

Privacy in the Age of Terror

Terrorists live with us—and attack us—at home; use diffuse structural networks; and are less predictable than adversaries from the past. To combat this threat, the need for effective information and intelligence gathering and sharing at home is greater now than ever before. Advances in technology have improved immeasurably the government's capacity to collect and use information to secure the nation. Still, past U.S. domestic intelligence activities demonstrate the threat that those activities can pose for the civil liberties of Americans. It is possible to adapt to these new needs and to take advantage of greater capabilities without undermining civil liberties or the significant strides that the United States has made in privacy protection since the 1970s. Doing so, however, will require a new model to protect individual privacy—one that relies less on prohibiting the collection and dissemination of private information and more on effective oversight and control of government activity.

The New Threat

The threat of terrorism poses significant new information and intelligence challenges for the U.S. government. Our Cold War adversary, the Soviet Union, operated almost exclusively overseas. In contrast, terrorists live, visit, work, and study in the United States and attack from within the nation's borders, resulting in a greater need now to collect information at home. The Soviets used a military and intelligence apparatus about which we had deep knowledge. U.S. Cold War intelligence

Mary De Rosa is a senior fellow at CSIS. Previously, she served as special assistant to the president and legal adviser on the National Security Council staff and as special counsel at the Department of Defense.

Copyright © 2003 by The Center for Strategic and International Studies and the Massachusetts Institute of Technology
The Washington Quarterly • 26:3 pp. 27–41.

collection was highly focused, and analysts looked for well-defined behavior and warnings.

Terrorists are less organized and more geographically diffuse. Their numbers are small, and it is far more difficult to track their actions and to predict their plans. Information about terrorist activities is scattered; difficult to isolate; and must be plucked from countless sources, then combined, collated, and analyzed. With a greater need to share information within and among governments—and even with the private sector—hierarchical, stovepiped information structures and restrictions on information sharing are now less acceptable. At the same time, technological advances have given the government the capacity to accomplish these tasks far more effectively. New technology, for example, is improving immeasurably the government's ability to conduct surveillance using electronic and biometric tools, to use data-mining and pattern-recognition tools to sift through masses of data, and to share information on networks.

Privacy and U.S. History

These threats and technologies all have profound implications for privacy and civil liberties. Mistrust of a powerful government is part of the U.S. heritage. Largely because of this mistrust, Americans—more than the citizens of most other countries—resist giving their government access to private information. They fear that the government is more likely to abuse their rights if it has information about their activities.

These fears are not without foundation. Discussion of privacy and security in the United States is not complete without an understanding of the history of domestic intelligence activities in this country. From the late 1930s through the early 1970s, the U.S. intelligence community collected “vast amounts of information about the intimate details of citizens’ lives and about their participation in legal and peaceful activities.”¹ In an attempt to uncover Communist sympathizers at home, U.S. agencies such as J. Edgar Hoover’s Federal Bureau of Investigation (FBI), the Central Intelligence Agency (CIA), the National Security Agency (NSA), and U.S. Army intelligence conducted domestic intelligence activities that included open-ended surveillance and disruption of legitimate activities of civil rights and antiwar organizations.

The 1976 Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, chaired by Senator Frank Church (D-Idaho)—the Church Committee—discussed these activities in its report entitled *Intelligence Activities and the Rights of Americans*. Although close to three decades old, the report remains critical reading for policymakers con-

sidering increased domestic intelligence and information-collection activity. The report found that activities conducted in the name of national security often went far beyond what was relevant or necessary for that purpose. It concluded that significant weaknesses in the system of accountability and control within the intelligence community allowed pervasive abuses of the privacy and liberties of U.S. citizens.

Among the committee's findings were that the U.S. intelligence community opened hundreds of thousands of first-class letters and millions of telegrams and created dossiers on hundreds of thousands of U.S. citizens and domestic groups based largely on their participation in activities that involved criticism of the U.S. government or U.S. society. At one point, the FBI had catalogued at least 26,000 individuals on a list of persons to be rounded up in the event of a "national emergency."²

FBI surveillance activities included informant infiltration of civil rights groups and the Women's Liberation Movement; long-running investigations of organizations such as the National Association for the Advancement of Colored People, even though there was no indication of Communist ties or criminal acts; and investigations of political adversaries of every U.S. president from Franklin Roosevelt through Richard Nixon.³

Even more disturbing than the government's information-collection activities were the significant and long-running covert actions directed against U.S. citizens. The campaign to discredit Dr. Martin Luther King Jr. from 1963 until his death in 1968 is perhaps the most notorious of the FBI's excesses.⁴ The FBI's Counterintelligence Program—COINTELPRO—was designed to "disrupt" and "neutralize" groups deemed to be threats to national security.⁵ COINTELPRO used tactics such as initiating anonymous attacks on targets' political beliefs to induce their employers to fire them; mailing letters to targets' spouses in attempts to destroy their marriages; obtaining IRS data on targets and attempting to provoke IRS investigations; falsely and anonymously labeling targets as government informants to put them at risk of expulsion from their organizations or even physical violence; and using misinformation to disrupt demonstrations.⁶

The Church Committee also identified those government failings that contributed to the abuses it uncovered. It found control and accountability failures in oversight and supervision. Those responsible for overseeing and supervising domestic intelligence activity delegated broad authority without establishing guidelines and procedural checks, failed to monitor activities,

The lines between law enforcement and intelligence gathering have been blurred.

were at times willfully ignorant of improper or illegal activity, and even requested questionable practices. Internal agency oversight was inadequate. Investigations were overbroad, operated without standards, and dragged out long after any national security objective had expired. Information was often collected and disseminated to serve the political interests of a particular intelligence agency or administration or to influence social policy and political decisions, and information on individuals was disseminated too freely and retained past any point of relevance for national security purposes.⁷

The Current System for Privacy Protection

The system of privacy protection in the United States today developed largely in reaction to the Church Committee's revelations and other examinations of these domestic intelligence activities.⁸ The system has two types of protections: restrictions and prohibitions designed to keep private information out of the government's hands and oversight of executive branch activity. In general, the government and privacy advocates have emphasized the first category. Perhaps as a result, oversight has not developed as successfully as it should have. Yet, the restrictions and prohibitions are most threatened by new intelligence and information-collection measures designed to counter terrorism.

RESTRICTIONS AND PROHIBITIONS

Many reforms implemented immediately following the Church Committee's report, and most that have come since, were designed to erect barriers to government collection, sharing, and use of private information, particularly in the disciplines of law enforcement and intelligence. These changes were based on the philosophy that it is better for the government never to possess private information about its citizens and not to share or disseminate the information it does have. This approach avoids abuse by preventing even the potential for such abuse. Some of these restrictions, though, have been relaxed since September 11, 2001, to allow greater information collection and sharing in the hunt for terrorists.

In understanding these restrictions, it is first useful to delineate the differences between law enforcement and intelligence. These disciplines have different purposes, although they often use similar tools and techniques. Intelligence is collected for the prevention of, and warning about, national security threats and for informing policy decisions related to those threats. Domestic intelligence is collected at home about the citizens and residents of a country. The purpose of law enforcement is to capture and prosecute

criminals. It is primarily reactive, and a significant concern in information collection for law enforcement is its suitability for use in court.

The first significant restriction designed to protect against privacy abuse in the wake of the Church Committee revelations was the limitation of the number of intelligence agencies permitted to collect information on U.S. persons. The purpose of this restriction was to increase control over domestic intelligence collection. Executive Order 12333, issued in December 1981, and agency regulations prohibit foreign-intelligence agencies, including the CIA, NSA, and intelligence agencies within the Department of Defense (DOD) from collecting intelligence on U.S. residents or, in most cases, on U.S. soil. The National Security Act of 1947 also prohibits the CIA from engaging in any “internal security function.”

After these reforms, the FBI became the primary agency with a domestic intelligence mission. The FBI maintained this mission because its domestic law enforcement responsibility ensures that it has some institutional experience with the constitutional protections afforded U.S. persons, which is not true of the foreign-intelligence agencies. In addition, the FBI reports to the attorney general, who is responsible for upholding constitutional protections for U.S. persons.

The FBI, then, is responsible for collecting information on U.S. persons both for purposes of intelligence and law enforcement. The FBI has no legislative charter for the conduct of its activities but, since the mid-1970s, has been subject to a second, significant set of restrictions in the Attorney General Guidelines for FBI Activities. Attorney General Edward H. Levi issued these guidelines in 1976, and successor attorneys general have revised them. The guidelines were designed in part to prevent the FBI from engaging in open-ended surveillance and information collection on individuals absent an allegation of criminal activity. Until their revision in May 2002 in response to the September 11 attacks, the Attorney General Guidelines prevented the FBI from searching even publicly available information, including newspapers, Internet sites, and commercial databases, and from visiting public places or attending public events to conduct surveillance if there was no indication of a crime.⁹

Some of the most serious abuses that the Church Committee uncovered involved electronic surveillance of U.S. citizens for intelligence, rather than law enforcement, purposes. Electronic surveillance such as wiretaps on telephones or microphones planted in living quarters can be extremely intrusive on individual privacy. Prior to the Church Committee’s revelations, statu-

The government is increasingly interested in using private-sector data.

tory restrictions existed on electronic surveillance conducted for law enforcement purposes,¹⁰ but no statute imposed a framework for electronic surveillance for intelligence or national security purposes. In 1978, Congress passed the Foreign Intelligence Surveillance Act (FISA) to set limits on the conduct of electronic surveillance for foreign intelligence purposes. FISA required the government to obtain a court order from a special Foreign Intelligence Surveillance Court (FISC) before conducting electronic surveillance on a U.S. person. The FISC conducts its proceedings secretly, and FISA targets are never made aware of the surveillance.

It is not fair to rely on Congress for systemic oversight of executive branch activities.

Until recently, use of FISA surveillance in law enforcement investigations has been restricted significantly. The standard for a FISA warrant is less rigorous than the standards that apply to surveillance for purposes of law enforcement. For a law enforcement wiretap, a judge must find probable cause that a specific crime is being or will be committed and that the wiretap will obtain communications about that crime. For a FISA wiretap on a U.S. person, the government

must show probable cause only that the target is, or is an agent of, a foreign power. Therefore, as long as the nexus to a foreign power exists, a FISA warrant is easier to obtain. The difference in standards reflects a different constitutional treatment of law enforcement and foreign intelligence surveillance; courts have allowed greater flexibility when searches are for national security and the targets are foreign powers or their agents.¹¹ The restriction on use of FISA for law enforcement was designed to ensure that prosecutors and criminal investigators did not use the less rigorous FISA procedures to circumvent constitutional warrant requirements in criminal cases. Recent changes to FISA and Department of Justice (DOJ) procedures, discussed below, lowered this barrier to allow the use of FISA for law enforcement purposes.

In addition to these restrictions on the collection and sharing of private information by intelligence agencies, the government adopted some general restrictions on its ability to maintain and use private information. The Privacy Act of 1974, for example, sought to regulate how the government can maintain and use private information about individuals. The act generally restricts agencies' ability to collect and maintain private records and to share those records within or outside government. Because of the Privacy Act's exceptions, however, it does little to restrict collection or sharing for purposes of intelligence or law enforcement investigations.

Since September 11, 2001, a number of changes to government information and intelligence practices have been implemented or proposed. These changes demonstrate how efforts to address the terrorist threat are straining the restrictions that are the backbone of the current system of privacy protection in the United States. The changes include:

- *Expansion of domestic intelligence beyond the FBI.* The new Terrorist Threat Integration Center (TTIC) is an intelligence fusion center where all intelligence related to terrorist threats—both foreign and domestic—will be gathered and analyzed in one place. TTIC, for now, is housed in the CIA complex and staffed by CIA and FBI personnel, and it reports to the director of central intelligence. Thus, the CIA now has a greater role in fusion and analysis, although not collection, of domestic intelligence. In addition, the Department of Homeland Security's Directorate for Information Analysis and Infrastructure Protection has the responsibility to access, receive, analyze, and integrate domestic law enforcement and intelligence information,¹² although precisely what role that office will play in domestic intelligence activities is not yet clear. Others have advocated an additional step: that the government establish an agency separate from the FBI to be responsible for collecting and analyzing domestic intelligence. Senator John Edwards (D-NC) has introduced legislation to create a domestic intelligence agency, similar to the United Kingdom's Security Service (MI-5),¹³ and several influential voices in the national security community support the idea.¹⁴
- *Attorney General Ashcroft's May 2002 revisions to the Attorney General Guidelines.* John Ashcroft's revisions to the Attorney General Guidelines for General Crimes permit the FBI to collect public information about U.S. residents and conduct surveillance in public places absent a link to suspected criminal activity.¹⁵
- *Changes in FISA-approval practices.* The USA PATRIOT Act, passed in the immediate aftermath of the September 11 attacks, and subsequent changes made by DOJ to practices for approval of electronic surveillance under FISA, allow greater use of the less rigorous FISA procedures in criminal investigations. These changes have blurred the lines between law enforcement and intelligence gathering in seeking warrants for electronic surveillance.
- *Government mining of third-party private transactional data.* The government is increasingly interested in using private-sector data about individuals' commercial transactions to track terrorists or find clues to their

plans. Programs such as the Transportation Security Agency's CAPPs II project—designed to profile prospective airline passengers using commercial databases—and DOD's research on Total Information Awareness (TIA), which looks at the potential for finding patterns of terrorist activity in transactional data, are just two examples. Ashcroft's guidelines revisions also permit the FBI to mine commercial databases without an allegation of criminal activity.

Because each of these changes would allow the government greater or less-constrained access to private data, each walks back—at least in spirit—one or more of the specific restrictions adopted in the aftermath of the Church Committee's report.

OVERSIGHT

The other area of privacy protection reform pursued after the mid-1970s was oversight of government collection and use of private information. A number of players are responsible for overseeing executive branch activities, including the collection and use of private information. Congress is responsible not only for guiding or restraining executive branch behavior by passing legislation, but also for monitoring executive branch implementation of the laws. This oversight is necessary for Congress to carry out its constitutional duty effectively. Within the executive branch, agency inspectors general and other officers such as the general counsel or privacy and civil rights officers are responsible for overseeing program actions, including adherence to laws and guidelines on the use of private information.

There have been significant strides in the area of oversight since 1976. In Congress, both houses established select committees to oversee intelligence activities. In the executive branch, the role of the inspectors general has been strengthened. General counsels at the CIA, FBI, DOD, and NSA are more involved in operations and play a far more significant role in assessing the legality and propriety of information-collection activities. In general, overseers in both branches have greater access to information than was the case before the mid-1970s.

Overall, although the actors are in place, the existing system of oversight has not adequately undertaken the task of ongoing, systemic review of the soundness and effectiveness of privacy protections. The Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence were created in the mid-1970s to oversee U.S. intelligence activities. Neither committee, nor any other in Congress, however, currently conducts effective ongoing oversight of agencies' practices that affect the privacy and civil liberties of U.S. citizens. Instead, when it comes to these

and other issues, congressional oversight is sporadic and, more often than not, reactive. Its focus is after-the-fact investigation. These investigations too often become politicized and interested more in finding individual culprits than in assessing a system's strengths and weaknesses.

Because it has failed to conduct periodic reviews of programs, Congress has come to rely—to a fault—on “whistle-blowers” to provide information about system failures. Whistle-blowers—usually people within an agency who come forward to criticize that agency—often act out of a true sense of loyalty and commitment to good government and can be extremely important resources. Yet, other motives, such as a desire for the limelight or personal bitterness at perceived mistreatment, can sometimes be just as strong. Also, whistle-blowers are not always those most familiar with the programs and practices they criticize. Once they come forward, however, these individuals are treated as heroes; their motives or conclusions are often difficult to question without appearing to be a bully or an apologist for the target agency. The result is often a less than fully informed inquiry and scandal-driven policies that do not effectively or completely address the causes of a problem.

Continuing to rely primarily on restrictions and prohibitions cannot be the answer.

Although Congress should clearly do better, it is not fair to rely on Congress for systemic oversight of executive branch activities. Congress is necessarily removed from management of the agencies it oversees and must rely on the executive branch for information about agencies' programs and practices. Despite some progress in increasing openness since the 1970s, the executive branch can still be quite secretive. Indeed, there are sometimes constitutional reasons, such as the preservation of the separation of powers, why there is less than full flow of information from the executive branch to Congress.

The primary responsibility, then, for effective systemic oversight lies with the executive branch, and it has failed as well. Despite some improvements since the 1970s, executive branch oversight suffers from failings similar to congressional oversight. The Inspector General Act of 1978 established inspectors general in most executive branch agencies and set forth their duties and authorities. Although energetic, inspectors general are too often reactive; driven by scandal; and insufficiently focused on the need for periodic review, clear guidelines, and training. In short, agency oversight does not focus sufficiently on ensuring the soundness of a program or on stopping problems before they happen.

The absence of truly healthy oversight means that privacy advocates and, to some degree, the U.S. public lack confidence that government abuse will be prevented, detected, or stopped, except sporadically. This lack of faith has contributed to the overreliance on restrictions and prohibitions on government access to private information.

What can be done to improve this system of privacy protection? Continuing to rely primarily on restrictions and prohibitions cannot be the answer. New measures that involve increased governmental use of private information should not be prohibited automatically, nor should they be constrained so that they are significantly less effective than they could be. On the other hand, the U.S. public cannot be expected simply to trust its government not to fall back into old patterns of abuse.

A New Framework: Balancing Rights and the New Reality

The answer, then, is to revise the framework for privacy protection, taking into account both new threats and new technological capabilities. Today's system of privacy protection must rely less on prohibiting the collection and sharing of information and more on oversight and control of government activity—those aspects that have, until now, been permitted to languish. A new framework should encompass the following:

EMPHASIZE SYSTEMIC OVERSIGHT

Reorienting oversight to become more integrated into operations and more focused on ensuring the overall health of the system rather than after-the-fact investigation is the single most important principle for a new approach to privacy protection. Those collecting and working with private information must understand what is permitted and what is not, and the collection and use of private information should be controlled and not permitted to run offtrack. The government should:

1. *Implement clear guidelines for operation.* The first requirement for improving effective systemic oversight is that employees know what information they are or are not permitted to collect and for what reasons, how they can collect it, and how long they should retain it. Although guidelines can constrain agency activity, if they are clear and consistent, they also empower agency employees. Fear of crossing an unknown line can cause timidity, but if the lines are clear, employees will be more likely to take appropriate action. If national security agencies must be permitted greater access to private information to detect terrorist planning and activity within U.S.

borders, clearer standards and guidelines for handling such information are critical.¹⁶ Specifically, guidelines must address:

- *Relevance.* Employees must have guidance to determine the purposes for which they may collect and use private information. The information collected should relate in some clear way to the purpose for collection—in this case preventing, responding to, or punishing terrorist activity. This guidance is important to avoid fishing expeditions. Under no circumstances should access to private information be permitted for political purposes.
- *Dissemination.* Information collected for just one purpose—preventing terrorism—should not be disseminated for any other purpose.
- *Retention.* Guidelines should address how to determine when information is no longer relevant and how that information should be handled when that time comes.
- *Reliability.* Guidelines should include directions on how to assess the accuracy of information and how to correct inaccurate information.

Technology can be used to jeopardize privacy, but it can also protect privacy.

2. *Commit to training.* Even where guidelines currently exist, adequate training in their application is the exception. The government must commit to training agents to collect, use, disseminate, and retain personal data appropriately. This instruction should be an integral part of training for the operational mission and should be repeated and updated regularly.

3. *Integrate oversight into operations.* Guidelines, although crucial, cannot address every situation that will arise; indeed, they should not. The system should allow workers flexibility. Therefore, it is important that decisions are made with as much guidance as possible. To become truly effective at stopping problems before they begin, agencies should make efforts to integrate some oversight personnel into the day-to-day decisionmaking in sensitive operations. Although this effort can make overseers less detached and independent, it is invaluable if the purpose of oversight is to prevent, rather than merely punish, abuse. Overseers located on-site can identify problems as they arise, answer questions about the appropriate application of guidelines, and refer to others any issues or problems that cannot be resolved immediately.

The CIA has effectively integrated personnel from its general counsel's office into its operations by locating them on-site at many operational centers, such as the counterterrorism center. At the new Department of Homeland Security, the FBI, the TTIC, or a new domestic intelligence agency (if one is created), the general counsel or the inspector general could also have representatives located with the employees most likely to work with private information. These individuals would help by answering questions as they arise and ensuring that problems do not get out of control before being discovered.

4. *Conduct periodic reviews.* Systemic oversight should also include regular reviews of operations, investigations, practices, and standards involving collection or use of private data. These reviews can evaluate whether programs

are functioning as intended, whether they still serve the purpose for which they were initiated, whether programs have veered off course in any way, and whether they should be revised or ended. Without reviews, operations and investigations can assume lives of their own, continuing beyond the point where anyone can articulate their usefulness.

A helpful model for periodic review (although not on the subject of government use of private information) is the National Security Council's annual review of covert action programs, instituted after the Iran-contra revelations. This review looks at each existing program to determine how well it works and whether it should be expanded or discontinued. Similar regular reviews of agency practices for use of private information would be an effective way to assure that these practices stay on track.

To protect privacy in an age of terrorism will require a new model for privacy protection.

ity Council's annual review of covert action programs, instituted after the Iran-contra revelations. This review looks at each existing program to determine how well it works and whether it should be expanded or discontinued. Similar regular reviews of agency practices for use of private information would be an effective way to assure that these practices stay on track.

MAKE TECHNOLOGY WORK FOR PRIVACY

Technology can be used to jeopardize privacy, but it can also protect privacy; the government should make every effort to explore these positive uses and employ them whenever private information is stored in databases. For example, the government should always ask whether the information that identifies individuals (names, addresses, and so forth) in a set of data is necessary for the task in question. When the information is not required, methods should be found to remove identifying information before the data are accessed. Filters can remove data not relevant to potential terrorist activities before agency employees are permitted to access and analyze data. When it is necessary to have identifying information in a database, that da-

tabase should be separated from others, and access to it should be more tightly controlled.

Technology can also be useful in limiting access to data and in ensuring the accountability of personnel who have access. Special access requirements can be established for databases containing private information, and reliable methods of user authentication should be explored and used. Audit trails of access to the database can help detect when information has been accessed inappropriately; they will deter abuse and can assist in holding personnel accountable when abuses do occur. These procedures are only examples of the kinds of technological protections that the government should investigate and employ. The government should explore these and others and, in general, be as energetic in its research of the use of technology to protect privacy as it is in exploring its use for increasing security.

INCREASE PERIODIC CONGRESSIONAL OVERSIGHT OF PRIVACY PROTECTIONS

Congress does not—and should not—manage executive branch programs and practices. Its oversight role is limited but important. Congress serves as the last layer of oversight for executive branch agencies to catch those problems that the executive branch has overlooked or refuses to correct. Because it is a more political branch, Congress is more inclined than the executive branch to keep the public informed. Openness is essential to a healthy oversight system, and responsible congressional reviews can contribute a great deal by shedding light on government operations.

Congress's record in recent decades for conducting thorough reviews of an agency's practices, rather than of particular breakdowns, has not been good. Periodic reviews will not have the profile of investigations focusing on specific failures, but because they are not about a single incident, they are more likely to produce rational and well-rounded solutions. Conducting these reviews requires responsibility and a long-term commitment, however, because there will seldom be a clear, immediate political payoff.

INCREASE TRANSPARENCY ABOUT GUIDELINES AND PRACTICES

As the Church Committee stated, "Abuse thrives on secrecy. ... Knowledge is the key to control."¹⁷ Not only must managers and overseers in the executive and legislative branches be fully informed, but the public also must have a fair and accurate idea of what the government is doing with the private information it collects. Particularly in the sensitive intelligence area, every natural instinct of the executive branch is to keep information secret. Regarding operational or investigation details, secrecy is certainly essential. The same is not always true, however, for the development of guidelines or

for changes to policies and practices that involve the collection and use of private information. To enhance legitimacy and strengthen acceptance of the end product, these guidelines, policies, and practices should be developed in close consultation with Congress and, to the maximum extent possible, with public involvement.

Open discussion of guidelines, policies, and practices that brings to light their potential benefits to security, the real costs to privacy, and possible alternatives will contribute to a sensible balance between security and privacy. Although privacy and security do not always conflict, at times they will. The executive branch's openness with Congress and, when possible, the public about proposed reforms can help minimize fear and suspicion that incomplete information about private-information collection creates.

Defending Privacy and Security

Public concern is growing that, in adapting to new security threats, the U.S. government is wiping out the web of privacy protections adopted since the mid-1970s, and soon nothing will remain to prevent government abuse. The debate over these issues tends to portray privacy and security as inevitably at odds. This argument is false and dangerous. What is true is that some new intelligence measures conflict with many existing mechanisms for protecting privacy. The solution to this problem is neither to reject new security measures nor to accept diminished privacy protection. To protect privacy in an age of terrorism will require a new model for privacy protection. Americans must remember the lessons of past government abuse but adapt those lessons to a new environment.

Notes

1. Select Committee to Study Governmental Operations with Respect to Intelligence Activities, United States Senate, *Intelligence Activities and the Rights of Americans*, bk. 2 (Washington, D.C.: 1976), p. 7 (final report, issued April 26, 1976) (hereinafter Church Committee Report).
2. *Ibid.*, pp. 6–7.
3. *Ibid.*, pp. 6–10.
4. *Ibid.*, pp. 11–12.
5. *Ibid.*, p. 10.
6. *Ibid.*
7. *Ibid.*, pp. 138, 165, 225, 253, 265–266.
8. See, e.g., *Report to the President by the Commission on CIA Activities within the United States* (June 1975) (report of the Rockefeller Commission).
9. Office of the Attorney General, *The Attorney General's Guidelines on General Crimes*,

- Racketeering Enterprise and Domestic Security/Terrorism Investigations*, www.usdoj.gov/ag/readingroom/generalcrimea.htm (accessed April 13, 2003).
10. Title III of the Omnibus Crime Control and Safe Streets Act of 1968.
 11. Jeffrey H. Smith and Elizabeth L. Howe, "Federal Legal Constraints on Electronic Surveillance," in *Protecting America's Freedom in the Information Age: A Report of the Markle Foundation Task Force* (October 2002), p. 137, www.markletaskforce.org/documents/Markle_Full_Report.pdf (accessed April 13, 2003).
 12. *Homeland Security Act of 2002*, Public Law 296, 107th Cong., 2d sess. (November 25, 2002).
 13. *Foreign Intelligence Collection Improvement Act of 2003*, 108th Cong., 1st sess., S. 410 (introduced February 13, 2003).
 14. See, e.g., *Fourth Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction* (December 15, 2002), www.rand.org/nsrd/terrpanel/terror4.pdf (accessed April 13, 2003) (report of the Gilmore Commission).
 15. Office of the Attorney General, *The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Domestic Security/Terrorism Investigations* (revised May 2002).
 16. For an excellent discussion of the use of guidelines to balance privacy and security, see *Protecting America's Freedom in the Information Age: A Report of the Markle Foundation Task Force* (October 2002), pp. 32–34, www.markletaskforce.org/documents/Markle_Full_Report.pdf (accessed April 13, 2003). The report contains detailed suggestions for guidelines for agency collection and use of private information.
 17. Church Committee Report, p. 292.

