The Silver Bullet: Protecting Privacy and Security through Law and Technology[1]

JEFFREY ROSEN
Professor of Law, George Washington University Law School

IT'S A GREAT HONOR to appear at the American Philosophical Society. I'm especially pleased to follow my friend and teacher Lawrence Lessig, whose challenge a few years ago led me to write a book from which part of the argument in this paper is drawn. We were appearing on a panel about privacy and security, and I denounced the proliferation of surveillance cameras in Britain—a technology that threatened privacy without, according to the British government's own studies, having any discernible effect in detecting violent crime or terrorism. Lessig politely but firmly called me a Luddite. Technologies of security will proliferate whether you like it or not, he suggested, and he encouraged me to learn enough about them to be able to describe the architectural and legal choices that could ensure they are designed in ways that protect privacy rather than threatening it. Based on Lessig's challenge, I became convinced that it is indeed possible to design technologies and laws that protect privacy and security at the same time. In my paper this morning, I'd like briefly to describe what those laws and technologies might look like. But then I'd like to discuss why I'm less optimistic than Lessig that the well-designed laws and technologies will, in fact, be adopted. Conceptions of privacy vary dramatically among different cultures, and the very different cultural expectations about privacy in Europe and America may vastly complicate the attempt to achieve comprehensive and balanced regulations.

Let me begin by giving two examples of the kind of technological design choices I have in mind. The simplest example is a high beam X-ray machine now being tested at Orlando International Airport. Let's call it the Naked Machine, for that's more or less what it is. An electronic strip search, the Naked Machine reveals not only metal but any plastics

[1] Read 24 April 2004, as part of the symposium "Privacy."

or foreign objects concealed under clothing.[2] But it also reveals the human body completely naked.

But the Naked Machine doesn't have to be designed in this way. Researchers at the Pacific Northwest Laboratory identified a simple programming shift that can project the images of plastics or explosives onto a nondescript mannequin, and scramble the images of the naked body into a nondescript blob.[3] With this simple adjustment, the Blob Machine, unlike the Naked Machine, guarantees just as much security while also protecting privacy.

Not all the technological choices are so simple, but I'm convinced that most of the technologies of security proposed since 9/11 can be designed in ways that look more like the Blob Machine than the Naked Machine. Consider the evolution of the Computer Assisted Passenger Profiling Systems, or CAPPS II, a controversial data-mining scheme tested by the Transportation Security Agency. In its original incarnation, the CAPPS II system proposed to unite government databases with consumer data held by private data warehouses such as ChoicePoint and Axciom. Using the same neural network technology used by credit card companies to identify credit card fraud, the initial proposals for CAPPS II planned to examine passengers' living arrangements and travel and real estate history, along with a great deal of demographic, financial, and other personal information, to determine whether or not individual passengers resembled the 9/11 terrorists. Based on their risk index, the CAPPS II program proposed to label travelers as "green," "yellow," or "red" security risks, and subject them to correspondingly intrusive scrutiny.[4]

In its original form, CAPPS II was a Naked Machine–like technology that raised two important objections—it was unlikely to increase security and it posed grave threats to privacy. The security objection is that terrorism is not the kind of activity that follows predictable patterns—the next attack is unlikely to resemble the last one. Unlike people who commit credit-card fraud—a form of systematic, repetitive, and predictable behavior that fits a consistent profile identified by millions of transactions—there is no reason to believe that terrorists in the future will resemble those in the past. There were only eleven hijackers

---

[2] Kevin Maney, "The Naked Truth About a Possible Airport Screening Device," *USA Today*, 7 August 2002, p. 3B.

[3] Mick Hamer, "All-Seeing Scan Spares Your Blushes," *New Scientist*, 17 August 2002, p. 10.

[4] Robert O'Harrow Jr., "Air Security Focusing on Flier Screening: Complex Profiling Network Months Behind Schedule," *Washington Post*, 4 September 2002, p. A1.

on 9/11, and those who followed them the next year weren't Saudi Arabians who went to flight school in Florida: they included Richard Reeves, the English citizen who hid a bomb in his shoe, and who had a Jamaican father and an English mother. By trying to identify people who look like the 9/11 hijackers, the profiling scheme is looking for a needle in a haystack, but the color and the shape of the needle keep changing. "Some terrorism experts are skeptical about terrorist profiling," writes a 1999 report prepared by the Library of Congress for U.S. intelligence agencies. "There seems to be general agreement among psychologists that there is no particular psychological attribute that can be used to describe the terrorist or any 'personality' that is distinctive of terrorists."[5] For this reason, the U.S. Secret Service, which once looked for people who fit profiles of stereotypes of presidential assassins, has abandoned its personality profiles and now looks for patterns of motive or behavior.[6]

Moreover, because the sample of known terrorists is so small, attempts to identify suspects with electronic profiles are bound to produce a high number of "false positives"—that is, passengers whom the system wrongly identifies as likely terrorists—and the costs of the system are likely to outweigh its benefits. To illustrate why data profiling systems are likely to be ineffective in looking for needles in haystacks, Christopher Guzelian and Mariano-Florentino Cuéllar of Stanford Law School note that, at one point, doctors used to recommend monitoring large numbers of people for signs of latent diseases such as diabetes or ovarian, lung, or skin cancer. But because of the inaccuracy of profiling systems in identifying symptoms that occur very rarely in the population at large, the medical establishment has concluded that the benefits of monitoring are outweighed by the costs, which include not only false positives—or people wrongly identified as being sick—but also false negatives—or people wrongly identified as being healthy.[7]

In the case of terrorism, of course, the prevalence of potential terrorists in the population as a whole is unknown. But imagine a profiling system that was set up to identify the 11 hijackers of 9/11. Searching for 11 individuals in a population of 300 million would yield exponentially more false positives: even assuming the profiling system is 99 percent accurate, because of the low prevalence rate, 3,000,000 (that's .01 ×

[5] Rex A. Hudson and the staff of the Federal Research Division of the Library of Congress, *Who Becomes a Terrorist and Why: The 1999 Government Report on Profiling Terrorists* (Guilford, Conn.: Lyons Press, 1999), 67.

[6] Ibid., 68.

[7] Christopher Guzelian and Mariano-Florentino Cuéllar, "When Terrorists Are the Needles and America Is the Haystack," unpublished draft on file with the author.

300 million) of those identified as potential terrorists by the system would be wrongly accused. Such a system would bring the nation's airports to a halt. In other words, only 0.000363 percent of the people who tested positive in a nearly perfect system actually would be positive—a success rate so low that the system would have to be stopping a nuclear bomb on the benefits side and imposing little more than a pat-down on the costs side to be justified. But in fact, of course, no data-mining system has proved to be 99 percent accurate in predicting terrorist behavior, because the new attacks so rarely resemble the previous ones. A system with only 1 percent accuracy would falsely accuse nearly all innocent travelers of being terrorists and correctly identify only a fraction of terrorists while missing nearly all of the real terrorists. No rational evaluation of costs and benefits would support the adoption of such a hopeless system as an effective tool for national security. For this reason, efforts to use dataveillance as a way of predicting terrorist behavior in the population at large, rather than investigating individuals who have been identified as terrorists by other means, seems empirically dubious.

In its original form, the CAPPS II system also posed grave threats to privacy. The designers of the system proposed to include in its database not only the passenger data that airlines currently maintain as part of the Computer Assisted Passenger Profiling System, or CAPPS—such as travel history, address, and telephone number—but also publicly available marketing data that is currently maintained by private companies. This could include living arrangements, household income, pet ownership, personal buying habits, and even lists of the books we buy and the music we listen to. In addition, some of the companies contacted by the government hoped to include personal data whose use is currently restricted by law, including records of individual credit card purchases of fertilizer or flight school lessons, for example, or international telephone calls to Afghanistan.

Because CAPPS II, as originally proposed, included no controls on the use of this data, it would have been possible for the government to scan a traveler's consumer behavior and telephone calls, share unusual behavior with law enforcement agencies, and prosecute him for low-level offenses that had nothing to do with terrorism. This raised a danger of politically discriminatory prosecutions of the kind that President Nixon engaged in when he scanned the tax returns of Vietnam protesters and threatened them with exposure. It was the effort to avoid this kind of Nixon effect that led Congress to pass the Privacy Act of 1974.

Happily, the CAPPS II system, in its current incarnation, has been redesigned in ways that look far more like the Blob Machine than the Naked Machine. Two important design modifications are worth noting. First, the system is now limited to the goal of "authenticating"

that individual airline passengers are who they say they are, rather than trying to identify them as possible terrorists based on their consumer profiles. By focusing on authentification rather than identification, the system avoids the dangers of false positives that arise from predictive data mining and is likely to be a more effective technology of security.

Second, as for privacy, the system now includes controls on the secondary uses of data. In its initial announcement last January, the administration proposed to share personal data from the CAPPS II system with national and international police to allow the prosecution of any civil or criminal violations. But critics objected that this could create widespread abuses, allowing the administration to scour the personal data of millions of people, uncover relatively minor offenses, and threaten its critics with vindictive prosecutions. In response to these criticisms, the Transportation Security Agency agreed last August to restrict officials from sharing personal data with law enforcement agencies, except in the cases of individuals who had an outstanding federal warrant for a violent crime.

This is a welcome and important victory for privacy. It recognizes an insight that some European countries have adopted in designing technologies of security. The German wiretap law, for example, allows intelligence authorities to use wiretaps for domestic surveillance only when there is factual basis to suspect that one of a list of crimes involving a threat to national security has been or is about to be committed. The German law says that evidence obtained through wiretapping can be used only in the investigation and prosecution of the specified national security crimes or certain other serious crimes; if the intelligence officers find evidence of low-level crimes, they may not share it with law enforcement officers or introduce it in court.[8]

Because of Germany's distinctive history with the Nazis and the Stasi, the German intelligence services have been constrained by a special sensitivity to privacy.

Unlike Germany, however, America has no comprehensive regulation of the sharing of information by commercial databases in the private sector. As a result, the victory of CAPPS II may prove to be illusory, and much of the data-mining originally proposed by the government may be contracted out to private organizations whose use of the data is unconstrained. To construct an effective Blob Machine–like regime of data mining, America would need a combination of public and private

[8] Craig M. Bradley, "The Exclusionary Rule in Germany," 96 *Harv. L. Rev.* 1032, 1054–55 (1983).

sector regulation of the kind that libertarians in Congress are reluctant to embrace. A bipartisan coalition of civil libertarian liberals and libertarian conservatives has proved effective in resisting the executive's most dramatic proposals for government surveillance after 9/11. But because of its suspicion of private sector regulation, the same coalition has been unwilling to consider the kind of complicated compromises and controls on the use of data by the public sector that an effective Blob Machine technology would require.

This leads me to focus, in the rest of my paper, on the cultural constraints that make effective regulation of technologies of security difficult to obtain. There are no generally shared intuitions about privacy: different countries respond to different dangers in different ways. To put the problem in brief: Americans tend to be much more concerned about government surveillance while Europeans tend to be more concerned about privacy invasions by the private sector; but because of the complicated technological interplay of public and private surveillance, any effective regulatory scheme has to take account of both concerns.

Contrast the American and European attitudes about financial information. Europeans are far more sensitive than Americans about disclosing financial information, steeped as they are in the aristocratic tradition that respectable people don't discuss money in public. And European law reflects this squeamishness. The traditional rule in France made it a violation of privacy rights to reveal another person's salary, and for hundreds of years the French nobility successfully resisted laws requiring public registration of their mortgages. In France and Germany today, consumer credit reports are available only in the case of people in financial difficulties. In Germany, consumers seeking credit must explicitly authorize lenders to share information about them, and before any information can be shared, the privacy interest of the borrower must be balanced against the commercial interests of the lender.[9]

Financial reporting is not the only area in which Americans' cultural ideas about privacy differ dramatically from those in Europe. If visitors from Europe are scandalized by the casual way Americans discuss their salaries with strangers, they are also surprised by Americans' discomfort with public nudity on beaches or with female bathroom attendants in men's restrooms. At the same time, Europeans are far more trusting of government, and willing to allow it to regulate personal choices in ways that Americans would find intolerable—such as the naming of infants, for example. And these cultural differences are reflected

[9] James Q. Whitman, "Two Western Cultures of Privacy: Dignity Versus Liberty," 113 *Yale Law J.* 1153, 1192–94 (2004).

in dramatic differences in law. European law protects not only consumer data and credit reporting but also email privacy in the workplace, discovery in civil cases, and the distribution of nude pictures on the Internet, while American law allows dramatic violations of privacy in all of these areas.

"Why is it that French people won't talk about their salaries but will take off their bikini tops?" James Whitman of Yale Law School asks in a pathbreaking article called "The Two Western Cultures of Privacy." "Why is it that Americans comply with court discovery orders that open essentially all of their documents for inspection but refuse to carry identity cards?"[10] Whitman's answer is succinctly expressed in his subtitle: "Dignity versus Liberty." When Europeans think about privacy, they are most concerned about personal dignity and the right to control one's public image—a right threatened primarily by the mass media, the Internet, and commercial data warehouses. By contrast, American conceptions of privacy are focused on personal liberty and the right to be free from state surveillance, threatened primarily by government intrusions into the home.

The European conception of privacy as a protection for dignity rather than liberty, Whitman argues, stems from its aristocratic tradition of protecting personal honor. For most of European history, this was a hierarchical tradition: for some people to have honor, it was necessary for others not to have it, and, for people to be treated with the honor to which they were entitled by their station, everyone had to know his or her place. But over the course of the nineteenth century, the defense of personal honor and interpersonal respect began to migrate from something that high-status people expected to defend through law. And during the twentieth century, the legal protections against personal insult were increasingly "leveled up,"[11] as Whitman puts it, and extended to all citizens, not only high-status ones. Repeatedly, however, the legal protections for personal honor in Europe clashed with two freedoms that Americans take for granted—property rights and freedom of the press.

The cultural differences between European and American conceptions of privacy have important legal implications for their attempts to balance privacy and security. Europeans tend in general to be less suspicious of centralized government authority than Americans. As Kim Lane Scheppele of the University of Pennsylvania has noted, Europe's greater deference to government authority led countries like Germany

[10] Id. at 1161.
[11] Id. at 1167.

and France to adopt surveillance measures after 9/11 that in some ways went farther than the U.S.A. Patriot Act. In 2002, for example, Germany adopted a sweeping law that increased the power of its security agencies in important ways. The government was authorized to create a central database with personal information about foreigners, including fingerprints and religious background. The law also authorized the German national identification cards to include biometric data, such as fingerprints. And it explicitly endorsed data mining along the Total Information Awareness model, requiring government agencies to turn personal information over to the federal police.[12]

The great variation between the European and American response to 9/11 reflects our different historical conceptions of privacy and state authority, but it also poses a challenge to policy makers: in an age of integrated databases and the Internet, it may be costly to have very different rules about what sort of information can be shared among and between intelligence agencies, law enforcement officials, and the private sector in America and Europe. It is now conventional wisdom, in fact, that increased information sharing is the best way of preventing terrorism, but information sharing between the public and private sector may be difficult if the Americans are focused on the dangers of state surveillance and the Europeans are concerned about protecting the dignity of the consumer. At the same time, in the age of the Internet, attempts to protect the rights of Europeans to control the distribution of their images in the name of dignity may be thwarted by the refusal of cyberspace to respect national boundaries.

Is there any possibility for privacy advocates to expand the cultural understandings of privacy in Europe and America, so that the Europeans come to care more about liberty and the Americans more about dignity? When it comes to the protection of privacy, legal values tend to reflect and follow social understandings, rather than the other way around. Perhaps those who hope to import European understandings of privacy into America, and vice versa, should focus on changing social understandings of privacy rather than on passing new laws.

But can social understandings of privacy easily be changed to accommodate both honor and liberty? Not necessarily. "In the beginning," said Locke, "all the world was America."[13] An unsettling possibility for privacy advocates is that as Europe becomes more and more like America—that is, more market driven, less hierarchical, more democratic,

---

[12] Kim Lane Scheppele, "Other People's Patriot Acts," unpublished draft on file with the author.

[13] John Locke, *An Essay Concerning the True Original, Extent and End of Civil Government, Book II* (London: Everyman's Library, 1986), 140.

and more distant from its aristocratic past—the popular consensus about the importance of protecting dignity will atrophy and eventually collapse under the weight of market forces. A society where citizens refuse to respect their own privacy is not one where privacy will be long respected; and the American experience suggests that citizens in an individualistic market democracy may perceive too many market rewards for exposure to respect their own privacy for long.

As European traditions of dignity are withering in the face of American-style assaults of the market, American traditions of suspicion of government may be threatened by the persistent anxieties of an age of terrorism. It's not hard to imagine, in the face of future attacks, the bipartisan libertarian coalition being overwhelmed in the face of public demands for security above all. Unrestrained by libertarian minorities, the public in a public opinion state will sacrifice privacy to security at every turn.

All this reminds us that privacy—understood as a protection for dignity or as a bulwark for liberty—is not an especially democratic virtue. It is a virtue historically demanded and enjoyed by aristocratic minorities and extended, in Europe and America, to a broader population that often was indifferent to its benefits and demands. Dignity requires a degree of self-restraint on the part of citizens—good manners, reticence, self-respect, and a willingness to respect the dignity of others; while liberty requires a degree of civic engagement—only informed and educated citizens can check the excesses of the state. Neither dignity nor liberty can easily be achieved in a nation of anxious exhibitionists, more concerned about attracting attention than deflecting it. To defend privacy, in other words, citizens in democracy have to care about privacy, and it's increasingly clear that many of us do not.