Order Code RS21915
August 19, 2004

Privacy: Key Recommendations of the 9/11 Commission

Gina Marie Stevens
Legislative Attorney
American Law Division

Harold C. Relyea
Specialist in American National Government
Government and Finance Division

Summary

Several of the recommendations made to protect against and prepare for terrorist attacks in the final report of the National Commission on Terrorist Attacks Upon the United States (9/11 Commission) focus on the protection of civil liberties. This report examines these recommendations, and those of other recent commissions. It will not be updated.

Some of the civil liberties questions raised in response to anti- terrorism efforts stem from the conflict between individual privacy interests and the intelligence needs of law enforcement and national security.[1] Programs and initiatives such as Terrorism Information Awareness (TIA),[2] the Computer Assisted Passenger Prescreening System (CAPPS II),[3] MATRIX,[4] and the United States Visitor and Immigrant Status Indicator Technology program (US-VISIT)[5] integrate advanced information technologies for the purpose of terrorist identification and prevention of terrorist attacks. These programs necessarily require enhanced information sharing by government agencies and the private sector, and are designed to assist the information needs of intelligence and national

[1] See *Terrorism and Civil Liberties* in the CRS Terrorism Electronic Briefing Book.

[2] CRS Report RL31730, *Privacy: Total Information Awareness Programs and Related Information Access, Collection, and Protection Laws*, by Gina Marie Stevens.

[3] CRS Report RL32366, *Terrorist Identification, Screening, and Tracking Under Homeland Security Presidential Directive 6*, by William J. Krouse.

[4] CRS CDM, *The Multi-State Anti-Terrorism Information Exchange (MATRIX) Pilot Project*.

[5] CRS Report RL32234, *U.S. Visitor and Immigrant Status Indicator Technology Program (US-VISIT)*, by Lisa M. Seghetti and Stephen R. Vina.

security. These programs operate in the context of a body of law relating to Federal government access to information. A recent survey of laws relating to Federal government access to information appears in RL31730, *Privacy: Total Information Awareness Programs and Related Information Access, Collection, and Protection Laws*.

The National Commission on Terrorist Attacks Upon the United States (9/11 Commission) recognized that information sharing is essential to combat terrorism.[6] While the benefits from the use of advanced technologies for antiterrorism efforts are clear, the risks to individual privacy and the potential for abuse and harm to individual liberty by Government officials and employees deploying such technologies are equally established. Civil libertarians, privacy advocates, and others worry that the Government's increased capability to assemble information will result in increased and unchecked government power.

The 9/11 Commission recognized that "Many of our recommendations call for the government to increase its presence in our lives — for example, by creating standards for the issuance of forms of identification, by better securing our borders, by sharing information gathered by many different agencies."[7] The Commission recommended consideration of privacy concerns in the formulation of presidential information sharing guidelines, a full and informed debate on expiring USA PATRIOT Act authority, and entrusting an entity with the responsibility to ensure that civil liberties concerns are appropriately considered across the government.[8]

The sixth public hearing of the 9/11 Commission focused on "Security and Liberty," and its second witness panel addressed "Protecting Privacy, Preventing Terrorism." The first witness, Judith A. Miller, former DOD General Counsel and member of the Markle Task Force on National Security in the Information Age,[9] addressed the benefits that advanced technological tools — such as data aggregation or integration, data analysis or data mining, and pattern-based analysis — can bring to the fight against terrorism, the risks to individual privacy from their use, and the development of policy to address these issues.[10] She recommended a systematic approach in developing new protections for privacy because of potential privacy abuses and harms when advanced technological tools are used to access private data. With respect to the development of new protections for

---

[6] The National Commission on Terrorist Attacks Upon the United States (known as the 9/11 Commission) was established by Title VI of P.L. 107-306, 107th Cong., 2nd Sess., November 27, 2002. It made its report public on July 22, 2004.

[7] U.S. National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (Washington: GPO, 2004), pp. 393-394.

[8] CRS Report RL32186, *USA Patriot Act Sunset: Provisions That Expire on December 31, 2005*, by Charles Doyle.

[9] The John and Mary R. Markle Foundation was established in 1927 "to promote the advancement and diffusion of knowledge ... and the general good of mankind." In 1998 the Foundation focused its efforts on addressing critical public needs in the information age. As part of its national security program, the Foundation has examined how best to mobilize information and information technology to improve national security while protecting civil liberties. See [http://www.markle.org].

[10] Available at [http://www.9-11commission.gov/hearings/hearing6/witness_miller.htm].

privacy, the Commission was referred to the reports of the Markle Foundation Task Force on National Security in the Information Age, and one of its principal recommendations — that the government implement guidelines for the use of private data, particularly with new technological tools. In addition, it was suggested that the guidelines include reinvigorated executive branch oversight to ensure that these guidelines are understood and followed, rigorous training on the guidelines for employees who use private data; and regular audit and review procedures to see that the guidelines are followed. The guidelines should also encourage the use of technological tools to protect privacy, such as technology that anonymizes data; control access to databases; and facilitate audits of database use. The second witness was Stewart A. Baker, partner and head of the Technology Department of Steptoe & Johnson, former General Counsel, National Security Agency and a member of the Markle Task Force on National Security in the Information Age.[11] The final witness was Marc Rotenberg of the Electronic Privacy Information Center.[12]

In the aftermath of September 11, 2001, several major commissions and task forces addressed information sharing and privacy safeguards. The Markle Foundation issued a report on *Protecting America's Freedom in the Information Age* in October 2002; the Joint Inquiry by the House and Senate Select Committees on Intelligence issued a final report on *Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001* in December 2002; the Markle Foundation issued its second report *Creating A Trusted information Network for Homeland Security* in December 2003; the DOD Technology and Privacy Advisory Committee (TAPAC) issued its report *Safeguarding Privacy in the Fight Against Terrorism* in March 2004; and the 9/11 Commission issued its final report July 22, 2004. Their key privacy-related recommendations are summarized:

Key 9/11 Commission Recommendations

- When determining the guidelines for information sharing among government agencies and the private sector, the President should safeguard the privacy of individuals about whom information is shared.

- The burden of proof for retaining a particular governmental power should be on the executive, to explain (1) that the power actually materially enhances security and (2) that there is adequate supervision of the executive's use of the powers to ensure protection of civil liberties. If the power is granted, there must be adequate guidelines and oversight to properly confine its use.

- At this time of increased and consolidated government authority, there should be a board within the executive branch to oversee adherence to

---

[11] Available at [http://www.9-11commission.gov/hearings/hearing6/witness_baker.pdf].

[12] Available at [http://www.9-11commission.gov/hearings/hearing6/witness_rotenberg.pdf].

the guidelines recommended and the commitment the government makes to defend civil liberties.[13]

Key Markle Foundation Task Force Recommendations

- Guidelines must be set by the President regarding personal information collection, analysis, and availability, which, among other considerations, will enable managers to embed respect for privacy and civil liberties into the core definition of analysis itself.

- Guidelines for database access and use should be prescribed, offering a framework and procedures to allow such information to be effectively used, analyzed, and disseminated, while also ensuring that information about people in the United States is used in a responsible fashion that respects responsible claims to individual privacy.

- The duties of the Department of Homeland Security Privacy Officer and Office of Civil Rights and Civil Liberties need to be clarified by combining the two offices into one well funded and staffed civil liberties and privacy office, with well spelled out referral criteria for the department's Inspector General.[14]

- The President should issue an executive order which, among other considerations, creates within the Terrorist Threat Integration Center (TTIC) appropriate institutional mechanisms to safeguard privacy and other civil liberties.

- Congress should undertake a review of the performance of federal agencies in improving analysis and information sharing as prescribed by the commission, and in utilizing private sector information while protecting civil liberties.

- Guidelines covering how information is collected, used, and shared among the relevant actors are critical for several different, but complementary, reasons, including a robust sharing of information only being pursued consistent with civil liberties interests.

- The President needs to set forth, in an executive order, guidelines that establish the principles for using the recommended information network to improve information collection, analysis, and sharing, while protecting civil liberties.

- The executive branch should create within the TTIC the appropriate institutional mechanisms to safeguard privacy rights.

---

[13] Op. cit., *The 9/11 Commission Report*, pp. 394-395.

[14] Markle Foundation, Task Force on National Security in the Information Age, *Protecting America's Freedom in the Information Age* (New York: October 2002), pp. 31, 32, 35.

- The government should establish guidelines to regulate access to, use, and sharing of private sector data among agencies, which would help the government to ensure that information is used in ways that are consistent with core national values, including privacy, other civil liberties, and the functioning of an accountable democratic political system.

- Rules governing access to and use of private sector data should be based primarily on two dominant considerations: the value of the information to the government, and the sensitivity of the information from the perspective of individual privacy and other civil liberties.

- It is strongly preferred that private sector data be kept in the private sector whenever possible rather than having the government retain it.

- In areas where the government has a compelling need to retain private sector information, a solution might be to create trusted data banks within the government with strict limitations on who has access to the underlying data and for what specific purpose.

- Another way to help limit the government retention of private sector data to that which is essential to the mission would be to require formal, written justifications for the creation and retention of data sets that contain personally identifiable information.

- The recommended guidelines must also address the question of how to assure compliance with the required policies and procedures and foster accountability, and some agency — the Department of Homeland Security is recommended — must have overall supervisory responsibility to oversee the application of the guidelines.

- Oversight of government use of private sector information should ensure the accuracy of the data that is brought into the information network, because accuracy is vital not only to protect the privacy and civil liberties of individuals who can be harmed by the use of inaccurate data, but also to assure that information has real value to the counterterrorism effort.[15]

Key Gilmore Commission Recommendation

- The President should establish an independent, bipartisan civil liberties oversight board to provide advice on any change to statutory or regulatory authority or implementing procedures for combating terrorism that has or may have civil liberties implications (even from unintended consequences).[16]

---

[15] Markle Foundation, Task Force on National Security in the Information Age, *Creating a Trusted Network for Homeland Security* (New York: n.d.), pp. 9, 10, 12, 18, 19, 32, 33, 34-35, 36.

[16] U.S. Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving (continued...)

Key TAPAC Recommendations

- The Secretary should recommend that Congress and the President establish one framework of legal, technological, training, and oversight mechanisms necessary to guarantee the privacy of U.S. persons in the context of national security and law enforcement activities.

- The Secretary should recommend that the President appoint an inter-agency committee to help ensure the quality and consistency of federal government efforts to safeguard informational privacy in the context of national security and law enforcement activities.

- The Secretary should recommend that the President appoint a panel of external advisors to advise the President concerning federal government efforts to safeguard informational privacy in the context of national security and law enforcement activities.

- The Secretary should recommend that the President and Congress take those steps necessary to ensure the protection of U.S. persons' privacy and the efficient and effective oversight of government data mining activities through the judiciary and by this nation's elected leaders through a politically credible process.

- The Secretary should recommend that the President and Congress support research into means for improving the accuracy and effectiveness of data mining systems and technologies; technological and other tools for enhancing privacy protection; and the broader legal, ethical, social, and practical issues involved with data mining concerning U.S. persons.[17]

Key Recommendation of the Joint Inquiry of the House and Senate Select Committees on Intelligence

- Within the Executive Branch, the position of Civil Rights and Civil Liberties Officer in the Department of Homeland Security be filled promptly by a senior and well respected official so that protection of civil liberties is an integral part of homeland security planning and strategy, and not as an afterthought.[18]

---

[16] (...continued)
Weapons of Mass Destruction, *V. Forging America's New Normalcy: Securing Our Homeland, Preserving Our Liberty* (Arlington, VA: Rand Corporation, 2003), p. 23.

[17] Technology and Privacy Advisory Committee, *Safeguarding Privacy in the Fight Against Terrorism* (March 2004), pp. 56-59.

[18] House Permanent Select Committee on Intelligence and Senate Select Committee on Intelligence, *Intelligence Community Activities Before and After the Terrorist Attacks on September 11, 2001*," H.Rept. 107-792 and S.Rept. 107-351, 107th Congress, 2nd session (Washington: GPO 2002).