisNexis, I have surrendered all expectations that the government will not use this information to classify me. With respect to surveillance cameras, I have no legitimate expectation of privacy in public once I voluntarily walk down the street. The possibility that my neighbor might follow me authorizes the government to follow me by placing a portable camera on my shoulder that reconstructs my movements over the entire course of the day. The fact that there is an obvious difference between the ubiquitous surveillance of the camera-on-the-back and the fallible memory of my nosy neighbor is not one that American courts have easily recognized.

We think of privacy in terms of private property. We put great stock in the privacy of the home, but the more elusive values threatened by invasions of privacy—in particular dignity and autonomy—are not ones that constitutional law is well equipped to describe. As Justice Brandeis mentioned in his famous article, American law has not traditionally taken stock of offenses against honor.[44]

Let us think more specifically about the forms that a challenge to dataveillance might take. An individual who suffers from the Nixon effect and complains that he has been pretextually prosecuted for a low-level offense, perhaps a youthful marijuana arrest, even though it was really because he was a critic of the government, will have no remedy. In America, pretextual searches are essentially unregulated, just as racial profiling is essentially unregulated. We know this from

---

42. Gallup Poll (Oct. 11–14, 2001).

43. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 742–46 (1979) (relying on telephone service to make a phone call surrenders the right to privacy in the phone numbers dialed); United States v. Miller, 425 U.S. 435, 442–44 (1976) (there is no legitimate expectation of privacy in financial information provided to a bank).

44. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 197–98 (1890).

two cases: *Whren v. United States*[45] and *Atwater v. City of Lago Vista*.[46] *Whren* established that pre-textual traffic stops are constitutionally permissible. In *Whren*, the Court held that cops can legitimately stop you for driving with a broken tail-light, and when they do so they may make a drug arrest, even if the real purpose of stopping you is for the drug arrest.[47] In *Atwater*, the Court held that it is perfectly reasonable to arrest a mother for driving without a seatbelt.[48] Atwater complained that the arrest was disproportionate to the trivial offense of driving without a seatbelt.[49] Justice Souter, writing for the majority, said that historically there was no requirement in proportionality between the invasiveness of the search and the seriousness of the crime.[50]

Justice Souter's historical view is open to question. Arguably, at the time of the framing, proportionality was indeed a constitutional value. For example, magistrates could only make warrantless arrests for felonies, which were capital offences and created a great danger of flight, or for misdemeanors committed in the officer's presence. However, the historical evidence is contested, and our courts have more or less abandoned the requirement of proportionality.

Consider the harm caused by the stigma that arises when I am unable to escape my past. When I arrive at the airport, or when I go into a bookstore, and I find my youthful wrongdoing tags me at every turn. I might be stigmatized. However, just last term in a challenge to the Megan's law sex-offender registration system, the Court said that stigma is not a constitutional injury.[51] The publication of truthful but embarrassing information, said the Court, does not amount to any cognizable constitutional injury, unless some long-protected right, such as the right not to be unreasonably fired from a particular job, is implicated.[52]

Justice Ginsburg had a wonderful dissent in *Smith v. Doe*, the Supreme Court case dealing with Megan's law. To Justice Ginsburg, the registry was punitive, and therefore an unconstitutional ex post facto law.[53] Only the bad information is published about the sex-offenders, not the good information. A court had found that the registered offender was a fit father and that he had overcome his past wrongs.[54] To Ginsburg, the law appeared to be designed to further punish the released offender, rather than to enhance the public welfare.[55] Ginsburg understood the dangers of being judged out of context. A single transgression may come wrongly to define us in the public's mind. The majority rejected this argument,[56] and therefore I would not expect the Court to recognize

---

45. 517 U.S. 806 (1996).
46. 532 U.S. 318 (2001).
47. *Whren*, 517 U.S. at 814–17.
48. *Atwater*, 532 U.S. at 346–54.
49. *Id.*
50. *Id.* at 327–38 (Souter's historical analysis).
51. Smith v. Doe, 538 U.S. 84 (2003).
52. *Id.* at 98 (holding that dissemination of truthful information does not equal punishment).
53. *Id.* at 115–17 (Ginsburg, J., dissenting).
54. *Id.* at 117 (Ginsburg, J., dissenting).
55. *Id.* at 117–18 (Ginsburg, J., dissenting).
56. *Id.* at 105–06.

the stigma that results from retaliatory, pretextual searches as constitutional injury either.

When you think about the indignities of this particular form of dataveillance, there is a threat not only to privacy but also to equality. Think about the real harms of these digital dossiers that try to predict our future behavior based on our past behavior, and separate us into different categories, like at the airport—red or yellow or green—based on the expectation that we will continue to behave consistently with our past behavior. This is not a privacy violation; it is a form of classification and exclusion, which these technologies are designed exactly to do. They were developed in the private sector to decide which of Amazon's or Oracle's customers were more likely to be trustworthy, more likely to spend money, or more deserving of better treatment. Now they are applied to the national securities sphere. Is it the business of the American Government to decide which of its citizens is trustworthy, or is it the business of the Government to win the trust of the citizens?

Injury to equality is a real danger, but I would not expect it to be constitutionally cognizable. To be unconstitutional, an offense against equality must be intentional.[57] Racial profiling is essentially unregulated, because courts have held there is no constitutional harm when law enforcement officials classify people based on public behavioral traits to predict dangerousness so long as they do not solely rely on immutable characteristics such as race or gender.[58]

So that is why constitutional doctrine, in its current incarnation, seems unlikely to save us from the harms of dataveillance. Could I imagine a different form of doctrine? Yes, I could imagine it. What would it look like? Here, Canada might provide a model. In Canada, former Supreme Court Justice La Forest developed a creative test for regulating surveillance cameras.[59] He does not ask whether the technology violates subjective expectations of privacy, which are lowered in response to new technology. Rather, he asks whether the technology is consistent with the goals of free and open society.[60] His colleague, the former privacy commissioner, George Radwanski, proposed an even more stringent four-part test that is similar to the strict scrutiny test applied by United States courts when a fundamental right is implicated. He would have the courts determine whether the invasiveness of the search is proportionate to the seriousness of the crime, the technology is empirically effective at stopping rather serious crimes, the technology is necessary or closely connected to the stoppage of serious crimes like terrorism or murder, and it is the least restrictive means of achieving the goal without unduly violating privacy.[61] However, I would not expect or even urge

---

57. *See* Washington v. Davis, 426 U.S. 229, 240–42 (1976).

58. *See, e.g.*, Whren v. United States, 517 U.S. 806, 813 (1996) ("[T]he Constitution prohibits selective enforcement of the law based on considerations such as race."); United States v. Brignoni-Ponce, 422 U.S. 873, 885–87 (1975) (holding that apparent Mexican ancestry did not raise reasonable grounds to believe vehicle occupants were illegal immigrants).

59. R. v. Wong, 3 S.C.R. 36 (1990).

60. *Id.* at 50.

61. *Id.*

United States judges to engage in this particular form of judicial activism. Privacy, unlike equality, is a goal that produces broad differences in opinions. People feel very differently about being naked at the airport. We all disagree strongly about the proper balance between privacy and security, and also about what values really are implicated. Is it dignity, time, or equality being judged out of context? There is passionate disagreement. Empirically and normatively, judges tend to thwart national majorities only when there is broad consensus about the kind of values that are being enforced, and when it comes to privacy, no such consensus exists.

If we are looking for governmental saviors, that leaves Congress or the Executive. If forced to choose, I would put my faith in Congress. Representative Butch Otter is joined by other heroes of privacy, people like Dick Armey and Bob Barr. These Representatives were not previously thought of as touchy-feely liberals as they represented the scourge of President Clinton during the Monica Lewinsky scandal. Joined by their civil libertarian allies, they took the same pro-privacy position when the Clinton administration proposed broad surveillance authorities after the Oklahoma City bombings in response to similar public fears. They have a principle, they have an instinctive distrust in government, and they have proved quite effective in saying no to the worst designed forms of Executive excesses.

The great victories for privacy since September 11 include saying no to total information awareness, saying no to the national identification card, imposing sunset provisions, proposing the Otter amendment, and the SAFE act. These are all Congressional rather than judicial initiatives. The libertarian tradition, when joined with our constitutional system of separation of powers and checks and balances, can impose meaningful limitations on the most repressive Executive excesses. Whether this Congressional coalition is equally effective at striking balanced compromises remains to be seen. The same suspicion of government that leads the libertarians to say no to every proposal for surveillance leads the Executive to say no to every proposal for balanced compromise, and may lead to a stalemate that would make it difficult to achieve balanced and complicated regulatory models such as the controlled-use model and the particularized suspicion model. I applaud Congress, but offer only qualified optimism because it is still unclear whether the ultimate goal of achieving these regulatory mechanisms can be achieved.

I close then by thinking about the Executive. Perhaps unsurprisingly, the Executive has been responsive to the public's demand for security above all. We should not be too surprised that our most democratic institution has proved unwilling to engage in the thoughtful compromises of the kind that our German and European allies have found helpful. I do not ascribe ill motives to the Executive, but there may be dangerous consequences when public fears are pattered to rather than urged to be transcended. It is hard to imagine Franklin Roosevelt issuing a system of color-coded threat indexes. Roosevelt urged the public to overcome its fears, not to dwell on them. I am convinced that our saviors will have to come ultimately not only from ourselves, but also from the sort of leadership that Roosevelt and others since September 11 have demonstrated. Rudolf Giuliani's calm stoicism in the face of public fears, not spinning, not pretending to have more knowledge than he actually had, not promising a zero-risk mentality of unrealistic protection against remote threats, but simple calm

confidence is the model for the kind of leadership that I admire. According to the behavioral scientists, leadership is the only way of winning public trust, and public trust is the only way of overcoming public fears.

Great leaders do not arise often in the American democracy. It will be foolish to expect another Roosevelt or Lincoln to appear at any moment. Lincoln, surely our greatest President and also our greatest constitutionalist, is a reminder of the inseparable complication of constitutional values and public leadership. Lincoln, faced with the greatest crisis in our history, did not unilaterally suspend habeas corpus in all circumstances. He initially suspended it only in the immediate area of insurrection, and later when it was extended outside the area of insurrection, he sought Congressional approval after-the-fact.[62] He understood the importance of bilateralism, and he was motivated by constitutional arguments. In Lincoln's hands, the arguments shaped the actions, not the other way around.

This is the President who produced the Spot-Resolutions, demanding that the administration show the precise spot on American soil where the Mexicans invaded during the Mexican-American War.[63] His actions were scrupulously guided and constrained by the transcendent and binding power of the Constitution itself. Lincoln reminds us of the importance of leadership, the importance of constitutional precision, and the idea that in the end we can only transcend our fears if we find the resources to do so in ourselves.

---

62. WILLIAM H. REHNQUIST, ALL THE LAWS BUT ONE: CIVIL LIBERTIES IN WARTIME 25, 60 (Vintage Books 2000).

63. Abraham Lincoln, "Spot Resolutions," National Archives and Records Administration, Records of the U.S. House of Representatives, RG-233, HR 30 A-B 3, *available at* http://www.archives.gov/digital_classroom/lessons/lincoln_spot_resolutions/images/resolution_page_1.gif, http://www.archives.gov/digital_classroom/lessons/lincoln_spot_resolutions/images/resolution_page_2.gif.