2004

Uncle Sam is Watching You

David Cole
Georgetown University Law Center

David Cole, "Uncle Sam is Watching You," The New York Review of Books, November 18, 2004, at 56 (reviewing Samuel Dash, The Intruders: Unreasonable Searches and Seizures from King John to John Ashcroft (2004) and Jeffrey Rosen, The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age (2004)).

October 2009

Uncle Sam is Watching You

The New York Review of Books, November 18, 2004, at 56.

David Cole
Professor of Law
Georgetown University Law Center
cole@law.georgetown.edu

The New York Review of Books

VOLUME 51, NUMBER 18 · NOVEMBER 18, 2004

Uncle Sam Is Watching You

By David Cole

The Intruders: Unreasonable Searches and Seizures from King John to John Ashcroft
by Samuel Dash
Rutgers University Press, 172 pp., $22.95

The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age
by Jeffrey Rosen
Random House, 260 pp., $24.95

1.

In October 2003, Congress voted to end Total Information Awareness (TIA), a Pentagon plan designed to analyze vast amounts of computer data about all of us in order to search for patterns of terrorist activity. At the time, the vote in Congress seemed one of the most notable victories for privacy since September 11. Computers record virtually everything we do these days—whom we call or e-mail, what books and magazines we read, what Web sites we search, where we travel, which videos we rent, and everything we buy by credit card or check. The prospect of the military and security agencies constantly trolling through all of this information about innocent citizens in hopes of finding terrorists led Congress to ban spending on the program.

Admittedly, much of the credit for TIA's defeat has to go to the Pentagon's public relations department, which not only gave the program its less than reassuring name, but also came up with a logo consisting of a pyramid topped by a large, digitized eye and the Latin motto *Scientia Est Potentia*, or "Knowledge Is Power." George Orwell and Michel Foucault could hardly have done better. It also helped that the Pentagon's Defense Advanced Research Projects Agency (DARPA), which developed the plan, was headed by John Poindexter, who had been convicted of lying to Congress in the Iran-contra affair, and whose conviction had been overturned on appeal only on a technicality. The vote to kill TIA came shortly after DARPA floated the idea of creating a market for betting on terrorist attacks and other disasters. Still, the fact that Congress rejected TIA seemed to suggest that it was willing to stand up for privacy even in the face of the threat of catastrophic terrorism.

But reports of the death of TIA were greatly exaggerated. Federal programs to collect and search vast computer databases for security purposes continue virtually unabated, inside and outside the Pentagon. The congressional ban did not apply to the Pentagon's classified budget, so the military's development of programs to collect and analyze computer data has simply moved behind closed doors. Congress has directed the Department of Homeland Security to develop "data mining and other advanced analytic tools...to access, receive and analyze data, detect and identify threats of terrorism against the United States." And with federal funding, several states are cooperating in the Multistate Antiterrorism Regional Information Exchange System, or MATRIX, which links law enforcement records with other government and private databases in order to identify suspected terrorists.

The private firm that is running MATRIX, Sesint, based in Florida, previously compiled a "terrorist index" of 120,000 persons using

> such factors as age, gender, ethnicity, credit history, "investigational data," information about pilot and driver licenses, and connections to "dirty" addresses known to have been used by other suspects.

Thus, despite the apparent victory for civil libertarians in stopping TIA itself, data mining remains a central instrument in the government's response to the threat of terrorism. As a special committee appointed by Defense Secretary Donald Rumsfeld wrote in its recently released report, "TIA was not the tip of the iceberg, but rather one small specimen in a sea of icebergs."

"Data mining," the computerized analysis of extensive electronic databases about private individuals for patterns of suspicious activity, is just one example of the threats to privacy that Americans have faced following the terrorist attacks of September 11, 2001. Since then, through the USA Patriot Act and various executive initiatives, the government has authorized official monitoring of attorney– client conversations, wide-ranging secret searches and wiretaps, the collection of Internet and e-mail addressing data, spying on religious services and the meetings of political groups, and the collection of library and other business records. All this can be done without first showing probable cause that the people being investigated are engaged in criminal activity, the usual threshold that must be passed before the government may invade privacy.

Of course, these laws and policies merely authorize such snooping. They do not compel it. The administration's message since September 11 has been "trust us." President Bush and Vice President Dick Cheney say that critics have cited "no abuses" of the USA Patriot Act, as if to suggest that absence of visible abuse shows that we can trust them. But the "no abuses" defense is fundamentally misleading in two respects.

First, there have in fact been abuses of the Patriot Act. In June, a jury in Idaho acquitted Sami Omar al-Hussayen, an Idaho student charged under the Patriot Act for aiding terrorism because he had a Web site that included links to other Web sites that included some speeches endorsing terrorism. The government never even alleged, much less proved, that al-Hussayen had intended to further any terrorist activity. Under its theory, any posting of a link to a Web site advocating terrorism is a violation of the Patriot Act's ban on providing "expert advice and assistance" to designated "terrorist organizations." If that's true, *The New York Times* could be prosecuted for including a link to Osama bin Laden's latest recorded message, and it would be no defense to show that the link was posted solely for educational purposes.

In another case involving the same Patriot Act provision, the Humanitarian Law Project, a human rights group in Los Angeles, faces the threat of criminal prosecution for advising a Kurdish group in Turkey on protecting human rights. The project has provided the training precisely to discourage violence and to encourage the pursuit of lawful means to advance Kurdish rights in Turkey. Yet the administration claims that it can prosecute such human rights advocacy as "material support of terrorism," even though it consists solely of speech and is not intended to promote violence. The courts have thus far ruled that the Patriot Act's application to such activity is unconstitutional, but the Bush administration is appealing.

Similarly ominous is the case of Khader Hamide and Michel Shehadeh, two longstanding permanent resident aliens from Palestine now in Los Angeles.[1] They have lived in the US for more than twenty-five and thirty years, respectively, and have never been charged with a crime. The administration is trying to deport them under the Patriot Act for having distributed magazines of a PLO faction in Los Angeles during the 1980s. The government does not dispute that it was entirely lawful to distribute the magazines at the time, or that the magazines are themselves legal and available in libraries across the country. Yet it claims that under the Patriot Act, it can retroactively deport the two Palestinians for engaging in activity that would plainly be protected by the First Amendment if engaged in by US citizens.

Still another provision of the Patriot Act allows the government to freeze the assets of any person or

entity it chooses, simply by claiming that he or it is under "investigation." It can then defend the action in court with secret evidence, presented to the court in a closed session but not disclosed to the entity or person whose assets have been frozen. The Bush administration has used this authority to close down three of the largest Muslim charities in the United States, without ever having to prove that they actually financed terrorism, and without affording the charities an opportunity to defend themselves.

In July, the administration invoked the Patriot Act to deny entry to Tariq Ramadan, a highly respected Swiss-born Muslim scholar. Ramadan, a moderate hired by Notre Dame to fill a chair in international peace studies, was apparently excluded under a Patriot Act ban on those who "endorse terrorism." The administration has refused to specify his allegedly offending words.

And in September, a federal court in New York ruled that the FBI's enforcement of still another Patriot Act provision squarely violated the First and Fourth Amendments. The court ruled that the provision, which authorizes the FBI to compel Internet service providers to turn over information about their customers, is invalid because it prohibits the provider from disclosing to anyone—even a lawyer—that the FBI request was made, and effectively precludes any judicial review.

So the first problem with the administration's claim that there have been no abuses under the Patriot Act is that it is simply false. There have been plenty of abuses.

The second problem is more insidious. Many of the Patriot Act's most controversial provisions involve investigative powers that are by definition secret, making it literally impossible for abuses to be uncovered. For example, the act expanded the authority to conduct wiretaps and searches under the Foreign Intelligence Surveillance Act (FISA) without having to show probable cause of criminal activity. We know from a government report that the number of FISA searches has dramatically increased since the Patriot Act was passed, and for the first time now exceeds the number of conventional wiretaps authorized in criminal cases. Yet that's all we know, because everything else about FISA searches and wiretaps is secret.

The target of a FISA search is never notified, unless evidence from the search is subsequently used in a criminal prosecution, and even then the defendant cannot see the application for the search, and therefore cannot test its legality in court. When the attorney general uses conventional criminal wiretaps, he is required to file an extensive report listing the legal basis for each wiretap, its duration, and whether it resulted in a criminal charge or conviction. But no such information is required under FISA. The annual report detailing use of the criminal wiretap authority exceeds one hundred pages; the report on the use of FISA is a one-page letter.

Another provision of the Patriot Act radically expands the government's ability to obtain personal business records without showing probable cause. Before the Patriot Act was passed, the government had to limit its inquiries to a specific set of financial, phone, and travel records, and these could be obtained only if the target was an "agent of a foreign power." The Patriot Act expanded the definition of records that may be seized, so that it now includes, among other things, library and bookstore records and medical files. And it eliminated the requirement that the person whose records are sought be an "agent of a foreign power." Now the government can get anyone's records. Here, too, the authority is veiled in secrecy. The Patriot Act makes it a crime for the person or organization ordered to produce records to tell anyone about the request. The act does not require the government to notify people whose records have been reviewed, and does not require that any report of its activities be made available to the public.

The Internet service provider that brought the successful challenge to the Patriot Act described above had to violate the law's nondisclosure provision to do so, and the lawsuit itself had to be filed in secret until the court allowed its existence to be acknowledged.

The administration's challenge to critics to come forward with examples of abuse under the Patriot Act is therefore disingenuous. The most controversial provisions contain legal requirements of secrecy that make it literally impossible to provide such examples. Moreover, when the House and Senate Judiciary Committees have requested even the most general information about how the Patriot Act authorities have been used, the administration has refused to supply it.

As Elaine Scarry has written, the government since September 11 has asserted that more and more of the lives of citizens must be open to scrutiny, while simultaneously insisting that more and more of its own operations have to be kept secret.[2] Yet a healthy democracy depends on exactly the opposite —transparency in government and respect for personal privacy. That is why, following Watergate, Congress in 1974 simultaneously enacted the Privacy Act, which strictly limits federal collection and use of information about its citizens, and expanded the Freedom of Information Act, which gives citizens access to information about their government. Supreme Court Justice Lewis Powell defended the essential role of privacy in a democracy in a landmark 1972 decision invalidating warrantless domestic security wiretaps:

> The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of Government action in private conversation. For private dissent, no less than public discussion, is essential in our free society.

As we all learned on September 11, improved technology has made it easier for terrorists to coordinate their attacks around the world. If improved technology might also help us detect and prevent the next terrorist attack from occurring, we surely must explore those possibilities. But the increased ability to monitor dangerous activity in the digitized age necessarily carries with it the increased ability to monitor political dissent, and history suggests that monitoring the one may quickly lead to monitoring the other. In the interest of identifying terrorists, the Justice Department after World War I created a Radical Alien Division to monitor and track subversive foreigners. When a series of terrorist bombings struck in the summer of 1919, that division responded with the Palmer Raids, in which thousands of foreign nationals were rounded up, denied lawyers, interrogated incommunicado, and issued deportation orders, not for their involvement in the bombings—the bombers were never found—but for their political affiliations.

The fear of communism in the cold war led the FBI to monitor and maintain files on hundreds of thousands of Americans, including politicians, judges, civil rights activists, and anti-war demonstrators. Before the Republican National Convention in New York, FBI agents confronted peaceful political activists with threats of prosecution if they failed to disclose any information about possible unlawful demonstrations. Such surveillance and harassment has a profoundly chilling effect on people's willingness to engage in the political activity that is essential to a vital democracy. If the threat to privacy seems abstract by comparison to the threat of a terrorist attack, consider what J. Edgar Hoover might have done had he had a program like TIA.

2.

How, then, should the tensions between privacy and security in the war on terrorism be resolved, and who is best situated to strike that balance—the courts, Congress, the executive branch, or the people?

Two books by prominent Washington law professors put forward different views about how best to answer these questions. *The Intruders*, by the late former chief counsel to the Senate's Watergate committee and Georgetown law professor Sam Dash, who died in May, is a passionate short history of the Constitution's principal safeguard of privacy, the Fourth Amendment prohibition on unreasonable searches and seizures. His book presents a tale of two courts—the Warren Court of the 1950s and 1960s, which aggressively expanded the protection of privacy, and today's Rehnquist Court, which has just as

aggressively decimated those rights. Like the great lawyer he was, Dash uses his stories to argue persuasively for the resurrection of meaningful judicial safeguards.

The Naked Crowd, by Jeffrey Rosen, a professor at George Washington University School of Law, considers the political, financial, and psychological factors that are likely to shape the law of privacy in the decades to come. Rosen spends less time on the law as such, and more on the social forces at play in the Internet age; our privacy, he argues, is threatened not only by government programs like TIA but by the public's low estimate of the value of privacy. Rosen is skeptical about the courts' willingness to protect privacy, but guardedly optimistic about Congress's ability to do so.

In his book, Dash reminds us that real safeguards against official intrusion into the lives and affairs of the people took centuries to develop. He notes, for example, that the Magna Carta did not bar the king from searching private homes whenever he wanted. And until 1961 the US Constitution's protections against unreasonable searches and seizures did not extend to state and local police, who carry out over 90 percent of law enforcement. In that year, the Supreme Court first applied the "exclusionary rule" to the states, meaning that evidence obtained in violation of the Fourth Amendment had to be excluded from the case against a defendant. Similarly, the Court did not give indigent defendants the right to appointed lawyers until 1963, and did not create Miranda rights in police interrogations until 1966.

There are good reasons why the rights of privacy and liberty flourished in the civil rights era. That period, perhaps more than any other, demonstrated the danger of unconstrained law enforcement, as Southern police and the FBI alike harassed and prosecuted civil rights activists, using the criminal law as a means to monitor, regulate, and penalize dissent.

Dash demonstrates, however, that almost as soon as the Fourth Amendment was extended to the states, the Supreme Court under Chief Justices Burger and Rehnquist began whittling away its protections. The Court created many exceptions to the "exclusionary rule" in the 1970s, permitting illegally obtained evidence to be used, for example, in grand jury, immigration, and civil tax proceedings. In 1978, the Court allowed the government to use illegally obtained evidence to incriminate anyone other than the person whose privacy rights were violated. In 1984, it ruled that as long as the police obtained a search warrant, the exclusionary rule ought not apply, even if the warrant itself was illegal. These exceptions dramatically weakened Fourth Amendment protections by telling police that they can use illegally obtained evidence for a wide variety of purposes.

The Court under Burger and Rehnquist also directly relaxed the requirements of the Fourth Amendment, allowing a great many kinds of searches without warrants or probable cause at all. Most of these changes were made in the context of the "war on drugs." Because narcotics are easy to conceal and there are often no complaining witnesses to drug crimes, the usual requirement that the police show probable cause that a person possesses an illegal substance before they can search him posed a considerable obstacle to enforcing drug laws. The Court accordingly relaxed the Constitution's requirements. But if the Fourth Amendment could not withstand the pressures of the war on drugs, how is it likely to fare in the war on terrorism?

Both Rosen and Dash express particular concern about data mining, which they compare to the "general warrants" that allowed the British colonial government to search anyone's home, without having any prior ground for suspicion. Like "general warrants," data mining permits officials to search the private computer records of innocent people without any specific basis of suspicion. Objections to "general warrants" in-spired the Fourth Amendment; yet the Framers could not have contemplated computerized searches of extensive public and private databases. And therefore, Dash suggests, it is up to the Supreme Court to extend Fourth Amendment principles to modern practices.

Ironically, the Supreme Court decision that is widely credited with adapting the Fourth Amendment to the twentieth century now threatens to render it powerless to regulate data mining and other modern

surveillance techniques in the twenty-first. In its 1967 decision *Katz* v. *United States*, the Supreme Court reversed forty years of precedent and ruled that the Fourth Amendment's prohibition on unreasonable searches and seizures applies to electronic eavesdropping and wiretapping. Federal officials had placed a listening device on a phone booth used by Charles Katz and had overheard him discussing illegal gambling activities. They did not obtain a warrant, because in previous decisions, the Supreme Court had ruled that the Fourth Amendment was not implicated so long as the government's investigatory tactics did not invade a person's property. Since Katz had no "property interest" in the phone booth, the federal government reasoned, there was no need to obtain a warrant to listen in on his phone call.

The Court in the *Katz* case held that the Fourth Amendment "protects people, not places." Under the new approach, the Fourth Amendment is violated whenever the police invade an individual's "reasonable expectation of privacy," regardless of property rights. Since people reasonably expect their phone conversations to be private, the police cannot listen in without a warrant and probable cause.

The *Katz* decision has long been hailed for recognizing the need to adapt the Fourth Amendment to advances in technology. Once phones could be tapped without going anywhere near a caller's property, the Court's property-based approach no longer made sense. Nothing less than a major shift in Fourth Amendment jurisprudence was required, and *Katz* provided it.

Today, however, a second and equally momentous shift is needed. The development of computer technologies threatens to radically alter the balance between privacy and security. Computers make it possible to find, store, exchange, retrieve, and analyze vast amounts of information about our private lives in ways that previously were unthinkable. But while the Court's ruling in *Katz* freed Fourth Amendment doctrine from its moorings in antiquated notions of property, its emphasis on "reasonable expectations of privacy" left privacy vulnerable to future advances in technology. As technology makes it increasingly easy to invade spaces that used to be private through the use of enhanced listening, viewing, and other sensing devices, "expectations of privacy" and the protection of the Fourth Amendment may be radically reduced.

The Rehnquist Court's most disturbing application of the *Katz* approach is its determination that people have no "reasonable expectation of privacy" concerning any information they share with others. When we convey information to another person, the Court has reasoned, we assume the risk that the person will share it with the government. On this theory, people have no expectation of privacy when they dial phone numbers, surf the Web, make a credit card purchase, put out their garbage, or talk with people they think are their friends but are in fact informants. As a result, the Fourth Amendment imposes no restriction on the government obtaining such information and subjecting it to searches for suspicious behavior, even when it has no good reason to suspect a person of wrongdoing.

Before the computer, the government's ability to collect and exploit such information was limited. In the future, the possibilities are likely to be unlimited. Computer searches can be used to identify "suspicious" patterns based on peoples' reading habits, travel, Web surfing, and cell phone records, not to mention their age, sex, race, and religion.

The Court's "third-party disclosure" doctrine is as inapt for the computer age as its property-based approach was for wiretapping. It is simply wrong to equate sharing information with a private corporation as a prerequisite to having a phone or e-mail line, and sharing that information with the government. It is one thing for AOL to know what Web sites you have searched; it is another matter entirely for the federal government to have that information. AOL can't lock you up, and has less reason to harass you for your political views.

As Justice John Marshall Harlan argued in a separate opinion in the *Katz* case, the test of whether the Fourth Amendment is violated should not be merely whether, as a factual matter, society expects a given form of communication to be private, but whether maintaining the privacy of that communication from

unwarranted government intrusion is essential to the workings of democracy. On that view, constitutional privacy under the Fourth Amendment is not an objective fact wholly captive to technology, but a social value that we choose to protect despite technological advances.

Jeffrey Rosen suggests that the threats to privacy come not only from technological advances and the courts' failure to confront them, but also from public attitudes. Surveying a wide range of psychological literature, Rosen argues that people are susceptible to powerful irrational fears that compromise their ability to protect their own interests in preserving privacy. Most people, he claims, have "trouble distinguishing improbable events," such as terrorist attacks, "which tend to be the most memorable, from mundane events, which are more likely to repeat themselves." They therefore demand "draconian and symbolic but often poorly designed laws and technologies of surveillance and exposure to eliminate the risks that are, by their nature, difficult to reduce." At the same time, many Americans in the modern age seem to crave exposure more than privacy, as demonstrated, he argues, by the increasing popularity of reality TV, Web logs, and advice books about how to "market" oneself.

The private market only reinforces these tendencies. Rosen shows that the high-tech industry has incentives both to encourage public anxiety about terror threats and to compete for the public dollars that will reward technological "solutions" to the demand for total security. Security is a growth industry; a speaker at a trade electronics forum in Las Vegas estimated that spending on security technologies, including listening devices and databases, will increase by 30 percent a year, reaching $62 billion a year in 2006. Rosen quotes Larry Ellison, Oracle's CEO, who boasts that in the name of advancing national security, his company will create a global database within the next twenty years, "and we're going to track everything."

Rosen agrees with Dash that Fourth Amendment doctrine does not adequately protect privacy in today's high-tech world; but he considers it a waste of time to look to the courts for relief. In his view, history shows that Congress is better situated to protect privacy. While the Supreme Court has radically diluted the protection of privacy and allowed government access to financial and other data through its "third-party disclosure" doctrine, Congress has enacted many statutes protecting privacy despite the Court's decisions, including the Privacy Act, the Fair Credit Reporting Act, the Right to Financial Privacy Act, and the Health Insurance Portability and Accountability Act. These laws restrict government access to financial and health-related data, and impose limits on the government's recording of political communications and other First Amendment activities.

Rosen's confidence in the political process is paradoxical, however, since he also believes that the public today is more interested in publicity than in privacy, and that both the public and the commercial markets favor security over privacy. The only sure thing about Congress is that it will respond to public opinion and market forces. If there is no possibility of increasing the public's concern about privacy, there is also little hope for Congress.

This brings us back to Dash's plea that the courts intervene on behalf of privacy. Recognizing the risk that the public and the political process may disregard fundamental rights in times of crisis, the Founders protected those values in a constitution that is difficult to change, and made it enforceable by judges with life tenure. The courts have often failed to live up to their responsibility to protect the Bill of Rights but that is no reason not to hold them to it. If Dash may expect too much from the courts, Rosen asks for too little.

The Supreme Court's recent decisions rejecting the Bush administration's sweeping assertion of unchecked authority to lock up human beings indefinitely without trial or hearing illustrate this point. Congress took no steps whatever to confront the President on behalf of the six hundred men held at Guantánamo or the three men held in a brig in South Carolina. Whatever the limitations of its recent decisions, it took the Supreme Court to challenge the President.

The ultimate defender of liberty, however, is neither the Court nor Congress, but the people. In 1931 Judge Learned Hand famously warned Yale Law School graduates that

> Liberty lies in the hearts of men and women; when it dies there, no constitution, no law, no court can save it.... While it lies there it needs no constitution, no law, no court to save it.

Like many memorable quotes, Hand's warning sacrifices nuance for rhetoric. The Constitution, the law, and the courts all serve to remind us of (and therefore to reinforce) our collective commitment to liberty.

But Hand was surely right that we cannot rely *exclusively* on constitutions, courts, or laws. In that light, perhaps the most promising development since September 11 for those who care about principles of liberty and privacy has been the grassroots campaign of the Bill of Rights Defense Committee. The committee was formed immediately after the Patriot Act was passed, by civil rights activists in Amherst, Massachusetts, who had what may have seemed the wildly impractical idea of getting local city and town councils to pass resolutions condemning the civil liberties abuses in the act. The committee began its campaign in the places one might expect—Amherst, Northampton, Santa Monica, Berkeley. But today, more than 340 jurisdictions across the country have adopted such resolutions, including legislatures in four states—Vermont, Alaska, Maine, and Hawaii—and many of the nation's biggest cities, including New York, Los Angeles, Chicago, Dallas, Philadelphia, and Washington, D.C.[3]

The resolutions typically condemn not only the surveillance provisions of the Patriot Act—particularly the surveillance of libraries and private records—but also the administration's tactics of mass preventive detention of noncitizens, open-ended imprisonment of "enemy combatants," ethnic profiling, and denials of access to lawyers. Although the resolutions don't have much legal effect, they have huge symbolic and organizing value. Each time a resolution is placed on the agenda of a city council, it provides an opportunity to educate the public about the lengths to which the Bush administration has already gone, about the fundamental values that underlie our constitutional commitments, and about the importance of ordinary people standing up and being heard. While the campaign has not had much attention in the national press and has been largely ignored on television, local politicians and active members of both parties have become well aware of it. And the campaign has helped to create a vast network of citizens concerned about liberty and privacy and ready and willing to speak up in their defense.

The quiet success of the Bill of Rights Defense Committee's campaign may well explain the Bush administration's failure thus far to introduce most of what has been dubbed "Patriot II," a draft of which was leaked in February 2003. Among other things, that bill called for presumptively stripping US citizens of their citizenship if they were found to have supported a "terrorist organization." It would also have given the attorney general unreviewable power to deport any nonnationals—presumably including citizens shorn of their citizenship—who, in his opinion, threaten our "national defense, foreign policy, or economic interests."

The campaign of the Bill of Rights Defense Committee may also explain the national tour Ashcroft launched last summer to promote and defend the Patriot Act. When that act was passed six weeks after the September 11 attacks, the vote in the Senate was 98–1.[4] The attorney general doesn't need to waste his time defending a statute with that kind of support. But it has lost much of that support, thanks in large part to the Bill of Rights Defense Committee. Its campaign also likely had an effect in prompting virtually all of the Democratic presidential candidates to condemn the Patriot Act; John Kerry is probably the first presidential candidate from a major party who has run *against* an anti-terrorism law.

Efforts like those of the Bill of Rights Defense Committee underscore the realities of American politics. If there is any hope for Congress, the courts, or even, in another administration, the executive branch, to do something about preserving privacy in the post–September 11 era, ordinary people will have to be mobilized to express their concerns in public. At the same time, the erosion of personal privacy and the

erection by the government of walls of secrecy make public debate and resistance all the more difficult and risky. Dash and Rosen argue eloquently for the critical need to protect privacy if we are to preserve democracy. They disagree about the institutions most likely to provide those protections. But they agree that it is up to us to hold our government accountable to the values that gave it birth and justify its very existence.

Notes

[1] I represent both men as well as the Humanitarian Law Project, mentioned above.

[2] Elaine Scarry, "Resolving to Resist," *Boston Review*, February/March 2004.

[3] For details on the campaign, see the Bill of Rights Defense Committee's Web site, **www.bordc.org**, and the ACLU's report, "Independence Day 2003: Main Street America Fights the Federal Government's Insatiable Appetite for New Powers in the Post 9/11 Era," at www.aclu.org.

[4] Only Wisconsin Senator Russell Feingold voted against it.