

GETTING REAL ABOUT PRIVACY: ECCENTRIC EXPECTATIONS IN THE POST-9/11 WORLD

*Jeff Breinholt**

BOOKS REVIEWED

The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age. By Jeffrey Rosen. *New York: Random House, 2004.* Pp. 272. \$24.95.

The Unwanted Gaze: The Destruction of Privacy in America. By Jeffrey Rosen. *New York: Random House, 2000.* Pp. 288. \$24.95.

Enemy Aliens: Double Standards and Constitutional Freedoms in the War on Terrorism. By David Cole. *New York: The New Press, 2003.* Pp. 256. \$24.95.

I. INTRODUCTION

Imagine an America completely free of violent crime. What if, through the combination of modern technology and political will, we could be entirely safe from physical assaults on our streets? What if this goal could be achieved without jeopardizing civil liberties or personal privacy? Impossible?

Consider the following hypothetical scenario. In the future, science establishes that persons have particular, distinctive gaits they display every time they go out in public. Suppose that scientists design a way to assign a unique identifier that corresponds to this gait. This identifier would be a set of alphanumeric digits, unique to each individual, that corresponds to how that person moves while walking. It would not be based on any private information; the act of putting one foot in front of the other to propel your body along a public street has never been

* Deputy Chief, Counterterrorism Section, Criminal Division, United States Department of Justice. J.D., University of California Los Angeles, 1988; B.A., Yale University, 1985. The views expressed in this article are the author's own and do not reflect those of his employer. The author can be reached at jeffrey.breinholt@usdoj.gov.

considered a private act or something reasonable people consciously try to conceal.

Assume that this identifier can be assigned on the basis of a video capturing a person walking ten paces and that it is robust enough to discern intentional attempts to disguise one's walking style. The gait identifier is assigned whenever one applies for a driver's license or enters the United States through an immigration checkpoint. It is done on the basis of a ten-second video capture that is taken at the same time as one's first receipt of a driver's license or first entry to the United States. A national "gait identity registry" is kept in a single secure government database, unavailable to the public. Because they do not comprise an urban violent crime threat, persons incapable of walking are exempted from the registry.

Meanwhile, satellite reconnaissance technology develops to the point where digital video can be taken of an entire urban area in the United States. This technology is efficient enough to operate effectively irrespective of weather and sufficiently precise to capture enough of a moving image to allow modern computers to compare it to the government-maintained gait index registry. Digital video can be taken continuously, twenty-four hours a day, and stored for a period of several months before being discarded.

Assume further that a legal regime is established through which law enforcement officials can petition a U.S. district court to order another part of the government to process and release a video clip of certain duration directed at particular geographic coordinates. Armed with the footage, law enforcement personnel can push a button and compare it to the nationwide gait index registry and establish who was present at a certain time and certain place, for example, in any of the five boroughs of New York City.

One night, a schoolteacher in the Bronx is killed in an apparent robbery as she walks away from an ATM machine. Pursuant to the established legal regime, local homicide detectives secure judicial approval to obtain four minutes of satellite footage of where the body is found at the approximate time of death. The police now have a digital recording of the murder, although it is not of sufficient quality for them to analyze it themselves.

Law enforcement personnel then run that footage against the gait index registry. This process quickly results in a hit. The computer finds a match and generates the name of a local thug whose unique style of movement matches the video of the assailant. Police subsequently locate and arrest the individual so identified. At his trial, the prosecutor calls a witness to authenticate the video footage and the particular method that resulted in the match on the gait index registry. The prosecutor then puts on an expert who describes this process and renders an opinion that the person who killed the schoolteacher has a gait that matches that of

the defendant to a mathematical certainty. The jury convicts the defendant of murder.

What happens now? The technology that facilitated this conviction is not a sensitive intelligence method. After all, it was deliberately disclosed and described to the public in the murder trial. In fact, by this time, the technology already is well known to the American people, whose elected officials enacted the legal regime that made it possible. This legislative process was the subject of extensive media coverage and public dialogue, as well as open discussion between civil libertarians and pro-security partisans. Both the U.S. Congress and the President, who signed the bill into law, carefully considered the regime they were creating.

Such public debate had additional benefits. The application of this new technology to the problem of violent street crime puts would-be violent criminals on notice that their conduct, when committed outdoors, is being captured on video perpetually and is capable of being reviewed should they commit violent crimes somewhere on the city streets. The footage, captured twenty-four hours a day, is only processed upon a court order supported by probable cause and is accessible by law enforcement personnel who demonstrate to a neutral judicial officer that a violent crime has been committed at a particular time and place.

Word spreads. The bad guys are deterred: as rational actors, would-be criminals soon figure the risk of being caught into their calculation of whether to engage in street crime. Their decisions are affected by their interminable fear that what they do, in the great outdoors, is in a setting as easily witnessed by innocent bystanders as by the government's eye in the sky. Violent crime committed outside becomes a thing of the past. Empirically, people are now safer outdoors than within their homes. The economy booms. The United States has become the sole democracy to eliminate violent crime.

What about the cost? The United States does not even need to establish satellite coverage of every American city. It merely needs to rotate the satellites in an unannounced way to keep violent criminals guessing and uncomfortable. Are Americans outraged by this? If so, they must weigh their disapproval against the obvious benefits: the certainty with which they can walk with their families—in any city, at any time, irrespective of their gender or socio-economic status—and be completely secure in their persons and property, something never thought possible. Urban violent crime is eliminated. Police presence is decreased. Many of the cops on the street are transferred to desk jobs, where they become experts in this new technology. It has taken a concerted, zero-tolerance enforcement initiative to convince the bad guys that crime is not worth the risk. Over time, an entire generation of Americans grows up without any personal sense of danger from strangers on the street, other than what they see in movies and television reruns set in the past.

What about the potential for abuse? The government puts its full weight behind the security of these tools, aggressively punishing those who try to hack into the system, as well as law enforcement personnel who do not follow the rules and leak information collected under this initiative. There is no private access to either the satellite product or the gait index registry. While the technology and its capabilities are well known, neither private persons nor rogue law enforcement personnel can access its product for their own personal agendas. Violations may occasionally occur, but the culprits are treated harshly enough for this not to become a common occurrence.

Is this scenario technologically feasible? For purposes of this essay, I am not concerned with that question because the foregoing is merely a tool through which to consider the controversy over the trade-offs between freedom and security in twenty-first century America. Since the events of September 11, 2001 (“September 11” or “9/11”), polemic arguments and academic studies have filled bookstores, offering prescriptions on how to assure the safety of Americans while maintaining our way of life. Many of these books argue that we are on the wrong path, destined to regret the hysterical reaction now on display towards Islamic fundamentalism. Such works seem to take on faith the notion that we are going too far in the application of technology to day-to-day police problems. Many such works buckle under the weight of their own arguments and do not adequately address the type of legal regime that I describe above.

II. JEFFREY ROSEN’S *THE NAKED CROWD* AND *THE UNWANTED GAZE*

One of the more recent books addressing privacy issues post-9/11 is *The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age* (2004), by George Washington University law professor Jeffrey Rosen.¹ Professor Rosen is very uncomfortable with the post-9/11 threat that modern technology poses to personal privacy and individual freedom.² Unlike other commentators, however, Rosen’s fear is not necessarily of a government run amok, although there is some of that. Crediting the possibility that Congress and the judiciary may be able to control crime-fighting technology effectively to prevent infringements on liberty, Rosen concerns himself mainly with the public itself, which—unlike him—appears incapable of seeing the dangers of feeling safe without actually being safe.³ As such, Rosen insists on a technological architecture that is both effective and privacy protecting.⁴ Because of the public’s ambivalence, Rosen argues, we are doomed to not recognize

1. See generally JEFFREY ROSEN, *THE NAKED CROWD: RECLAIMING SECURITY AND FREEDOM IN AN ANXIOUS AGE* (2004) [hereinafter ROSEN, *NAKED CROWD*].

2. See *id.* at 7–9.

3. *Id.* at 6.

4. *Id.*

necessary controls and to accept draconian government surveillance while losing our most cherished freedoms.⁵

Rosen's view of the average citizen in a democratic society drives his argument, and his title derives from a certain security technology that he describes in the prologue. After September 11, security officials tested a machine that Rosen calls the Naked Machine.⁶ By bouncing microwaves off the human body, the machine produces a three-dimensional, naked image of the subject.⁷ The machine discloses not only guns and weapons concealed in the subject's clothing, but also the subject's unique anatomical characteristics.⁸

The utility of the Naked Machine to counterterrorism is obvious. It seems that the Naked Machine could be refined further to produce images that extract the concealed objects and project them onto a sexless mannequin, an invention Rosen calls the Blob Machine.⁹ Intuitively, it would seem that Americans care deeply about personal privacy and human dignity and, given the choice, obviously would prefer the Blob Machine to the Naked Machine. To Rosen's chagrin, though, studies show that this is not always the case. Rather, many people actually seem to prefer the Naked Machine.¹⁰ Rosen explains:

When asked why, the people who choose the Naked Machine over the Blob Machine give a range of responses. Some say they are already searched so thoroughly at airports that they have abandoned all hope of privacy and don't mind the additional intrusion of being seen naked. Others say they're not embarrassed to be naked in front of strangers, adding that those who have nothing to hide should have nothing to fear. (A few are unapologetic exhibitionists.) Still others are concerned that the Blob Machine would be less accurate in identifying weapons than the Naked Machine, and they would prefer not to take chances. And in each group there are some people who say they are so afraid of terrorism on airplanes that they would do anything possible to make themselves feel better, even if they understand, on some level, that their reaction is based on emotions rather than evidence. They describe a willingness to be electronically stripped by the Naked Machine as a ritualistic demonstration of their own purity and trustworthiness in much the same way that the religiously devout describe rituals of faith. They don't care, in other words, whether or not the Naked Machine makes them safer than the Blob Machine because they are more concerned about feeling safe than being safe.¹¹

5. *See id.* at 3–31.

6. *Id.* at 3–7.

7. *Id.* at 3.

8. *Id.* at 3.

9. *Id.* at 4.

10. *Id.* at 4–5.

11. *Id.* at 5.

Rosen bemoans this fact. Anxiety over personal safety means that people are willing to show themselves naked, to join the Naked Crowd, rather than hold to their principles and insist on technological restrictions to assure their continued privacy.¹² Rosen's book is devoted to trying to convince us of the dangers.¹³ He detests citizens' willingness to embarrass themselves over the Internet,¹⁴ and he attributes this to increased anxiety over identity, which he claims drives people to be more concerned with maintaining their feeling of connectedness than with the "social costs of exposure."¹⁵

What would Rosen say about the gait index registry scenario that I posit above? Based on *The Naked Crowd*, Rosen likely would object, overstating the dangers while minimizing the significance of a crime-free society. While Rosen acknowledges the possibility of designing technology and laws that protect both liberty and security, he argues that this process needs to be value-driven, lest we accept a juggernaut of technologies that are both ineffective and threaten our privacy.¹⁶ To illustrate his point, Rosen describes the United Kingdom's fixation with surveillance cameras, a technology that he claims, relying on empirical studies, has failed to make British society any safer.¹⁷ It is here that Rosen gives himself away. Discussing the U.K. experience with video cameras as crime-fighting tools, Rosen notes that the cameras are designed not to produce arrests but to make people feel that they are constantly being watched.¹⁸ The cameras are "intended to scare local hoodlums into thinking they might be setting off alarms even when the cameras are turned off."¹⁹ This, to Rosen, is a terrible thing.²⁰ He argues that the cameras are in tension with the values of society because they "promot[e] social conformity"²¹ and that it would be a mistake for the United States to follow the lead of our English colleagues.²² Rosen fails, however, to answer the obvious question: What is wrong with promoting conformity through laws designed to prevent people from physically abusing others?

12. *Id.* at 4.

13. *See generally id.*

14. *Id.* at 166 ("Many citizens, of course, don't care if they embarrass themselves before strangers on the Internet . . .").

15. *Id.* at 169-70 ("The ease with which we reveal ourselves to strangers suggests that in the face of widespread anxiety about identity, people are more concerned with the feeling of connection than with the personal and social costs of exposure.").

16. *See id.* at 6-7.

17. *See id.* at 35-38.

18. *Id.* at 37-38.

19. *Id.* at 42.

20. *See id.* at 51.

21. *Id.* "In addition to threatening privacy and promoting social conformity, the cameras are in tension with the values of equality." *Id.*

22. *See id.* at 59-60. "But if the American system follows the path of the English system, it would be foolish to expect the courts to save us." *Id.*

The reason for this failure may be Rosen's cavalier attitude towards crime and a dismissive attitude towards those who feel Americans have a right to be secure in their persons and property or who believe that a society like ours need not tolerate lawlessness that can be eliminated or minimized without infringing on reasonable expectations of privacy. Rosen is afraid of the government's use of technology becoming too efficient, of America becoming too safe.²³ He openly worries that modern technology raises the prospect that persons will be misidentified as serious criminals when punished for "trivial crimes that are far easier to detect" while ignoring that even small crimes are criminal offenses.²⁴ Rosen hypothesizes that "citizens will experience the sense of indignation at living in a zero-tolerance society" in which they are prosecuted for minor infractions of the law.²⁵ If crime is the price we pay for living in a free society, Rosen seems to say, the elimination of crime cannot occur without the elimination of privacy. It is as if security and privacy are on opposite sides of an algebraic equation. If crime could be eliminated through technology, the people who would feel the real indignation are those who do not realize already that all crime-fighting involves invasions of reasonable expectations of privacy. If a silver-bullet crime-fighting technology does not offend most people, Rosen believes that it should. Why? Because, like many commentators, Rosen embraces eccentric notions of privacy.

Rosen's previous writing demonstrates such sympathies. Written after September 11, *The Naked Crowd* acknowledges (and complains about) the need to consider technological advances to increase security.²⁶ Rosen's views have not changed much from his previous book on the subject, *The Unwanted Gaze: The Destruction of Privacy in America* (2000), released prior to September 11.²⁷ The chosen title of this earlier book is a tip-off about Rosen's tolerance for eccentricity.

The concept of the unwanted gaze comes from what Rosen describes as a "remarkable" development in Jewish law, known as the *hezzek re'iyah*.²⁸ This doctrine would expand the right of privacy to protect people not only from physical intrusions into their homes but also from surveillance "by a neighbor who is outside the home, peering through a window in a common courtyard."²⁹ He writes:

Jewish law protects neighbors not only from unwanted observation, but also from the *possibility* of being observed. Thus, if your neighbor constructs a window that overlooks your home or

23. See generally *id.* at 60–61.

24. *Id.* at 22.

25. *Id.* at 24.

26. *Id.* at 100–01.

27. See generally JEFFREY ROSEN, *THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA* (2000) [hereinafter ROSEN, UNWANTED GAZE].

28. *Id.* at 18.

29. *Id.* at 18–19.

courtyard, you are entitled to an injunction that not only prohibits your neighbor from observing you but also orders the window to be removed. From its earliest days, Jewish law recognized that it is the uncertainty about whether or not we are being observed that forces us to lead more constricted lives and inhibits us from speaking and acting freely in private spaces.³⁰

Rosen will need to excuse those who differ with him on whether the concept of an “unwanted gaze” should guide post-9/11 U.S. domestic security policy.³¹ Many ancient cultures felt threatened by the intrusion of such modern inventions as photography, believing that the act of taking their pictures constituted a theft of their souls,³² yet few argue that such beliefs are something modern society should institutionalize. The very concept of the unwanted gaze seems to credit the notion that people can subjectively determine how much privacy they can enjoy as they go about their lives, no matter how strange or incompatible with a modern society. Does Rosen recognize such incongruity? He apparently did not before September 11, for *The Unwanted Gaze* shows a high degree of tolerance for world views driven by anachronistic beliefs:

In traditional Muslim societies, any social recognition between the sexes can be interpreted as a prelude to sexual intercourse. Islamic canon law requires women to cover all but their hands and face. Muslim women are expected to look demurely at the ground at the approach of a man, while men are enjoined from gazing directly at women, especially unveiled women. These different examples suggest that although social norms of accessibility vary widely according to culture and context, people have a general expectation that they won't be molested by social overtures to which they haven't explicitly or implicitly given consent.³³

In *The Unwanted Gaze*, as later in *The Naked Crowd*, Rosen expresses chagrin that more Americans do not care about privacy.³⁴ He uses the example of Jennifer Ringley, a twenty-something exhibitionist in Washington, D.C., who has a Web camera trained on her bedroom twenty-four hours a day.³⁵ Rosen seems to be asking, “Have we no sense of decency?” If Ms. Ringley does not feel embarrassed, maybe she

30. *Id.* at 19.

31. *Id.*

32. *Id.* at 218.

33. *Id.* at 16–17 (citation omitted). The temptation to cite archaic legal artifacts in complaints about the U.S. government's post-9/11 counterterrorism efforts must be great, since it proved too much even for the likes of such legal luminaries as the late Samuel Dash. In what turned out to be his final book, Professor Dash cites a Babylonian law from the eighteenth century B.C.: “If a man makes a breach into a house, one shall kill him in front of the breach, and bury him in it.” SAMUEL DASH, *THE INTRUDERS: UNREASONABLE SEARCHES AND SEIZURES FROM KING JOHN TO JOHN ASHCROFT* 9 (2004). Most would agree that, however quaint, this legal doctrine is somewhat extreme and of tenuous applicability in the post-9/11 world.

34. See ROSEN, *UNWANTED GAZE*, *supra* note 27, at 197; see also ROSEN, *NAKED CROWD*, *supra* note 1, at 3–31.

35. ROSEN, *UNWANTED GAZE*, *supra* note 27, at 50.

should. Civil libertarians, however, should be among her strongest supporters in arguing that this choice is hers. By contrast, Rosen seems to be arguing that there should be a uniform standard for personal privacy. The problem, of course, is in determining who decides on such a standard; perhaps those who take offense at the concept that people are free to look at them, and that the unwanted gaze should be legally actionable, should decide.

To his credit, Rosen does not argue directly that U.S. courts currently accept eccentric notions of privacy. As a good lawyer, Rosen believes that the law is against him, that neither the Constitution nor various federal statutes designed to protect against the dissemination of private information recognize an inalienable right to be free from all subjectively unwanted attention.³⁶ At some point, the legitimate interest of the state predominates, and courts label eccentric notions for what they are.³⁷

A recent Supreme Court case, an appeal from a Nevada state court conviction of a person who refused to identify himself to a local sheriff,³⁸ illustrates this point. Reporting to the scene of a roadside commotion, the sheriff explained to a drunken man standing beside a truck that he was investigating a report of a fight and asked for identification.³⁹ The man refused, became agitated, insisted that he had done nothing wrong, and began to taunt the officer by placing his hands behind his back and telling the officer to arrest him and take him to jail.⁴⁰ This routine kept up for several minutes, and the officer asked for identification eleven times but was refused each time.⁴¹ After several warnings, the sheriff placed the man under arrest.⁴² The arrested man turned out to be Larry Dudley Hiibel, who, for refusing to provide his name, was charged with and convicted of obstructing a public officer in the attempted discharge of a legal duty of his office.⁴³ A majority of the Supreme Court upheld Hiibel's conviction,⁴⁴ suggesting that there is no inalienable constitutional right to refuse to provide your name to law enforcement personnel, no matter how unwanted their attention may be.⁴⁵

In American jurisprudence, a person's expectation of privacy need not be obviously eccentric to be rejected by American courts as unreasonable. Consider the case of *Wabun-Inini v. Sessions*.⁴⁶ In March 1989, Wabun-Inini left two rolls of color film for processing at an F-Stop

36. *See id.* at 43–52.

37. *Id.*

38. *See Hiibel v. Sixth Jud. District Court*, 542 U.S. 177, 182 (2004).

39. *Id.* at 180–81.

40. *Id.* at 181.

41. *Id.*

42. *Id.*

43. *Id.*

44. *Id.* at 190–91.

45. *See id.* at 186–87.

46. 900 F.2d 1234 (8th Cir. 1990).

One Hour Photo Store in Minneapolis.⁴⁷ An FBI agent later entered the store, displayed his credentials, and asked a store clerk whether he could purchase a set of prints from the film Wabun-Inini had left to be developed.⁴⁸ The employee obliged.⁴⁹ Upon Wabun-Inini's return to the F-Stop, store employees informed him that they had provided the FBI with prints of his film.⁵⁰ Two months later, Wabun-Inini filed a complaint seeking a declaration that the government's seizure of the prints was unlawful and requesting injunctive relief.⁵¹ The district court granted partial summary judgment in favor of the government, and Wabun-Inini appealed.⁵²

Citing the seminal Supreme Court case of *Katz v. United States*,⁵³ the Eighth Circuit noted that there is a two-part test for determining whether a governmental search or seizure is unconstitutional: whether (1) the person exhibited an actual (subjective) expectation of privacy, and (2) society is prepared to recognize such expectation as reasonable.⁵⁴ Finding that Wabun-Inini had established a subjective expectation of privacy in his film, the Eighth Circuit turned to the second prong.⁵⁵ The court described a principle that has remained steadfast: "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."⁵⁶ To the court, Wabun-Inini's subjective expectation of privacy was not one that society was prepared to recognize as "reasonable" in light of the record revealing that his photographs were exposed to public view during the development process.⁵⁷ The court noted that trash, which is enclosed in opaque plastic bags and left on the curb in front of one's home for collection, can be searched without a warrant.⁵⁸ While the residents of the house may minimize the likelihood that the bags' contents would be inspected by anyone, this belief is objectively unreasonable because the residents had sufficiently exposed their garbage to the public to defeat their Fourth Amendment protection claim.⁵⁹ By analogy, Wabun-Inini's use of the F-Stop for photo processing exposed his photographs to the public sufficiently to defeat his claim to Fourth Amendment protection:

We simply hold that Wabun-Inini's decision to leave his film with the photo processor in this instance, which used processing techniques involving exposure of the photographs to public view for

47. *Id.* at 1236.

48. *Id.*

49. *Id.*

50. *Id.* at 1237.

51. *Id.*

52. *Id.* at 1237-38.

53. 389 U.S. 347 (1967).

54. *Wabun-Inini*, 900 F.2d at 1239 (citing *Katz*, 389 U.S. at 361 (Harlan, J., concurring)).

55. *Id.* at 1240.

56. *Id.* at 1241 (citing *Katz*, 389 U.S. at 351).

57. *Id.*

58. *Id.* (citing *California v. Greenwood*, 486 U.S. 35, 39 (1988)).

59. *Id.* (citing *California v. Greenwood*, 486 U.S. 35, 40 (1988)).

a limited time, make his expectation of privacy objectively unreasonable. Accordingly, we hold that the FBI action here did not violate Wabun-Inini's rights under the Fourth Amendment.⁶⁰

In American law, ratification of people's eccentric desires ultimately fails because a refusal to be examined when one goes out in public is not legally cognizable.⁶¹ To be sure, courts recognize the constitutional right to privacy, but this is defined by objectively *reasonable* beliefs.⁶² In America, one cannot refuse to have one's picture taken, at least if one wants such modern conveniences as the right to operate a motor vehicle. That view of personal privacy would not be objectively reasonable. In *The Unwanted Gaze*, Rosen is very direct about his disagreement with these types of results and with the *Katz* doctrine.⁶³ He argues that while Justice Harlan's test was applauded as a victory for privacy, "it soon became clear that it was entirely circular."⁶⁴ Rosen further explains: "People's subjective expectations of privacy tend to reflect the amount of privacy they subjectively experience; and as advances in the technology of monitoring and searching have made ever more intrusive surveillance possible, expectations of privacy have naturally diminished, with a corresponding reduction in constitutional protections."⁶⁵ With all due respect, what is the problem? Society moves on. We have gone beyond the belief that photographs of us constitute thefts of our soul. Our expectations have evolved, with the help of technology. Is this bad? It seems that technology also has increased our life expectancy. In thinking about personal security, we should not be bound by Luddite beliefs. Over time, history exposes the eccentricity of such ideas.

Although unknown to Rosen when he wrote *The Unwanted Gaze*, attempts to credit eccentric views of privacy have recently played out in townhalls across America. For example, section 215 of the USA PATRIOT Act,⁶⁶ a truly benign provision, lies at the center of a major

60. *Id.* at 1243. See also *California v. Ciraolo*, 476 U.S. 207, 209, 215 (1986) (holding that a person's expectation that his backyard, fenced by a six-foot outer fence and ten-foot inner fence, was protected from police aerial surveillance, was objectively unreasonable, and it was unreasonable to expect that his marijuana plants were constitutionally protected from being observed with the naked eye from an altitude of one thousand feet.); *Dow Chem. Co. v. United States*, 476 U.S. 227, 239 (1986) (holding that the EPA's aerial observation of an industrial complex using sophisticated surveillance equipment did not violate the Fourth Amendment); *Oliver v. United States*, 466 U.S. 170, 179 (1984) (upholding a warrantless search of land with marijuana crops based on the open fields doctrine); *Marshall v. Barlow's, Inc.*, 436 U.S. 307, 315 (1978) ("What is observable by the public is observable, without a warrant, by the Government inspector as well.").

61. See generally *Katz v. United States*, 389 U.S. 347, 351-52 (1967).

62. *Wabun-Inini*, 900 F.2d at 1239.

63. See ROSEN, UNWANTED GAZE, *supra* note 27, at 60-61 (citing *Katz*, 389 U.S. at 360 (Harlan, J., concurring)).

64. *Id.* at 60.

65. *Id.* at 60-61.

66. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, § 215, 115 Stat. 272 (codified at 50 U.S.C.S. §§ 1861-1862 (2006)). Section 215 concerns access to records under the Foreign Intelligence Surveillance Act (FISA). *Id.* For a discussion of section 215 and related law enforcement capabilities, see *infra* notes 67-73 and accompanying text.

hysteria. Librarians, a class of people that perhaps more than other special interest group has less of an excuse to be misinformed about laws, would have the public believe that the USA PATRIOT Act, which nowhere mentions the word “library” or “librarians,” represents a major threat to library patrons.⁶⁷ It appears, then, that with sufficient predication, the FBI actually can examine library circulation records.⁶⁸

Is this capability a new consequence of the USA PATRIOT Act? Hardly. Law enforcement personnel always have had the ability to inquire, for example, into bookstore retail records, as Rosen knows.⁶⁹ Take the unfortunate example of Monica Lewinsky, whom Rosen portrays as a victim in *The Unwanted Gaze*.⁷⁰ Ms. Lewinsky felt aggrieved by Independent Counsel Ken Starr’s issuance of a subpoena for her bookstore purchases.⁷¹ As Rosen describes,

Lewinsky herself was especially unsettled by Starr’s decision to subpoena a Washington bookstore for receipts of all her book purchases since 1995. In her memoir, Lewinsky pointed to the bookstore subpoenas as one of the most invasive moments in the Starr investigation, along with the moment when prosecutors retrieved from her home computer the love letters that she had drafted, but never sent, to the President. “It was such a violation,” she complained to her biographer, Andrew Morton. “It seemed that everyone in America had rights except for Monica Lewinsky. I felt like I wasn’t a citizen of this country anymore.”⁷²

Using the Monica Lewinsky bookstore situation as an example of an invasion of privacy suffers from two problems. First, the Starr prosecutors were able to obtain a copy of her bookstore purchases years before September 11 or the enactment of the USA PATRIOT Act. Clearly, section 215 does not raise a new threat; law enforcement personnel, armed with a legitimate need for evidence that may reflect reading habits and retail decisions, always have been able to obtain such records.⁷³

Second, the sympathy one might be inclined to feel for Ms. Lewinsky’s expression of outrage should be tempered by the realization that such outrage is being expressed in the context of her *autobiography*, a project designed to expose her life to as many people as possible. If the Starr investigation unfairly brought Ms. Lewinsky into the public eye, she

67. See, e.g., Rene Sanchez, *Librarians Make Some Noise over Patriot Act*, WASH. POST, Apr. 10, 2003, at A20.

68. Cf. ROSEN, UNWANTED GAZE, *supra* note 27, at 167.

69. *Id.* at 4.

70. *Id.*

71. *Id.*

72. *Id.*

73. James B. Perrine, *The USA Patriot Act: Big Brother or Business as Usual?*, 19 NOTRE DAME J.L. ETHICS & PUB. POL’Y 163, 191 (2005); see also Ulrika Ekman Ault, Note, *The FBI’s Library Awareness Program: Is Big Brother Reading over Your Shoulder?*, 65 N.Y.U. L. REV. 1532, 1534 (1990).

certainly did not mind being there in the end. Like Jennifer Ringley, maybe Monica Lewinsky should be embarrassed. That she was not so embarrassed as to preclude writing a memoir contradicts rather than supports Rosen's views of privacy and of a population that does not view privacy as he thinks they should.

Expressions of this frustration fill Rosen's books⁷⁴ and ultimately lead Rosen to offer questionable prescriptions. In *The Unwanted Gaze*, Rosen acknowledges that "[u]nless we pull down the curtains and never leave the house, none of us can avoid being observed, and therefore judged, fairly and unfairly, by others."⁷⁵ In terms of what Americans should do to protect themselves from the unwelcome glare of others, such a conclusion seems excessive.

III. DAVID COLE'S *ENEMY ALIENS*

Across town from Rosen, another academic makes similar arguments. In addition to teaching at Georgetown Law Center, Professor David Cole has represented accused supporters of Palestinian terrorists.⁷⁶ His latest book, *Enemy Aliens: Double Standards and Constitutional Freedoms in the War on Terrorism* (2003), focuses mainly on Cole's often-repeated mantra that there should be no legal distinction between Americans and non-Americans, apparently even as to the conferral of the benefits of American citizenship.⁷⁷ Cole believes that actions taken by the United States against non-citizens in this country are a prelude to what the United States eventually will do to its own nationals.⁷⁸ In Cole's words, "What we are willing to allow our government to do to immigrants today creates a template for how it will treat citizens tomorrow."⁷⁹

74. See, e.g., ROSEN, *UNWANTED GAZE*, *supra* note 27, at 25 ("Americans have been similarly passive in adjusting our lives to the intrusions of technology, by avoiding the use of e-mail for private communications, for example, and paying with cash to evade detection by direct marketers. . . . We have the ability to rebuild the private spaces we have lost. But do we have the will?").

75. *Id.* at 44. Rosen's complaint seems to be with the constitutional jurisprudence of privacy itself:

The Court's hastily improvised solution was to pretend that all sorts of dramatic intrusions on privacy, such as planting bugs in people's clothing, rummaging through their trash, and spying on them with high-powered binoculars, weren't really searches or seizures in the first place. The result was a legal climate that constricted the constitutional protections for privacy at the very moment that techniques of surveillance were growing more invasive.

Id. at 34.

76. See, e.g., R. Jeffrey Smith, *Patriot Act Used in 16-Year-Old Deportation Case*, WASH. POST, Sept. 23, 2003, at A3; David Cole, Op-Ed., *Misdirected Snooping Doesn't Stop Terror*, N.Y. TIMES, June 4, 2002, at A19.

77. See DAVID COLE, *ENEMY ALIENS: DOUBLE STANDARDS AND CONSTITUTIONAL FREEDOMS IN THE WAR ON TERRORISM* 231-33 (2003).

78. *Id.* at 7.

79. *Id.* Cole refers to disparate treatment between American citizens and non-citizens as a "double standard." *Id.* at 107. He also argues that "equality between non-nationals and citizens appears to be the constitutional rule." *Id.* at 211.

Like Rosen, Cole knows that the law is not on his side.⁸⁰ Also like Rosen, Cole is chagrined that Americans are not more outraged about what is being done in the name of national security. He is shocked, for example, by a National Public Radio poll taken a year after September 11 that found that only seven percent of Americans felt that they personally had sacrificed any important rights or liberties in the war on terrorism.⁸¹ Civil libertarians like Cole frequently claim that the events of September 11 did strange things to people. To such commentators, the government's reaction—rounding up several hundred illegal aliens from Middle Eastern countries and rushing the USA PATRIOT Act through Congress—surely represented mass hysteria. Too frequently, however, such commentators fail to turn this inquiry into the effects of the events of September 11 on themselves.

For those familiar with Cole's career, the big surprise in *Enemy Aliens* crops up about a quarter of the way through the book, when Cole seemingly exposes himself to be a law-and-order type. After the shock of September 11, Cole may be in the pro-security camp after all:

The PATRIOT Act made many changes to criminal, immigration, banking, and intelligence law. Some of these changes sensibly updated criminal law to reflect changing technologies. For example, the advent of cell phones justified the PATRIOT Act's authorization of so-called "roving wiretaps," which permit wiretapping of any phones that a target may reasonably use, rather than only specified phone numbers, and nationwide warrants, which permit taps to follow an individual even if he travels outside the jurisdiction of a particular federal district. Other provisions removed barriers to the sharing of information between foreign intelligence officials and law enforcement officials in international terrorism investigations, on the reasonable ground that international terrorism is simultaneously a matter of foreign intelligence *and* criminal law enforcement. We certainly want law enforcement authorities with knowledge of Al Qaeda's activities abroad talking to those with knowledge of Al Qaeda's stateside activities. The PATRIOT Act's extensive money laundering provisions seek to respond to new methods of money laundering, and while the financial community has questioned whether the changes will have any effect on terrorism, these provisions do not raise significant civil liberties objections.⁸²

80. For example, Cole cites (and criticizes) the Supreme Court's decision in *Denmore v. Kim*, 538 U.S. 510 (2003), which upheld a statute mandating preventive detention during deportation proceedings of a foreign national charged with certain criminal offenses. According to Cole, "the majority expressly rested its decision on a double standard, noting that Congress can make rules in the immigration setting that would be unacceptable for citizens. . . . *Denmore* thus asserts but does not justify differential treatment of foreign nationals' due process rights." *Id.* at 224.

81. *Id.* at 18.

82. *Id.* at 57.

When it comes to the use of modern technology to gain an insight into the activities of those who would cause us harm, it seems that David Cole—unlike Jeffrey Rosen—is not a Luddite. Cole appears not to be alarmed by new technology or the prospect that it could be harnessed effectively by a legal regime to protect against unfair invasions of privacy.

That hope, however, is quickly destroyed. A few pages later, Cole is back to his old self, criticizing some of the provisions that he had just heralded as sensible:

[The USA PATRIOT Act] authorizes secret searches and wiretaps in criminal investigations without probable cause to believe that the target is engaged in criminal conduct or that evidence of a crime will be found. . . .

It accomplishes this by amending the Foreign Intelligence Surveillance Act (FISA). FISA authorizes wiretaps and searches, based not on the usual showing of probable criminal conduct or evidence, but on the much easier showing that the target of the intrusion is an “agent of a foreign power,” defined broadly to include any officer or employee of a foreign-based political organization. . . .

. . . .

The extraordinary authority provided by FISA was initially justified on the ground that foreign intelligence gathering is different from criminal law enforcement, and that the intelligence power would not be used for the purpose of investigating crime. . . . [The USA PATRIOT Act’s changes to FISA in effect deny] the Fourth Amendment’s most basic protection to any person who might qualify as a foreign agent—predominantly but not exclusively foreign nationals.⁸³

Cole’s endorsement of the USA PATRIOT Act’s information-sharing rules, premised on the recognition that “international terrorism is simultaneously a matter of foreign intelligence *and* criminal law enforcement,”⁸⁴ appears to have fallen by the wayside, as has his acceptance of the need for intelligence agents and law enforcement officers to share information about Al Qaeda. His earlier favorable assessments, it seems, were premised on the assumption that intelligence-collection methods such as FISA should be taken away from the government. Why is FISA unconstitutional? According to Cole, the legality of FISA surveillance is never subject to adversarial testing in the

83. *Id.* at 57, 66–67.

84. *Id.* at 57.

courts.⁸⁵ This conclusion would surprise courts that have issued judicial opinions on the constitutionality of specific FISA investigations.⁸⁶

Unlike Rosen, Cole does not spend much space arguing that the American public is too dense to see the risks to their own privacy.⁸⁷ Cole is more concerned with government run amok.⁸⁸ Here, though, he seems to agree with Rosen that a certain amount of lawlessness is a good thing, since stamping it out would mean the government is too efficient. Cole notes, for example, that “[w]hile no one condones threats of violence, surely every noncitizen who gets into a bar fight with a weapon does not warrant unilateral executive detention, particularly as our law does not authorize such detention even for the most hardened, recidivist criminal citizens.”⁸⁹ Carried to its logical extreme, Cole’s argument proposes that a government armed with the technological tools that permit it to eliminate violent crime within the confines of constitutional jurisprudence should not deploy such tools because a little crime and violence are somehow an important part of the American experience. If the law permits the development of such technology and the American public reaches a consensus that it wants such technology, it is because the courts and the people do not share Cole’s and Rosen’s views. Both authors’ criticism is directed at the government; the private sector is spared their wrath. Interestingly, neither Cole nor Rosen seems particularly bothered by the kind of surveillance undertaken by commercial enterprises. Rather, their real beef is with the government, and law enforcement in particular.⁹⁰

What is particularly amazing about Cole’s position is that he voices it while acknowledging that some post-9/11 law enforcement powers have made us safer. Cole nonetheless opposes such powers, so ingrained is his anti-government animus:

85. *See id.* at 67.

86. *See* *United States v. Squillacote*, 221 F.3d 542 (4th Cir. 2000); *United States v. Isa*, 923 F.2d 1300 (8th Cir. 1991); *United States v. Ott*, 827 F.2d 473 (9th Cir. 1987); *United States v. Duggan*, 743 F.2d 59 (2d Cir. 1984).

87. ROSEN, *NAKED CROWD*, *supra* note 1, at 17.

88. COLE, *supra* note 77, at 228.

89. *Id.* at 66.

90. *Id.* at 73 (“Virtually everything we do in the modern world leaves a computer trace, including our credit card and banking transactions; our library borrowing records; our e-mail, Internet, and phone traffic; and our travel plans. At present, however, while many distinct entities have select portions of this information for their own legitimate purposes, the government lacks the capacity to collect and search it on a mass scale for law enforcement ends.”); *cf.* ROSEN, *UNWANTED GAZE*, *supra* note 27, at 7 (“On the Internet, every Web site we visit, every store we browse in, every magazine we skim, and the amount of time we spend skimming it, create electronic footprints that increasingly can be traced back to us, revealing detailed patterns about our tastes, preferences, and intimate thoughts.”). Like Cole, Rosen accepts technologies of customer relations management designed to put customers in categories depending on their perceived value to the company. However, Rosen does not like the prospect of similar technology being used by the government, which would result in “different citizens being put in different risk categories based on the threat they are perceived to pose to the state.” ROSEN, *NAKED CROWD*, *supra* note 1, at 27.

Some of the measures that I have criticized may well make us safer. Laws aimed at denying financial support to organizations that engage in terrorism, for example, are likely to hinder those organizations' ability to do evil, even as they also hinder many people's rights to do good. . . . And relaxing the threshold requirements for searches and surveillance may lead to the discovery of evidence that would have otherwise eluded detection.

I do not deny, in other words, that some of the measures adopted since September 11 may well have made us safer. My point is that when the government relies so heavily on double standards to strike the balance between liberty and security, its loss of legitimacy among persons, communities, and nations potentially our partners in the struggle against terrorism has its own substantial security costs.⁹¹

In other words, Cole seems to suggest that it may be better to risk the lives and safety of Americans in their own homeland rather than offend those who are visitors here (and who, incidentally, are barred from voting in a perfectly constitutional form of discrimination based on nationality) and would view the U.S. government as less *legitimate* because of its efforts to protect its own citizens.

IV. BACK TO THE FUTURE?

Perhaps we should come back to reality by briefly considering how Cole and Rosen might view my hypothetical satellite-assisted gait index registry of the future. As noted, the power of this scenario is not in its realism or feasibility, but rather in what it says about our legal and political culture. If such technology were developed, could it be implemented?

One of the beauties of the scenario is that it avoids the complaints about racial profiling. The gait index is race-blind, as is the technology that compares it against satellite surveillance. As such, nobody can claim that certain ethnic groups are being unfairly targeted for persecution. This would seem to solve many of Cole's complaints, even though the technology may well result in a disparate impact on defendants of certain ethnicity and national origin. The disparate impact of accurate technology is not objectionable, however, at least not as a constitutional matter.

What about personal privacy, the focus of Rosen's works? If courts were more inclined to agree with him, people could assert that they have a constitutional right not to have their gait recorded and stored or their movements in public recorded by satellites. These arguments, however, would be unavailing in light of the *Katz* doctrine.⁹² Similar to having

91. COLE, *supra* note 77, at 207–08.

92. See *Katz v. United States*, 389 U.S. 347 (1967).

your driver's license photograph taken, a videotape capture in modern society does not amount to a theft of your soul. Faced with this reality, Rosen likely would be relegated to arguing that the technology could not be perfected. This is, after all, how he addressed a British technology that comes close to being the silver bullet of crime fighting:

In 1996, the City of London adopted a predecessor to the current automated license-plate-recognition system that records the plates of all cars entering and leaving the city. The stored license plate numbers are compared with a database of those of stolen cars, and the system can set off alarms whenever a suspicious car enters the city.⁹³

Exactly what is so wrong with this? Rosen does not say, other than noting that current human face recognition technology is not as reliable. That current deficiency hardly means that such technology and other similar technology should not be pursued.

For Rosen, the future is grim because Americans are no longer alarmed by technology. As he notes in *The Naked Crowd*,

[N]othing in this book offers any reason to expect that the public will demand laws and technologies that protect liberty and security at the same time. . . . Refusing to evaluate whether or not these new laws and technologies in fact increase security, the public may willingly acquiesce in the destruction of privacy without getting anything tangible in return.⁹⁴

Why is this the case? According to Rosen, our civic debate is too polarized. On the one side are what he calls the technopositivists, who greet every proposed expansion of government surveillance power with unthinking enthusiasm.⁹⁵ On the other side are the "principled Luddites," who are fighting the quixotic battle against the proliferation of technologies that ultimately will ruin our humanity.⁹⁶ This polarity minimizes the prospect that a true balance can be struck. If true, it is not hard to discern where Jeffrey Rosen falls on the continuum.

93. ROSEN, *NAKED CROWD*, *supra* note 1, at 39.

94. *Id.* at 193.

95. *Id.* at 18.

96. *Id.*