Getting Real About Privacy: Eccentric Expectations in the Post-9/11 World

by Jeff Breinholt[1]

<u>Books Reviewed</u>:
***The Naked Crowd*, by Jeffrey Rosen (Random House, 2004)**
***The Unwanted Gaze*, by Jeffrey Rosen (Vintage, 2000)**
***Enemy Aliens*, by David Cole (The New Press, 2003)**

Imagine an America completely free of violent crime. What if, through the combination of modern technology and political will, we could be 100 percent safe from physical assaults on our streets ? What is this could goal could be achieved without jeopardizing civil liberty or personal privacy? Impossible?

Consider this scenario:

In the future, science establishes that every person on earth has a particular gait they display every time they show themselves in public. Let's say that scientists design a way to assign a unique identifier that corresponds this gait. This identifier will be a set of alpha-numeric digits, unique to each individual, which correspond how we move while walking. It is not based on any private information; the act of putting one foot in front of the other to propel your body down a public street has never been considered a private act or something reasonable people consciously try to conceal.

Let's assume that this identifier can be assigned on the basis of a video capturing a person walking 10 paces, and that it is robust enough the discern intentional attempts to disguise one's walking style. The "gait identifier" is assigned whenever someone applies for a driver's license or enters the United States through an immigration checkpoint. It is done on the basis of a 10-second video capture that is taken at the same time driver's license or US entry. The national "gait identity registry" is kept in a single secure government database, unavailable to the public. Persons incapable of walking, since they do not comprise an urban violent crime threat, are exempted from the registry.

Meanwhile, satellite reconnaissance technology develops to the point where digital video can be taken of an entire U.S. urban area. 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 be able to compare it to the government-maintained gait index

---

[1] J.D., UCLA 1988; B.A., Yale, 1985. Deputy Chief, Counterterrorism Section United States Department of Justice. 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.

registry. A digital video can be taken continuously, 24 hours a day, and stored for a period of several months before being discarded.

A legal regime in 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 videoclip of certain duration directed at particular geographic coordinates. Armed with the video, law enforcement can push a button and compare it to nationwide gait index registry, and establish who was present at a certain time and certain place in the five boroughs of New York City.

One night, a school teacher 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 obtain judicial approval to obtain the satellite footage for a four-minute period where the body is found, at the approximate time of death. The cops now have a digital recording of the murder, although it is not of sufficient quality for them to analyze it themselves.

Armed with this footage, the cops cause it to be run against the gait index registry. This process quickly gives them a hit. The computer finds a match and generates the name and a local thug whose unique style of movement matches the video of the assailant. They locate and arrest him. 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. She then puts on an expert who describes this process, and renders an opinion that the person who killed the school teacher 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, it is already well-known to the American people, whose elected officials have enacted the legal regime that made it possible. This legislative process was the subject of extensive media coverage and public dialogue, and open discussion between the civil libertarians and the pro-security partisans. It was carefully considered by the U.S. Congress and the President who signed the bill creating the regime.

This public debate had some additional benefits. The application of this technology to the problem of violent street crime puts would-be violent criminals on notice that their conduct, committed outdoors, is perpetually being captured on video and capable of being reviewed if they decide to commit violence crime somewhere on the city streets. The footage, captured 24-hours a day, is only processed upon a court order supported by probable cause, and is accessible by law enforcement 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. Rational actors, they soon work the risk of being caught into their calculation whether to engage in street crime. Their decisions are affected by their interminable fear that what they do, in the great outdoors, in a setting as easily witnessed by innocent bystanders as by the government's eye in the sky. Outside violent crime becomes a thing of the past. Empirically, people are now more safe 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 U.S. 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 the violent criminals guessing and uncomfortable. Are Americans outraged by this? If so, they are going to have to weigh their disapproval against the obvious benefits – the certainty that they can walk with their families, in any city, any time, day or night, 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 it's 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 watch 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 of either the satellite product or the gait index registry. While the fact of the technology and its capabilities is well-known, the product of it can be accessed neither by private persons nor rogue law enforcement for their own personal agendas. Violations may occasionally occur, but the culprits of treated sufficiently tough for it not to be a common occurrence.

Is this scenario technologically feasible? For purposes of this article, I am not concerned with that question, since the foregoing is merely as a tool through which to consider the controversy over the trade-offs between freedom and security in 21st Century America. Since 9/11, bookstores have been filled with polemic arguments and academic studies, 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. They seem to take on faith the notion that we are going way too far in the application of technology to day-to-day police problems. Many of them break down on the weight of their own arguments, and do not adequately address the type of legal regime I describe above.

Jeffrey Rosen and *The Naked Crowd*

One of the more recent books is *The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age (*Random House*,* 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. Unlike other commentators, however, Rosen's fear is not necessarily a government run amok, although there is some of that. Crediting the possibility that Congress and the judiciary may be able to effectively control crime-fighting technology so it does not infringe of liberty, Rosen's concern is mainly with the public itself who -- unlike him -- appears incapable of seeing the dangers and insisting on technological architecture that is both effective and privacy-protecting. Because of this ambivalence, he argues, we are doomed not recognize necessary controls and to accept draconian government surveillance while losing our most cherished freedoms.

Rosen's view of the average citizen in a democratic society drives his argument. The title of the book derives from a certain security technology he describes in the prologue. After 9/11, security officials tested a machine that Rosen calls the Naked Machine. By bouncing microwaves off the human body, the machine produces a three-dimensional naked image of the subject. Not only does it expose guns and weapons concealed in the subjects' clothing, but also their unique anatomical characteristics.

The utility of the Naked Machine to counterterrorism is obvious. It seems that the Naked Machine can be refined further, to produce images that extract the concealed objects and projects them onto a sexless mannequin – an invention Rosen calls the Blob Machine. Americans care deeply about personal privacy and human dignity and, given the choice, obviously prefer the Blob Machine to the Naked Machine, right? To Rosen's chagrin, studies how this is not always the case. It seems that many people actually express of preference for the Naked Machine. He 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 searches so thoroughly at airports that they have abandoned all hope of privacy and don't mind the additional intrusion of being 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.[2]

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 continuing privacy. Rosen's book is devoted to tries to convince us of the dangers. He hates that citizens are so willing to embarrass themselves over the Internet,[3] 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 the "social costs of exposure."[4]

What would Rosen say about the "gait index registry" scenario I posit above? Based on his words in the *Naked Crowd*, he would be likely to find something wrong with it, overstating the dangers while minimizing the significance of a crime-free society. In the book, while he acknowledges 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 the juggernaut of technologies that are both ineffective and threaten our privacy.[5] To illustrate his point, he describes the United Kingdom's fixation with surveillance cameras as a cure for their crime problem, technology he claims, through empirical studies, has failed to make British society any safer.[6] 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 they are constantly being watched.[7] They are "intended to scare local hoodlums into thinking they might be setting off alarms even when the cameras are turned off."[8] This, to Rosen, is a terrible thing. He argues that the cameras are in tension with the value of society, since they "promote social conformity."[9] and that it would be a mistake for the U.S. to follow the lead of our English colleagues.[10] He does not answer the obvious question: what's wrong with promoting conformity with laws designed to prevent people from physically abusing others?

The reason for this may be the author'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 believe that a society like ours need not tolerate lawlessness which 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 an America becoming too safe. He openly worries that modern technology raises the prospect that persons misidentified as serious criminals being punished for "trivial crimes that are far easier to detect," while ignoring the fact that even small crimes are criminal offenses.[11] He hypothesizes that citizens will feel a sense of indignation at living in a zero-tolerance society in which they are prosecuted for minor infractions of the law.[12] 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 cannot be weaned of their notion that all crime-fighting involves invasions of reasonable expectations of privacy. If the "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 his sympathies. Written after 9/11, *The Naked Crowd* and acknowledges (while complaining about) the need to consider technological advances to increase security. Rosen's views have not changed much since the release of his previous book on the subject, *The Unwanted Gaze*: *The Destruction of Privacy in America* (Vintage 2000), released prior to 9/11.[13] 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'iyyah*. 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 outside the home, peering though a window in the common courtyard."[14] 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 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 was the uncertainty about whether or not we are being observed that forces us to lead more constricted lives and inhibits us from speaking or acting freely in public spaces.

Professor 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. As we know, many ancient cultures felt threatened by the intrusion of such modern inventions as photography, believing that the act of taking their picture represented a theft of their souls. Few argue that such believes are something modern society should institutionalized. The very concept of the "unwanted gaze" seems to credit the notion that people can subjectively determine how much privacy that can enjoy as they go about their lives, no matter how strange or incompatible with a modern society. Does Rosen recognize this? He apparently did not before 9/11, for *The Unwanted Gaze* shows a high degree of tolerance for ethnic communities whose world view is driven by anachronistic beliefs:

> In traditional Muslim societies, any social recognition between the sexes can be interpreted as a prelude to sexual intercourse. Islamic cannon law requires women to cover all but their heads 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.[15]

As he does later in *The Naked Crowd*, Rosen in *The Unwanted Gaze* expresses chagrin that more American do not care about privacy.[16] In the latter, he uses as an example Jennifer Ringley, "a twenty-one year old exhibitionist in Washington D.C. who has a Web-cam trained on her bedroom twenty four hours a day."[17] He seems to be asking, Where is our sense of decency?

If Ms. Ringley does not feel embarrassed, maybe she should. Civil libertarians, however, should be among her strongest supporters in arguing that this choice is her's. Rosen seems to be arguing that there should be a uniform standard for personal privacy. The problem: who decides? 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.

Rosen does not directly argue for eccentric notions of privacy are currently accepted by U.S. courts. A good lawyer, he recognizes the law is against him, for in America neither the Constitution nor the various federal statutes designed to protect against the dissemination of private information recognize an inalienable right to be free of all subjectively "unwanted" attention. At some point, the legitimate interest of the state predominates, and courts label eccentric notions for what they are.

This point was illustrated during this most recent Supreme Court term, the appeal from a Nevada state court conviction of someone who refused to identify himself to a local sheriff.[18] Reporting to the scene of a commotion by the side of the road, the sheriff explained to a drunken man standing beside a truck that he was investigating a report of a fight, and asked for identification. The man refused, became agitated, insisted 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. This routine kept up for several minutes: the officer asked for identification eleven times and was refused each time. After several warning, the sheriff placed him under arrest. The arrested man turned out to be Larry Dudley Hiibel, who was charged and convicted of the state crime of obstructing a public officer attempting to discharge any legal duty of his office, by refusing to provide his name. A majority of the Supreme Court upheld Hiibel's conviction. It appears that there is no inalienable constitutional right to refuse to provide your name to law enforcement, no matter how "unwanted" their attention is.

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, also known as Vernon Bellacourt.[19] In March 1989, he left two rolls of color film for processing at an F-Stop One Hour Photo Store in Minneapolis An FBI agent 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. The employee obliged. Upon Wabun-Inini's return to the F-Stop, store employees informed him that they had provided the FBI with prints of his film. 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. The district court dismissed his case, and Wabu-Inini appealed the dismissal.

The Eighth Circuit Court of Appeals, citing the seminal Supreme Court case of *Katz v. United States,*[20] 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) the expectation be one that society is prepared to recognize as "reasonable."

Finding that Wabun-Inini had established a subjective expectation of privacy in his film, the Eighth Circuit turned to the second prong. It described a principle that has remained steadfast over time: what a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. To the court, Wabun-Inini's subjective expectation of privacy was not one that society is prepared to recognize as "reasonable," in light of the record revealing that his photographs were exposed to public view during the development process. It noted that trash, which is enclosed in opaque plastic bags and left on the curb in front of their home for collection, can be searched without a warrant. 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 they had exposed their garbage to the public sufficiently to defeat their claim to Fourth Amendment protection.

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 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.[21]

In American law, the idea that people's weird desires should be subsidized ultimately fails, for one's refusal to be examined when one goes out in public is not legally cognizable. To be sure, courts recognize the constitutional right to privacy, but this is defined by objectively *reasonable* beliefs. 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. While the case applauded as a victory for privacy, ""it soon became clear that it was entirely circular." He argues:

> People's subjective expectation or privacy tend to reflect the amount of privacy they subjectively experience, and as advances in the technology of monitoring and searching have made even more intrusive surveillance possible, expectations of privacy have naturally diminished, with the corresponding reduction in constitutional protection.[22]

So what is the problem? Society moves on. We have gone beyond the belief that photographs of our faces are thefts of our soul. Our expectations have evolved, with the help of technology. Is this bad? It seems that technology has also increased our life expectancy. In thinking about personal security, we should not be bound by Luddite beliefs. Over time, history exposes them for what they are: eccentric cranks.

Although unknown to Professor Rosen when he wrote *The Unwanted Gaze*, attempts to credit eccentric views of privacy is being played out right now in townhalls across America. It involves a truly benign provision of the USA PATRIOT Act that the ACLU has used to launch a major industry-wide hysteria. The particular industry that claims to be aggrieved by Section 215 - the organized librarians (a class of people, perhaps more than other special interest groups, have less of an excuse to be misinformed about laws.) They would have the public believe that the PATRIOT Act, which nowhere mentions the word "library" or "librarians," represent a major threat to library patrons. It appears that the FBI, armed with sufficient predication, can actually examine out library circulation records.

Is this a new consequence of the USA PATRIOT Act? Hardly. Law enforcement always had the right to inquire into the retail records, as Rosen knows. Take the unfortunate example of Monica Lewinsky, who Rosen in *The Unwanted Gaze* portrays as a victim. Ms. Lewinsky felt aggrieved by the Independent Counsel Ken Starr's issuance of a subpoena for her bookstore purchases. As Rosen describes it:

> Lewinsky herself was especially unsettled by Starr's decision to subpoena a Washington bookstore for receipts of all her book purchases as one of the most invasive moments in the Starr investigation, along with the moment the prosecutors retrieved from her home computers the love letter she had drafter, 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."[23]

Using the Monica Lewinsky as a example of invasion of privacy suffers from two problems. First, the Starr prosecutors were able to obtain a copy of her bookstore purchases years well before 9/11 and the USA PATRIOT. Clearly, Section 215 does not raise a new threat; law enforcement, armed with a legitimate need for evidence that may reflect reading habits and retail decisions, has always been able to obtain such records. Second, the sympathy one might be inclined to feel for Ms. Lewinsky 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 around the world. If she was unfairly brought into the public eye by the Starr investigation, she certainly did not mind being there in the end. Like Jennifer Ringley, maybe Monica Lewinsky should be embarrassed. The fact that she was not disputes, rather than supports, Rosen's views of privacy, and of a population that does not view privacy as he thinks they should. Both of Rosen's book are filled with expressions of this frustration.

> 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

patters about our tastes, preferences and intimate thoughts.[24]

As in the *Naked Crowd*, he acknowledges in *The Unwanted Gaze* that "Unless we pull down the curtains and never leave the house, none of us can avoid being observed, and therefore judged, fairly or unfairly, by others."[25] In terms of what Americans should do to protect itself from the "unwelcome" glare of others, is that not a little over the top?

David Cole and *Enemy Aliens*

While Rosen expresses these views, across town another academic is making similar arguments. When not teaching at Georgetown Law Center, Professor David Cole represents accused supporters of Palestinian terrorists. His latest book, *Enemy Aliens: Double Standards and Constitutional Freedoms in the War on Terrorism* (The New Press, 2003) mainly focuses on Cole's often-repeated mantra: that there should be no legal distinction between Americans and non-Americans, apparently even when conferring such things as the benefit of American citizenship. Cole believes that the actions the U.S. takes against non-citizens here are a prelude to what we will eventually to our own nationals should not exist, since what we do to our illegal residents is bound to be turned on us. In his words, "What we are willing to allow our government to do to immigrants today creates a template for how it will treat citizens tomorrow."[26] Like Rosen, Cole knows that the law is not on his side.[27] Also like Rosen, he 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 9/11 found only 7 percent of American felt they had personally sacrificed any important rights or liberties in the war on terrorism.[28]

Civil libertarians frequently claim that the events of 9/11 did weird things to people. To them, the government's reaction - the round-up of several hundreds of illegal aliens from Middle East countries, rushing the USA PATRIOT Act through Congress -- surely represented mass hysteria. What about what 9/11 did to them?

For those familiar with Professor Cole's career, the big surprise on *Enemy Aliens* crops up about a quarter of the way through the book, when the liberal scholar exposes himself to be as a law-and-order type. It seems that Cole, after the shock of 9/11, may be in the pro-security camp after all. He writes:

> 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 the wiretapping of any phones that a target may reasonably use, rather than only specified phone numbers, and the 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 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 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 these changes will have any effect on terrorism, these provisions do not raise civil liberties objections.[29]

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: he is not alarmed by this new technology or the prospect that it could be effectively harnessed by a legal regime to protect against unfair invasions of privacy.

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

> [The PATRIOT Act] authorizes secret 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 very 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 purposes of investigating crime....[The PATRIOT Act changes to FISA] in effect denies the Fourth Amendment's most basic protection to any person who might qualify as a foreign agent – predominantly but not exclusively foreign nationals.

What happened to Cole's endorsement of the PATRIOT Act's information-sharing rules, premised on the recognition that "international terrorism is simultaneously a matter of foreign intelligence *and* criminal law enforcement?" What about 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 taken away from the government. Why is FISA unconstitutional? According to Cole, it is because the legality of particular FISA surveillance is never subject to adversarial testing in the courts. This conclusion would be somewhat surprising to those courts that have issued judicial opinions on the constitutionality of specific FISA investigations.[30]

Unlike Rosen, Cole does not spend much space arguing that the American public is too dense to see the risks to their privacy. He is more concerned with government run amok. Here, Cole 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. He notes, for example, "While no one condones threats of violence, surely every non-citizen who gets into a bar fight with a weapon does not warrant unilateral detention, particularly as our law does not authorize such detention even for the most hardened, recidivist criminal citizen."[31] To David Cole, a government armed with the technological tools that permits it to eliminate violent crime within the confines of the constitutional jurisprudence should not deploy them 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 reach a consensus that they want it, it is because the courts and the people, unlike Cole and Rosen, do not see things their way. Both authors' criticism is directed at the government. The private sector is spared their wrath. Neither is particularly bothered by the kind of surveillance undertaken by commercial enterprises. Their real beef is with the government, and law enforcement in particular.[32]

What is particularly amazing about Cole's position is it voiced while he acknowledges that some of the post-9/11 law enforcement powers have made us us safer. He is nonetheless against them, so ingrained is his anti-government animus:

> Some of the measures 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's ability to do evil, even as they hinder many people's ability 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., in other words, that some of the measure 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 terrorist has it own substantial security costs.[33]

In other words, it is better if we risk the lives and safety of Americans on own homeland than offend those who are visitors here (and who, incidentally, are barred from voting, in a perfectly constitutional form of discrimination based on nationality), who would view the U.S. government as less "legitimate."

Back to the Future?

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

One of the beauties of my scenario is that it avoid the complaints about racial profiling. The gait index is race-blind, as is the technology that compares it against the satellite surveillance. As such, nobody can claim that certain ethnic groups are being unfairly targeted for prosecution. This would seem to solve many of Professor Cole's complaints, although 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, at least not as a constitutional matter.

What about personal privacy, the focus of Professor 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 being recorded and stored, or their movements in public being recorded by our satellites in the sky. This argument would be unavailing in light of the *Katz* doctrine. Like having your driver license photograph taken, a videotaped capture, in modern society, does not amount to a theft of your soul. Faced with this reality, Rosen would likely be relegated to arguing that the technology could not be perfected. This is, after all, how he handled 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 plat numbers are compared with a database of those stolen cars, and the system can set off an alarm whenever a suspicious car enters the city.[34]

What, exactly, is so wrong with this? Rosen does not say, other then noting current science on human face recognition is not as reliable. That hardly means that such technology should not be pursued. For him, the future is grim, since Americans are no longer alarmed by technology. As he notes in *The Unwanted Gaze*, "[Nothing in this book offers any reason to except that the public will demand laws and technologies that will 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."[35]

Why is this the case? According to Rosen, it is because our civic debate is too polarized. On the one side is what he calls the technopositivists: those who greet every proposed expansion of government surveillance power with unthinking enthusiasm. On the other side are the "principled Luddites," who are fighting the Quixotic battle against the proliferation of technologies that will ultimately ruin our humanity.[36] This polarity minimizes the prospect that a true balance can be struck. If true, it is not hard discern where Jeffrey Rosen falls on the continuum.

Endnotes

---

1. Jeffrey Rosen, *The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age* (Random House, 2004)

2. *Id.* at 5.

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

4. *Id.* at 169 ("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 persons and social costs of exposure.")

5. *Id*. at 6-7.

6. *Id*. at 34.

7. *Id*. at 36-37.

8. *Id.* at 42.

9. "In addition to threatening privacy and promoting social conformity, the cameras are in tension with the values of equality." *Id*. at 51.

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

11. *Id.* at 22.

12. *Id*. at 22.

13. Jeffrey Rosen, *The Unwanted Gaze: The Destruction of Privacy in America* (Vintage 2000)

14. *Id* at 19.

15. *Id* at 16-17. The temptation to cite archaic legal artifacts in complaints about the U.S. government' post-9/11 counterterrorism efforts must be great, since it proved too much even for the like of such legal luminaries as the late Sam Dash. In what turned out to be his final book, *Intruders: Unreasonable Searches and Seizures from King John to John Ashcroft* (Rutgers University Press 2004), Professor Dash cites an old Babylonian law from the 18th Century B.C.: "If a man makes a breach into a house, one shall kill him in front of the breach, and bury him it" (page 9). Most would agree that, however quaint, this legal doctrine is somewhat extreme and of

tenuous applicability in the post-9/11 world.

16. *Id* at 197.

17. *Id* at 50.

18. *Hiibel v. Sixth District Court of Nevada*, 542 U.S. 177, 124 S. Ct. 2451 (2004).

19. *Wabun-Inini v. Sessions*, 900 F.2d 1234 (8th Cir. 1990).

20. 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967).

21. *Wabun-Inini, supra*. at 1243. See also *California v. Ciraolo,* 476 U.S. 207, 106 S.Ct. 1809, 90 L.Ed.2d 210 (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 to expect that his marijuana plants were constitutionally protected from being observed with the naked eye from an altitude of 1,000 feet.); *Dow Chemical Co. v. United States,* 476 U.S. 227, 239, 106 S.Ct. 1819, 1827, 90 L.Ed.2d 226 (1986) (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, 104 S.Ct. 1735, 1741-42, 80 L.Ed.2d 214 (1984) (upholding warrantless search of land with marijuana crops based on the open fields doctrine); *Marshall v. Barlow's*, 436 U.S. 307, 315, 98 S.Ct. 1816, 1821-22, 56 L.Ed.2d 305 (1978) ("What is observable by the public is observable, without a warrant, by the Government inspector as well.").

22. *The Unwanted Gaze* at 61.

23. *Id.* at 4.

24. *Id*. at 7. He also notes that "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 marketers .... We have the ability to rebuild the private spaces we have lost. But do we have the will?" *Id.* at 25.

25. *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 domestic 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.

26. *Enemy Aliens* at 5. Cole refers to disparate treatment between American citizens and non-citizens as a "double standard" (page 107), while arguing that "[E]quality between non-nationals

and citizens appears to be the constitutional rule" (page 211).

27. For example, Cole cites (and criticizes) the Supreme Court's decision in *Denmore v. Kim*, 123 S.Ct. 1708 (2003), which upheld a statute mandating preventive detention during deportation proceedings of 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 national due process rights." *Id*. at 224.

28. *Id.* at 18.

29.*Id.* at 57.

30. *See e.g. United States v. Sqillacote*, 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 (2nd Cir. 1984).

31.*Enemy Aliens* at 66.

32."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 that information for their own legitimate purposes, the government lacks the capacity to collect and search it on a mass scale for law enforcement ends." *Enemy Aliens* at 73. Like Cole, Rosen accepts technologies of customer relations management designed to put customers in categories depending on their perceived value to the company. He does not like the prospect that the same 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." *Naked Crowd* at 27.

33.*Enemy Aliens* at 207.

34. *The Naked Crowd* at 39.

35. *Id.* at 193

36. *Id.* at 18.