1

Providing Security and Protecting Liberty

CLAYTON NORTHOUSE

On November 9, 2002, readers of the *New York Times* learned that Pentagon researchers planned to develop a massive virtual database, potentially containing data on every American, that could provide "instant access to information from Internet mail and calling records to credit card and banking transactions and travel documents."[1] Known as Total Information Awareness (TIA), the program originated in the Defense Department's Information Awareness Office, which was set up after September 11 to help develop predictive technologies that could aid the government in preventing future attacks. TIA planners hoped to exploit the vast amount of electronic information stored in commercial and governmental databases to find and track terrorists. Their goal was to develop analytical tools that would search through these mountains of data and generate an electronic profile of likely terrorists. Taken together, these tools and the databases to which they were applied could provide the government with an all-seeing eye on the world. In fact, TIA's logo was the all-seeing eye found on the U.S. dollar bill, and its motto was "scientia est potentia" (knowledge is power).

News of TIA unleashed a firestorm of protest, not only among left-leaning civil libertarians but also on the right. A few days after news of TIA broke, William Safire used his *Times* column to warn:

> Every purchase you make with a credit card, every magazine subscription you buy and medical prescription you fill, every Web site you visit and e-mail you send or receive, every academic grade you receive, every bank deposit you make, every trip you book and every event you attend—all these transactions and communications will go into what the Defense Department describes as "a virtual, centralized grand database."
>
> To this computerized dossier on your private life from commercial sources, add every piece of information the government has about you—passport application, driver's license and bridge toll records, judicial and divorce records, complaints from nosy neighbors to the F.B.I., your lifetime paper trail plus the hidden camera surveillance—and you have the supersnoop's dream: a "Total Information Awareness" about every American citizen.[2]

Other analysts came to TIA's defense, arguing that the new security challenges facing the United States demanded a new type of response. Since the end of the cold war, nonstate actors had replaced foreign governments as the major threats to U.S. national security. In order to track and defeat enemy combatants in decentralized networks spanning the globe, the intelligence community had to collect more data than ever before and draw links between seemingly innocuous bits of information. "It is the only way to protect ourselves," explained former CIA official John MacGaffin. "For the last forty years, there were a finite number of bad guys coming out of a finite number of places. Now we have an infinite number of threats from an infinite number of things."[3]

Tools such as Total Information Awareness, advocates maintained, were critical to this task. In addition, they argued, concerns about civil liberties could be addressed by ensuring that privacy safeguards were in place. A combination of judicial oversight and modern technologies, such as anonymity tools, could allow the government to fight the war on terror without infringing unduly on ordinary citizens' rights.

The public and Congress were not convinced. For many, TIA's Big Brother overtones were too difficult to ignore. And the fact that the Information Awareness Office was headed by retired rear admiral John M.

Poindexter, who was convicted of lying to Congress about the Iran-Contra affair, did little to allay their concerns. In May 2003 the Defense Department responded to TIA's critics by releasing a detailed report, as required by Congress, that pledged to make the protection of Americans' privacy and civil liberties a "central element" of the program. It also announced that henceforth TIA would be known as Terrorist Information Awareness rather than Total Information Awareness. But the critics were unappeased. Even Poindexter's resignation later that summer—following a new flap over plans to launch a terrorism futures trading market—failed to quell opposition to the programs he had helped create. In September 2003 Congress cut off funding for TIA and shut down the Information Awareness Office.

This case illustrates the controversy provoked by ambitious efforts to harness information technology to the cause of homeland defense. It also raises a number of questions that will remain vital long after this particular program's demise: What principles should guide us in negotiating the relationship between security and liberty in the aftermath of September 11? How does technology factor into this complex set of concerns? What benefits do techniques like data mining offer, and how should they be used? To what extent are we willing to give the government control over our personal information? Do current efforts to exploit information and information technology violate the principles embodied in the Fourth Amendment?

The contributors to this volume address these critical questions. In the next essay in this section, Alan Westin examines public opinion data to identify the broad contours of the current debate over security, liberty, and technology. In the second section, "Protecting Security and Liberty: Information Technology's Role," James Steinberg, Zoë Baird, James Barksdale, Gilman Louie, Gayle von Eckartsberg, and Bruce Berkowitz analyze the necessary restructuring of the intelligence community and the role that technology can play in combating terrorism. They also suggest how technology can be used to protect the homeland without necessarily threatening civil liberties. Finally, in the third section, "Technology, Security, and Liberty: The Legal Framework," Larry Thompson, Jerry Berman, Beryl Howell, Senator Jon Kyl, and Senator Russell Feingold focus on key legal issues at the intersection of liberty and security and continue the debate over the proper legal restrictions on the government's power to use information technologies for national security purposes.

Security and Liberty: The Fundamental Debate

American history is, to a great extent, a study of the tension between liberty and security. The Founders' desire to protect what they saw as inalienable rights, including liberty of thought, association, and speech and freedom from unwarranted government incursions into citizens' homes, is enshrined in the Bill of Rights. Yet over the more than two hundred years since the Constitution was ratified, these basic liberties have been compromised repeatedly during periods of national uncertainty.[4]

In 1798, with the nation prepared for war, President John Adams and the Federalists passed the Alien and Sedition Acts, which made any "false, scandalous, and malicious" statement against the United States government punishable by fine and imprisonment. In addition, they gave the president the exclusive authority to deport any foreigner considered to be a threat to national security. At a time of rising tensions with France, the Federalists argued that these measures were necessary to preserve order and protect the nation. But in practice, they were used primarily to muzzle the opposition Republican Party. Nearly all of the newspaper writers and editors arrested under the Alien and Sedition Acts were Republicans. The acts expired on the last day of Adams's presidency, and his successor, Thomas Jefferson, released and pardoned all those jailed as a result of this legislation. The Alien and Sedition Acts have since become a black mark in the history of free speech in America and the subject of condemnation by the Supreme Court.

Some sixty years later, in the midst of the Civil War, President Lincoln faced opposition to Union forces in Baltimore. When rioting broke out among Confederate sympathizers, resulting in the death of several Union soldiers, Lincoln suspended the writ of habeas corpus, which gives detained individuals the right to have their case heard before a judge, and declared the entire state of Maryland under martial law. Throughout the war, Lincoln suspended the writ of habeas corpus eight times, finally issuing a nationwide order. As a result, thousands of supposed Southern sympathizers, draft dodgers, and deserters were detained without access to a civilian court of law. After the end of the Civil War, the Supreme Court condemned these actions, ruling in *Ex Parte Milligan* that it was unconstitutional to detain a U.S. citizen under martial law without access to functioning civilian courts.[5]

The next major challenge to Americans' civil liberties came during World War I. With the Espionage Act of 1917 and the Sedition Act of

1918, the United States returned to many of the practices authorized under the Alien and Sedition Acts. In the first of what would become two Red Scares, thousands of individuals were arrested for speaking out against the war and for criticizing the United States government. At the time the Supreme Court upheld a number of decisions involving the detention of individuals who had opposed the war, but all of these decisions were subsequently overturned, and every individual arrested under the Espionage and Sedition Acts was eventually released.

Later, during World War II, widespread panic up and down the West Coast led to the internment of 120,000 people of Japanese descent. Under tremendous political pressure, President Roosevelt issued Executive Order 9066 ten weeks after the attack on Pearl Harbor. This order gave the Army the power to establish military zones from which certain individuals could be excluded. Ninety percent of Japanese Americans were uprooted from their communities, forced to leave their homes and businesses, and relocated to internment camps in which they remained for up to three years. In *Korematsu* v. *United States,* which was decided in 1944, the Supreme Court upheld this policy. Writing for the majority, Justice Hugo Black stated that "the power to protect must be commensurate with the threatened danger."[6] Since then, several presidents have apologized for the forced internment of the Japanese, and the Supreme Court has never relied on *Korematsu* as a precedent in deciding later cases.

Perhaps most famously, at the height of the cold war, the Red Scare of the 1950s involved the blacklisting of hundreds of supposed Communist sympathizers and the incarceration of Communist Party leaders. The House Un-American Activities Committee blacklisted hundreds of artists and writers, and under the Smith Act, members of the Communist Party were prosecuted for conspiring to overthrow the U.S. government. In *Dennis* v. *United States,* the Supreme Court affirmed the constitutionality of the Smith Act and upheld the conviction of Eugene Dennis and ten other Communist Party leaders, declaring their speech to pose a clear and present danger. In a strong dissenting opinion, Justice Black observed, "Public opinion being what it now is, few will protest the conviction of these Communist petitioners. There is hope, however, that in calmer times, when present passions and fears subside, this or some later Court will restore the First Amendment liberties to the high preferred place where they belong in a free society."[7] Eventually, the Court vindicated Black's hopes and brought the second Red Scare to an end by restricting

the scope of the Smith Act and prohibiting Congress from investigating people's political beliefs.

As these examples demonstrate, the issues raised by the sometimes conflicting demands of security and liberty are not new. But today the controversy surrounding the relationship between these two goals is heightened by the advent of powerful and, to some, frightening new technologies. Cameras can now record the geometric structure of a subject's face and instantly compare those measurements against data on suspected criminals. Giant databases can store information on every credit card transaction, medical record, bank account, and plane reservation. Analysts can perform clandestine searches of the data stored on individuals' computers and collect data transmitted over the Internet, including the addresses to which e-mail is sent and the websites that a user has visited. In some eyes these capabilities evoke the Orwellian nightmare of a paternalistic, omnipotent government that observes its citizens' every move.

How will the government respond to the civil liberties challenges that these new technologies raise? In large part the answer to this question lies in public beliefs about how the balance between security and liberty should be struck. As Learned Hand said, "Liberty lies in the hearts of men and women; when it dies there, no constitution, no law, no court can save it; no constitution, no law, no court can even do much to help it."[8] Accordingly, in the following essay, Alan Westin offers a detailed examination of the public's attitudes toward civil liberties and national security before and after September 11. Based on the results of five surveys conducted since the September 11 attacks, he finds that large majorities both support the government's expanded powers and remain concerned about safeguarding civil liberties. This attitude of "rational ambivalence," he concludes, should be seen as an opportunity to ensure that both support for antiterrorist programs and protections for civil liberties remain strong.

Protecting Security and Liberty: Information Technology's Role

The second section of *Protecting What Matters* focuses on the intelligence challenges posed by terrorism and the role that information technology can play in this new threat environment. During the cold war, as James Steinberg points out, the task facing the intelligence community was relatively straightforward: "We generally knew what to look for and where

to look for it." Moreover, most of the necessary information concerned military activities overseas, and the expertise needed to collect and analyze it resided in the federal government. Since September 11 all that has changed. In his essay Steinberg discusses how the intelligence community must adapt to meet future security challenges. He also identifies new technologies that can aid in this task, as well as tools that can promote accountability in the collection and use of sensitive personal information.

Zoë Baird and James Barksdale, cochairs of the Markle Task Force on National Security, focus on one of the most important aspects of the new intelligence challenge: the need to improve information sharing across different agencies and levels of government. Based on the task force's work, they outline six criteria that an effective Systemwide Homeland Analysis and Resource Exchange (SHARE) network must meet and analyze the proposed network's technological components. They also review recent policy developments—notably the executive orders issued by President Bush in August 2004 and the Intelligence Reform and Terrorism Prevention Act of 2004—that create a national framework for better information sharing and, ultimately, greater security.

Gilman Louie and Gayle von Eckartsberg also explore information technology's role in the post–September 11 world, but their emphasis is on tools that make it possible to protect civil liberties and the nation at the same time. For example, selective revelation and anonymizing technologies can limit violations of privacy while granting the government access to a great deal of useful information. The availability of such techniques, Louie and von Eckartsberg argue, makes security-versus-liberty a false choice.

Finally, Bruce Berkowitz looks beyond specific technologies to delineate the role of policies and procedures in creating a safe zone for collecting and sharing information while protecting civil liberties. "Since September 11," he writes, "the main approach to resolving these problems has been to 'lower the bar'—that is, reduce the barriers that preclude intelligence and law enforcement agencies from investigating individuals and sharing information." Instead, he argues, the government should "adopt measures that limit the potential damage of such investigations." By limiting the mandate of information collectors, controlling the use of information, and providing recourse for the subjects of mistaken investigations, the intelligence community can more effectively take advantage of technology's potential without unduly infringing upon individual rights.

Technology, Security, and Liberty: The Legal Framework

The essays in the final section of *Protecting What Matters* analyze the legal context for the current debate on technology, security, and liberty. Four overlapping areas of law are relevant to this discussion. First, the Fourth Amendment provides protection against unreasonable searches and seizures, whether physical or electronic. Title III of the Omnibus Crime Control and Safe Streets Act of 1968 builds on this foundation by setting forth the procedures the government must follow to obtain a warrant for electronic surveillance. Second, a weaker set of regulations controls governmental access to information voluntarily conveyed to third parties, such as checking account records or the telephone numbers of incoming and outgoing calls. Third, the Foreign Intelligence Surveillance Act of 1978 controls the government's use of electronic surveillance to collect foreign intelligence for national security purposes. Finally, a disjointed collection of privacy legislation governs the use of personal information in the public and private sectors. The remainder of this introduction provides a brief overview of these four areas of law as background for the more detailed analyses presented by the volume's contributors. It also discusses the changes introduced by the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act).

The Fourth Amendment and Title III

Much of the law guiding the debate over civil liberties and national security centers on the Fourth Amendment, which protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." In *Katz* v. *United States*, the Supreme Court extended this right to include protection against electronic intrusions.[9] As Justice Potter Stewart wrote for the majority,

> The Fourth Amendment protects people, not places. What a person knowingly expresses to the public, even in his own home or office, is not a subject of the Fourth Amendment protection. . . . But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected . . . once it is recognized that the Fourth Amendment protects people—and not simply "areas"—against unreasonable searches and seizures, it becomes clear that

> the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure.[10]

Justice Stewart also observed that "searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions."[11] Consequently, in order to meet the constitutional test, the procedures for authorizing electronic search warrants must be clearly established, and government wiretapping must receive prior approval from a judge.

In response to *Katz*, Congress enacted the Omnibus Crime Control and Safe Streets Act of 1968 (OCCSSA). Title III of OCCSSA prohibits warrantless wiretapping of electronic, telephone, and face-to-face conversations and establishes procedures regulating the use of wiretaps. For a limited set of criminal offenses, including murder, kidnapping, extortion, gambling, and drug sales, a judge or magistrate can authorize the Department of Justice (DOJ) to eavesdrop on conversations for up to thirty days. After this period the courts are bound to notify those whose conversations were monitored. To obtain authorization for a wiretap under Title III, the DOJ must, among other things, prove that there is probable cause to believe that the targeted person committed or is about to commit one of the criminal offenses.

In the decades since the enactment of OCCSSA, the government has faced the constant challenge of keeping up with the advance of technology. In 1994 Congress passed the Communications Assistance for Law Enforcement Act (CALEA) to ensure that new communications technologies would permit eavesdropping by law enforcement agencies. However, CALEA's reality has never lived up to its promise. In his essay Larry Thompson argues that this piece of legislation needs to be more vigorously enforced. Otherwise, he warns, "The government may simply not have the technological ability or the capacity to undertake timely electronic surveillance"—making concerns about potential tradeoffs between security and liberty moot.

Access to Third-Party Information

The Fourth Amendment and Title III do not apply to documents and information voluntarily conveyed to third parties. The Supreme Court established this principle in *United States* v. *Miller*, which dealt with

access to checks and other financial records held by a third party, such as a bank. The Court reasoned that there was no reasonable expectation of privacy in such a situation because the documents were "voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[12] Consequently, no matter how sensitive the data—be it medical records, educational records, financial records—the government is allowed to search and seize documents voluntarily given to third parties without fear of violating the Fourth Amendment (although privacy legislation may bar the government from doing so in specific cases). To obtain a court order authorizing access to such records, the government need only show reasonable grounds for believing that the targeted information is relevant and material to a criminal investigation—a far lower hurdle than the one established by Title III.

The standard of evidence is even lower when it comes to "contentless" data routinely held by third parties, such as the information collected by pen registers and trap-and-trace devices. These technologies are like caller IDs, recording the telephone numbers for incoming or outgoing calls on a given line. In *United States* v. *New York Telephone Company* (1977), the Supreme Court found that Title III does not cover the use of pen registers and trap-and-trace devices because the content of the conversations is not captured, only the phone numbers being used.[13] Two years later, in *Smith* v. *Maryland*, the Court ruled that the Fourth Amendment offers no protection against the government's use of these devices.[14] The Court argued that there was no reasonable expectation of privacy in such cases because it is common knowledge that telephone companies record these numbers in the normal course of business. (For example, the numbers dialed are printed on phone bills.) Consequently, the government can receive a court order for the use of these devices by simply making a sworn declaration that the sought-after information is relevant to a criminal investigation. The orders and the information received never have to be revealed to their targets.

Foreign Intelligence

An entirely different legal regime—the Foreign Intelligence Surveillance Act of 1978 (FISA)—governs domestic surveillance of foreign powers or agents of foreign powers. FISA created two secret courts: the Foreign Intelligence Surveillance Court and the Foreign Intelligence Surveillance Court of Review. In order to receive a secret warrant for the collection of

foreign intelligence information, the Department of Justice must demonstrate to the Foreign Intelligence Surveillance Court that there is "probable cause to believe that . . . the target of the electronic surveillance is a foreign power or an agent of a foreign power."[15]

Under FISA the bar for receiving a search warrant is set much lower than under Title III. For this reason, the legislation was carefully crafted to prevent prosecutors from using FISA to get around the more stringent requirements that apply to information gathering in ordinary criminal investigations.

Privacy Law

The final piece of the legal puzzle is an array of efforts to safeguard the privacy of personal information. The most prominent statute protecting privacy in the public sector is the Privacy Act of 1974, Congress's first attempt to control the federal government's collection, dissemination, and use of personal information. It applies to the use by all federal government agencies of "systems of records" or, in other words, any collection of records retrievable by an individual identifier, such as a name or Social Security number, that is under an agency's control.

The Privacy Act is based on four principles. First, federal agencies must give any American citizen or permanent resident access to any information stored about him or her. Second, agencies must follow "fair information practices" in handling and storing personal information. Among other things this means that the information collected must be accurate and necessary for an agency to fulfill its functions. Third, strict limits are set on an agency's ability to release individually identifiable information to other organizations or individuals. Finally, individuals can sue government agencies that fail to abide by these principles.

However, a number of limitations make the Privacy Act's protection of personal information less than complete. The term *agency* has been interpreted broadly in order to allow divisions within federal departments to share information. The Privacy Act also allows agencies to release data for "routine use," defined as a use that is compatible with the purposes for which the data were collected. The sharing of information for law enforcement purposes is exempt from the requirements of the act. And the Privacy Act does not apply to the government's use of data stored in the private sector, where only piecemeal legislation to protect privacy exists.

In his essay Jerry Berman highlights the lack of comprehensive legislation concerning the government's use of private sector data as a leading source of uncertainty for the public, the government, and the private sector. He also calls for the development of a new legal framework building on existing constitutional doctrine and fair information practices and argues that such rules "will not only protect civil liberties but will also enhance the effectiveness of government counterterrorism activities."

The PATRIOT Act

The PATRIOT Act of 2001 modified many of these areas of law. For example, sections 201 and 202 add terrorism, production or dissemination of chemical weapons, and computer crimes to the list of offenses that can be cited in requests to authorize wiretaps under Title III. Section 213 also gives the government the power to conduct a Title III search and seizure without contemporaneous notification of the target. If it is reasonable to think that the notification will have "an adverse effect," notice need not be given for a "reasonable" period of time. Such "sneak and peek" searches are not new. What makes section 213 controversial, though, is that "reasonable" is not defined. Moreover, under this provision, the government can seize, as well as search, property and communications without giving notice.

The PATRIOT Act also expanded government access to information held by third parties. Section 216 extends the regulations governing pen registers and trap-and-trace devices to allow the government to capture e-mail address and header information without notifying the target and without abiding by the strict principles of Title III. It also grants the government access to the URLs of the websites an individual has viewed. In addition, sections 216 and 220 permit nationwide orders for the interception of electronic communications. Previously, courts could only issue orders for the jurisdictions where they were located.

Perhaps most important, the PATRIOT Act loosened some of the legal restrictions that were designed to keep intelligence collection and domestic law enforcement distinct. Before the PATRIOT Act's passage, strict procedures governed the sharing of intelligence information with those responsible for criminal prosecutions. The criminal branch of the Department of Justice was prohibited from making recommendations for investigation and from directing or controlling intelligence-gathering activities. This separation of functions was reflected in FISA's requirement that "the

purpose" of surveillance must be to capture foreign intelligence. However, the PATRIOT Act changed this wording to "a significant purpose." This change in language has permitted greater coordination between the criminal and intelligence branches of the DOJ. Critics warn that this shift has opened the possibility for abuse of FISA warrants since the Department of Justice can now monitor U.S. citizens who are believed to be agents of foreign powers, even if criminal prosecution is the investigation's primary goal.[16] In her contribution to this volume, Beryl Howell addresses these issues by reviewing FISA's legislative history, including the amendments introduced by the PATRIOT Act, with a focus on the change in FISA's "purpose" restriction. She also examines some of the problems that may arise as a result of this change and proposes steps both to strengthen FISA and to enhance public confidence in the law.

Finally, the PATRIOT Act has extended the government's intelligence-gathering powers in several important ways. For example, section 206 permits roving wiretaps on the target of a FISA search. The government can monitor all communications coming to or from the target without specifying the particular technologies that will come under scrutiny. This means the government may monitor public means of communication, such as public phones and computer terminals in libraries, causing many people who are not associated with the target to come under surveillance.

Spurring controversy among librarians and booksellers, section 215 allows the government to issue orders to obtain business records by certifying before the Foreign Intelligence Surveillance Court that such records are relevant to a terrorism investigation or clandestine intelligence activity. Furthermore, without court approval or congressional oversight, section 505 gives the FBI the power to issue National Security Letters (NSLs). NSLs are used to require that Internet service providers and telephone companies release web history, e-mail, and telephone information relating to a particular person relevant to a terrorism investigation. The targets of NSLs and section 215 orders are prohibited from disclosing to any third party the receipt of an order or the seizure of records.

In the two chapters that conclude this book, Senators Jon Kyl and Russ Feingold debate the value and significance of the PATRIOT Act. Senator Kyl argues that this legislation provides the necessary means for overcoming previous intelligence failures, without endangering civil liberties. Senator Feingold, the only member of the Senate to vote against the PATRIOT Act, takes an opposing view, maintaining that the powers it grants the government are overly broad.

Domestic Spying

In late 2005 the *New York Times* revealed that in the months following September 11, 2001, President Bush secretly authorized the National Security Agency (NSA) to spy on Americans without a warrant or court order.[17] Since then the NSA has been monitoring international phone calls and intercepting international e-mails between United States citizens and people in certain Middle Eastern countries.[18]

Two basic positions have been taken on the program's legality. The Department of Justice argues that President Bush acted at the "zenith of his powers in authorizing the NSA activities."[19] The American Civil Liberties Union, on the other hand, argues that the NSA program "seriously violates the First and Fourth Amendments" and is "contrary to the limits imposed by Congress."[20]

One of the central issues in this complex legal debate is whether the NSA program is in violation of the Foreign Intelligence Surveillance Act. As noted by the ACLU, when Congress enacted FISA, it also amended Title III of the Omnibus Crime Control and Safe Streets Act to state that the procedures of Title III and FISA "shall be the exclusive means by which electronic surveillance . . . and the interception of domestic wire, oral, and electronic communications may be conducted."[21] Hence, the ACLU concludes, because the NSA is acting outside of Title III and FISA procedures, it is in violation of the law.

The Department of Justice counters that section 109 of FISA "expressly contemplates that the Executive Branch may conduct electronic surveillance outside FISA's express procedures if and when a subsequent statute authorizes such surveillance."[22] The Authorization for Use of Military Force (AUMF) passed by Congress a week after September 11, 2001, authorized the president to "use all necessary and appropriate force" against those who attacked the United States. The Department of Justice argues that this gives the president the express authority to protect the nation and that a necessary component of protecting the nation is collecting intelligence on those who attacked the United States. Hence, Justice argues, the NSA program is consistent with FISA.

Former Senate majority leader Tom Daschle writes that he is "confident that the 98 senators who voted in favor of [AUMF] did not believe that they were also voting for warrantless domestic surveillance."[23] The Congressional Research Service (CRS) makes the additional point that, "Even if AUMF is read to provide the statutory authorization necessary

to avoid criminal culpability under FISA, it does not necessarily follow that AUMF provides a substitute authority under FISA to satisfy the more specific language in Title III."[24] But CRS goes on to note that the legality of the NSA program is "impossible to determine without an understanding of the specific facts involved and the nature of the President's authorization, which are for the most part classified."[25]

These points will continue to be debated in Congress and before courts of law. In the process, the nation's laws and counterterrorism programs must adapt to the new environment created by the advancement of technology in the age of international terrorism. The chapters in this book sketch differing views on how these adjustments can take place as the government attempts to maximize the powers of information technologies to protect against terrorism while preserving civil liberties.[26]

Conclusion

How do we give the government the power to use technology for national security purposes while preserving our basic rights to privacy and freedom? New information technologies have the potential to be potent weapons in the war on terror. But if abused, they can also pose a significant threat to individual liberties. This challenge must be met head-on if the government is to succeed in its dual task of protecting liberty and providing security. The essays that follow do just that.

Notes

1. John Markoff, "Threats and Responses: Intelligence; Pentagon Plans a Computer System that Would Peek at Personal Data of Americans," *New York Times,* November 9, 2002, p. A12.

2. William Safire, "You Are a Suspect," *New York Times,* November 14, 2002, p. A35.

3. Siobhan Gorman, "Intelligence: Adm. Poindexter's Total Awareness," *National Journal,* May 8, 2004, p. 1430.

4. Geoffrey Stone, "Civil Liberties in Wartime," *Journal of Supreme Court History* 28, no. 3 (2003): 215–51; Geoffrey Stone, *Perilous Times: Free Speech in Wartime* (New York: W.W. Norton, 2004).

5. *Ex Parte Milligan*, 71 U.S. 2 (1866).

6. *Korematsu* v. *United States*, 323 U.S. 214 (1944).

7. *Dennis* v. *United States*, 341 U.S. 494, 580 (1951).

8. Learned Hand, *The Spirit of Liberty* (New York: Knopf, 1952), p. 190.

9. *Katz* v. *United States*, 389 U.S. 347 (1967). This decision rests in part on Justice Louis Brandeis's dissenting opinion in *Olmstead* v. *United States*, 277 U.S. 438 (1928).

10. *Katz* v. *United States*, 389 U.S 347, 351, 354 (1967).

11. Ibid., p. 357.

12. *United States* v. *Miller*, 425 U.S. 435 (1976).

13. *United States* v. *New York Telephone Company*, 434 U.S. 159 (1977).

14. *Smith* v. *Maryland*, 442 U.S. 735 (1979).

15. 50 U.S.C. 1801(e)(1).

16. As the Foreign Intelligence Surveillance Court of Review writes, "It can be argued . . . that by providing that an application is to be granted if the government has only a 'significant purpose' of gaining foreign intelligence information, the Patriot Act allows the government to have a primary objective of prosecuting an agent of a non-foreign intelligence crime." Ibid.

17. The story was first revealed by the *New York Times* in Jame Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers without Courts," *New York Times*, December 16, 2005, p. 1A.

18. The *New York Times* reports that the NSA program has been collecting large amounts of information (Eric Lichtblau and James Risen, "Spy Agencies Mined Vast Data Trove, Officials Report," *New York Times*, December 24, 2005, p. 1A), whereas the Bush administration claims that the program is narrow in scope.

19. U.S. Department of Justice, "Legal Authorities Supporting the Activities of the National Security Agency Described by the President," January 19, 2006, p. 2 (see www.fas.org/irp/nsa/doj011906.pdf).

20. Complaint for Declaratory and Injunctive Relief, *American Civil Liberties Union, et al.* v. *National Security Agency*. U.S. District Court, Eastern District of Michigan Southern Division, January 17, 2006.

21. 18 U.S.C. section 2511(2)(f).

22. Ibid., p. 20.

23. Tom Daschle, "Power We Didn't Grant," *Washington Post,* December 23, 2005, p. A21.

24. Elizabeth B. Bazan and Jennifer K. Elsea, "Memorandum: Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information," Congressional Research Service, January 5, 2006, p. 43.

25. Ibid., pp. 42–43.

26. The chapters in this volume, written after the revelation of the NSA program, do not directly address the domestic spying issue, except for the chapter by Alan Westin.