The Sui Generis Privacy Agency:

How the United States Institutionalized Privacy Oversight After 9-11

By Marc Rotenberg*

Abstract

Privacy scholars have long noted that the United States, unlike many other countries, lacks an independent office for privacy protection. However, as part of the response to 9-11, the US Congress created several new privacy entities. These "sui generis" privacy offices were established to counterbalance the surveillance authority that resulted from the creation of the Department of Homeland Security and the consolidation of the intelligence agencies in the federal government, as well as to advise the President on emerging privacy issues.

This article looks at the Chief Privacy Officer of the Department of Homeland Security, the President's Civil Liberties and Privacy Oversight Board, and the Civil Liberties Protection Officer of the Office of the National Intelligence Director. The article explores the circumstances under which the agencies were established and their legislative mandates. It reviews their activities to date and concludes that, measured primarily against their statutory responsibilities, only the DHS Chief Privacy Officer has had any meaningful impact on the privacy practices of the federal government.

The article makes specific recommendations for how each office might be more effective. In almost all instances, more transparency, regular reporting, frequent public consultation, and great independence are necessary. The article concludes that "in the absence of effective oversight within federal agencies for the new powers created after September 11," the effective checks and balances are likely to be the courts and the Congress.

Table of Contents

---

* Marc Rotenberg is Executive Director of the Electronic Privacy Information in Washington, DC (www.epic.org) and Adjunct Professor at Georgetown University Center. He is a former counsel to the Senate Judiciary Committee. This article was prepared with the excellent assistance of the 2006 Summer IPIOP clerks Courtney Anne Barclay, D. Richard Rasmussen, Anthony Ritz, Jay Goodman Tamboli, and Sunni Yuen. The Internet Public Interest Opportunities Program ("IPIOP") is made possible by a grant from the Glushko-Samuelson Foundation. Professor Francesca Bignami, former Privacy Commissioner David Flaherty, and Professor Jerry Kang provided very helpful comments.

I. Introduction

Privacy scholars have long noted that the United States lacks an independent office for privacy protection as would be found in many other countries.[1] Typically, such offices have a designated commissioner, a full-time staff, investigative authority, and a web site.[2] They publish papers on emerging privacy issues, promote consumer education, and participate in policy debates.[3] They issue annual reports on their activities and appear before legislative oversight committees. Privacy agencies have been called an essential check on the growing surveillance ability of both the government and the private sector.

Such an office was proposed for the United States when the Privacy Act of 1974 was under consideration. But the negotiation between the White House and the Congress that led to the ultimate passage of the Act came at the cost of a privacy office. Since that time, virtually all commentators have suggested the creation of a privacy office, and several bills have been introduced that would fill the gap left open in the 1974 Act.[4] Typically, the debate over these proposals has focused on the scope of authority, whether

---

[1] DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES: THE FEDERAL REPUBLIC OF GERMANY, SWEDEN, FRANCE, CANADA, AND THE UNITED STATES 381-82 (1989); * * *

[2] Consider Argentine, Canada, Germany, and Hong Kong as four models. Argentina's Dirección Nacional de Protección de Datos Personales has a full-time staff of 12, investigates complaints, and can impose criminal and administrative sanctions. Canada's Privacy Commissioner is charged with investigating complaints against the federal government. In Germany, the Federal Data Protection Commissioner, an independent federal agency with 70 on staff, monitors compliance with the Federal Data Protection Act. Hong Kong's Office of Privacy Commissioner, with a staff of 39, ensures compliance with the Personal Data Privacy Ordinance.

[3] The Information and Privacy Commissioner of Ontario publishes reports on new privacy issues and releases them on its web site, http://www.ipc.on.ca/scripts/index_.asp?action=31&N_ID=1&P_ID=21&U_ID=0. Similarly, the European Commission's Article 29 Working Group develops policy statements on privacy issues and solicits comments in the development process.

[4] *See, e.g.*, Privacy Protection Act of 1993, S. 1735, 103d Cong. (1993).

there would be regulatory enforcement against private sector entities, and whether such an agency should exist independently of the executive branch.

But the attack on the United States on September 11 and the subsequent response of Congress changed the terms of debate about the creation of a privacy agency. The original formulation of a general purpose agency with varying degrees of authority was replaced by a series of proposals for specific offices and officials that existed within various agencies. These offices were largely an effort to counterbalance the new surveillance authority that was established by the Congressional response to 9-11 and followed from a recommendation from the 9-11 Commission.[5]

This article looks at three different offices within the federal government that were established after September 11 to address emerging privacy concerns.[6] The article explores the circumstances under which the agencies were established and their legislative mandate. It reviews their activities to date and tries to assess the effectiveness of their work, measured primarily as against their legislative authorization. The article than makes specific recommendations for how the offices might be more effective.[7]

Finally, the article provides general observations about the significance of the creation of *sui generis* privacy agencies in the United States. It appears fair to say that only the office of the Chief Privacy Officer in the Department of Homeland Security has had any meaningful impact on privacy practices in the United, and even there the record

---

[5] FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES 395 (2004).

[6] The article does not discuss the role of the Federal Trade Commission and the various state agencies and officials that have played an increasingly important role in the protection of consumer privacy interests. For more on that topic, see DANIEL J. SOLOVE & MARC ROTENBERG, INFORMATION PRIVACY LAW 541-53 (2003).

[7] The article does not generally address the more detailed theoretical work that has been pursued on the structure and operation of the modern data protection agency. *See, e.g.,* DAVID FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES, *supra*. The article generally seeks to evaluate the effectiveness of the agencies established based on their statutory authority.

is mixed. As to the other entities, there is simply too little information available at this time to assess their performance.

There is some urgency in determining whether the *sui generis* privacy office is an effective means to safeguard privacy interests in the United States. Since 9/11, the federal government has pursued several proposals that have been widely criticized by the public and by the Congress because of their impact on privacy. Some of these programs have been cancelled. Other programs continue though questions about their legality and constitutionality remain. Still other activities are currently under way that raises significant civil liberties concerns, even though there has been hardly any discussion.

The first part of the article provides a brief overview of the most controversial programs pursued by the federal government after 9-11. A key point here is that there is already a recognition that some of these proposals will be modified and others cancelled. At least one measure of a privacy office is whether it plays a meaningful role in this process.

II. Government Surveillance After 9-11

A. Surveillance Programs Cancelled

Central to a functioning political state is the ability to reject proposals put forward by the executive. Even at times of war, a government based on checks and balances must allow for the legislature and the judiciary to make determinations that are independent of the President. Therefore, it is significant that some of the proposals put forward in the United States after 9-11 to expand surveillance of the general public were eventually cancelled, following public opposition and the intervention of Congress or the courts.

The most significant government surveillance program that was eventually withdrawn was the Total Information Awareness program, conceived by former National Security Advisor John Poindexter. Mr. Poindexter had urged the development of a new government database of databases that would accumulate all information on everyone, including communication records, travel records, employment records, and purchase records. Data that was not currently available, such as the identification of individuals in public spaces, would be obtained through the development of new technologies that would be funded by the Department of Defense. Advanced datamining and algorithms would then be applied to this vast data repository to uncover patterns that might suggest the planning of a future terrorist act.

While several of the activities proposed by Mr. Poindexter were adopted by the government in various forms after 9-11, the central design of Total Information Awareness was brought to an end after Congress cancelled the program that was to operate out of the Department of Defense. The months of public debate and opposition had indicated that such a sweeping program of surveillance, at least as conceived by Mr. Poindexter, was more than the American people would support.

Other program met similar fates. The Attorney General proposed a "Terrorism Information and Prevention System" (TIPS) that would have encouraged cable technicians, meter readers, and UPS truck drivers to report suspicious activity to the federal government. Opposition to "operation snitch" mounted.[8] The House of Representatives voted for a version of the Homeland Security bill that prevented the funding of the program.

[8] Dahlia Lithwick, "A Snitch in Time: Don't kill the TIPS program, fix it," Slate, July 31, 2002, http://www.slate.com/?id=2068690&device=

A similar fate met the proposal to establish a formal national ID card in the United States. The legislation that created the Department of Homeland Security included the following language: "Nothing in this Act shall be construed to authorize the developments of a national identification system or card."[9]

Other programs failed because of concerns about reliability and design, in addition to privacy and civil liberties. The Department of State proposed a new hi-tech passport that would incorporate an RFID-chip and enable remote identification of American passport holders, such that it would no longer be necessary to remove a passport from a pocket or purse.

The technology, which was based on a similar system designed to process the passage of cows though a narrow chute, was criticized by technology experts who said that the lack of shielding in the passport and "Basic Access Control," which would allow the individual to determine whether the person accessing the passport was authorized to do so, created an unnecessary privacy risk. Eventually, the hi-tech passport was redesigned with shielding and better control for the passport holder.

B. Surveillance Programs Continuing

There were many new programs undertaken after September 11 to prevent future acts of terrorism, promoted by the President and supported by the Congress. The initiative that was most widely debated was the USA Patriot Act, the legislation enacted in the fall of 2001 that significantly expanded the government's authority to conduct surveillance in the United States, to investigate money laundering, to expel illegal aliens, and to strengthen border security. The provisions in the Patriot Act concerning electronic

[9] Sect. 554 (National Identification system not authorized).

surveillance received the most attention because unlike the other provisions of the bill, the expanded search provisions were subject to four-year sunset that required Congress to reconsider the provisions. But while the debate on Patriot Act renewal was contentious and subject to several extraordinary delays, the Congress ultimately decided to renew the surveillance provisions of the Act, much as they had passed originally.

A second activity of the federal government that has not received support from the Congress is the President's program of domestic surveillance outside of the Foreign Intelligence Surveillance Act. According to news reports in the New York Times and USA Today, the President has authorized the interception of thousand of domestic communications and also authorized the collection of millions of toll records from US telephone companies without judicial approval. The Department of Justice has defended the interception program and stated that the resolution on the Authorized Use of Military Force resolution, passed by the Congress in the fall of 2001, implicitly approved the program. The Department of Justice has also said that the President's inherent powers under Article II put the matter beyond the reach of Congress. As for the toll record disclosure matter, the Justice Department has taken a different tack, choosing neither to affirm or deny the activity.

Although Congress has chosen not suspend funding for these programs, it has not shown support for these activities as it did for the USA Patriot Act. In a series of hearing in both the Senate and the House, lawmakers have questioned the legality of the programs and considered legislation to censure the President. The recent ruling of the Supreme Court in *Hamdan* lends support to those who have said that the President's domestic surveillance program violates the law.

Another major area of expanded surveillance is the US-VISIT program. Established originally to promote border security and to identify terrorists who may be seeking to enter the United States, the program administered by the Department of Homeland Security is rapidly evolving into the hub of identification, linking, profiling, and assessing technologies that span the federal government. Public scrutiny of US-VISIT has largely been left to those outside of the United States because the American citizens and travelers are still not the primary target for the data system. But the program is expanding. Citizens of visa waiver countries are now subject to US-VISIT, and lawful permanent residents ("green card holders") will also now be required to provide a complete ten-print to the Department of Homeland Security. A the Department has made clear that the long-term goal is to police the "virtual border," the prospects for increased identification and surveillance within the United States are self-evident.

The ongoing expansion of US-VISIT begins to suggest the privacy challenges that federal agencies will face in the next several years.

C. Surveillance Programs Emerging

There are a series of programs being pursued by the federal government that have not yet attracted the attention of the programs described above. Typically they involve advanced uses of new technology for monitoring, surveillance, and identification. Some of the programs target populations that have diminished rights under U.S. law, such as immigrants and green card holders. Other programs take advantage of widespread adoption of new systems of public surveillance, such as video cameras that are placed in public spaces in linked together through closed networks that enable ongoing observation by the police.

Perhaps the most sweeping new technology that will impact the civil liberties ands privacy rights of Americans is the emergence of biometric identification. Although the public generally believes these new requirements will fall on visitors and immigrants to the United States, the reality is that over the next several years, virtually every form of identification an American carries could undergo a significant change. Social Security cards could become machine-readable, enabling employees to quickly determine whether an individual is eligible to work in the United States, and perhaps also tapping into databases of background information on prospective employees. The state drivers license may become machine-readable and also include a unique biometric identifier that could reduce the incidence of identity theft, but also magnify problems when identity theft occurs. Various forms of employee identification in both the government and the private sector will enable real-time tracking through the use of RFID chips that provide locational information.[10]

The problem of identification may soon leave the physical construct of an identity document if RFID chips are implanted in humans and become the basis for authentication in a networked environment. Such proposals are already being developed for the elderly, children, and those in the criminal justice system. One company has recently proposed the routine RFID tagging of visitors to the United States.

While it may be too ambitious to imagine that any privacy agency could assess the full scope of these various proposals and make appropriate recommendations, it is not unreasonable to expect a reasonably comprehensive assessment as to their application with a particular agency by asking for Privacy Impact Assessments in each instance. The

[10] [Example]

next sections of this article considered how well three different privacy officers are up to this task.

III. Early Experiments with the Sui Generis Privacy Office: The Computer Systems Security and Privacy Advisory Board

Before turning the privacy offices created after 9-11, it would be helpful to look at one of the early *sui generis* privacy agencies. The Computer System Security and Privacy Advisory Board was established by the Computer Security Act of 1987.[11] As originally conceived, the duties of the CSSPAB were:

> "(1) to identify emerging managerial, technical, administrative, and physical safeguard issues relative to computer systems security and privacy;
>
> "(2) to advise the Bureau of Standards and the Secretary of Commerce on security and privacy issues pertaining to Federal computer systems; and
>
> "(3) to report its findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the National Security Agency, and the appropriate Committees of the Congress.

The role of the CSSPAB was placed within the Department of Commerce; its role was clearly advisory and it lacked many of the authorities that would be found in an independent commission or a privacy agency. Nonetheless it managed to play a significant role in one of the key civil liberties and national security debates that emerged

[11] Pub. L. No. 100-235.

in the federal government during the 1990s and that was whether the federal government should regulate encryption, a critical technique for computer security.[12]

In the February of 1994, the federal government announced a plan to mandate the use of "key escrow encryption," which would have required the use of a computer security standard that would have required those who encoded communications to make available to the federal government copies of their private keys so that their communications could be later decoded. [FN] The proposal provoked a firestorm of controversy and was eventually withdrawn. [FN]

This article will not review the history of the Clipper chip debate, but it is appropriate to note the significant role that the Privacy Advisory Board, established by the Computer Security Act, played in the public debate associated with the proposal. Following a series of briefing with government officials, technical experts, industry leaders, and representatives of civil liberties organizations, the Advisory Board concluded that the technical proposal was deeply flawed. On June 1, 1994, the Advisory Board passed a resolution that warned, "The Government's continued adherence to the Clipper/Capstone key escrow approach risks a costly and ineffective system which will not achieve its objectives." [FN] The CSSPAB resolution gave rise to a significant study by the National Academy of Sciences that described in considerable detail the risks of the key escrow proposal.

How was a federal privacy office able to respond effectively to a government proposal that had high-level support in the national security community? There were at least four factors. First, the Advisory Board was established by statute and had the

[12] See, e.g., National Research Council, CRYPTOGRAPHY'S ROLE IN SECURING THE INFORMATION SOCIETY (National Academy Press 1996).

authority to undertake inquiries into emerging privacy and security issues and to issue reports and resolutions. The question of security standards for the federal government properly fell before the Advisory Board and its authorizing legislation made clear that recommendations and assessments would be expected.

Second, the Advisory Board had distinguished representation from the government, the private sector, and the technical community. The composition of the Board, which was set out in statute, helped ensure that various stakeholders were represented in the decisionmaking of the office and also that members were selected because of their technical qualifications. On matters involving the assessment of technology-based proposals, decisionmakers were somewhat more willing to defer to the views of the advisory board.

Third, the board actively sought input from the public, through both formal and informal channels, and sought to channel the information it received into its work. Public forums were routinely held, public comment was sought, and briefings with officials from other agencies were arranged. The board acted on the information it received through the issuance of letters and statements directed to key government decisionmakers on matters that fell within the board's purview.

Fourth, the board was able to maintain independence. It was expected to advise the Secretary of Commerce, the Director of the NSA and the OMB, and Congressional Committees, but it was not subject to provide political direction or expected to align with a political program. Because its mission was based on the evaluation of scientific and technical proposals, it's credibility was largely tied to the assessment of technology experts.

In evaluating the privacy offices that were established after 9-11, it is worth considering how they compare with the Computer Systems Security and Privacy Advisory Board and whether they would have the ability to reach similar decisions on the proposals under their purview as was the CSSPAB with respect to the Clipper proposal.

IV. The Office of the Chief Privacy officer of the Department of Homeland Security

"First, we will balance our homeland security requirements with citizens' privacy."

– National Strategy for Homeland Security[13]

A. Establishment of the Office

Although the Executive Office of Homeland Security established by President Bush in 2001 included no mention of individual privacy or a privacy office,[14] the earliest versions of the House bill creating the Department of Homeland Security ("DHS") included provisions for the creation of a Chief Privacy Officer ("CPO") within the Department.[15] The Homeland Security Act of 2002, § 222, gave the Secretary of DHS the responsibility to "appoint a senior official in the Department to assume primary responsibility for privacy policy."[16] No confirmation is necessary; the CPO serves in the Office of the DHS Secretary. The responsibilities of the CPO include:

1. assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information;

2. assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act of 1974;

---

[13] OFFICE OF HOMELAND SECURITY, NATIONAL STRATEGY FOR HOMELAND SECURITY (2002) available at http://www.dhs.gov/interweb/assetlibrary/nat_strat_hls.pdf.
[14] Exec. Order No. 13,228 (2001) available at http://www.dhs.gov/dhspublic/display?theme=13&content=5282.
[15] H.R. 5005, 107th Cong. (2002) (enacted Pub. L. 107-296).
[16] 6 U.S.C. § 142.

3. evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government;

4. conducting a privacy impact assessment of proposed rules of the Department or that of the Department on the privacy of personal information, including the type of personal information collected and the number of people affected; and

5. preparing a report to Congress on an annual basis on activities of the Department that affect privacy, including complaints of privacy violations, implementation of the Privacy Act of 1974, internal controls, and other matters.[17]

In addition, the Secretary has created the DHS Data Privacy and Integrity Advisory Committee ("DPIAC") to advise the Secretary and the CPO on "programmatic, policy, operational, administrative, and technological issues relevant to DHS that affect individual privacy, data integrity and data interoperability and other privacy related issues."[18] The Secretary has also delegated Freedom of Information Act ("FOIA") implementation oversight for DHS to the Privacy Office.[19] This additional responsibility for FOIA compliance was assigned to the Privacy Office in recognition of the close connection between privacy and disclosure laws.

The mission of the DHS Privacy Office is to "minimize the impact on the individual's privacy, particularly the individual's personal information and dignity, while

[17] *Id.*
[18] Department of Homeland Security Organization, Department Structure, Privacy Office - DHS Data Privacy and Integrity Advisory Committee, http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0512.xml (last visited July 25, 2006).
[19] Department of Homeland Security Organization, Department Structure, The Privacy Office of the U.S. Department of Homeland Security, http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0338.xml (last visited July 25, 2006).

achieving the mission of the Department of Homeland Security."[20] The Privacy Office seeks to achieve its mission through:

A. internal education and outreach efforts to imbue a culture of privacy and a respect for fair information principles across the department;
B. constant communication with individuals impacted by DHS programs to improve our understanding of DHS's impact, and, where necessary, modify DHS activities—through formal notice, constructive policy discussions, and complaint resolution mechanisms; and
C. encouraging and demanding at all times an adherence to the letter and the spirit of laws promoting privacy, including the Privacy Act of 1974 and the E-Government Act of 2002, as well as widely accepted concepts of fair information principles and practices.[21]

Since the establishment of the office of Chief Privacy Office, three individuals have served. Secretary of Homeland Security Tom Ridge named Nuala O'Connor Kelley on April 16, 2003. Ms. O'Connor Kelly had previously served as legal counsel for DoubleClick Inc and then as Chief Privacy Office at the Department of Commerce. O'Connor served until September 2005 when she left to take a job as head of privacy issues for General Electric.[22]

Following O'Connor-Kelley's departure, Maureen Cooney, Chief of Staff and Director of International Privacy Policy with the Privacy Office, was named acting Chief Privacy Officer. Previously, Ms. Cooney served as Legal Advisor for International Consumer Protection at the U.S. Federal Trade Commission. In that capacity, she also served as a principal liaison for the FTC to the European Commission and Article 29

[20] Department of Homeland Security Organization, Department Structure, Privacy Office – About the Privacy Office, http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0510.xml (last visited July 25, 2006).
[21] *Id.*
[22] Sara Kehaulani Goo and Spencer S. Hsu, "First Privacy Officer Calls 'Experiment' a Success," Wash. Post. Sept. 25, 2006, at A21, available at http://www.washingtonpost.com/wp-dyn/content/article/2005/09/28/AR2005092802173.html

Working Party on privacy issues, including implementation of the U.S-EU Safe Harbor Framework.

On July 26, 2006, DHS Secretary Michael Chertoff named Hugo Teufel, the Department's Associate General Counsel, Chief Privacy Office.[23] Unlike his predecessors, Mr. Teufeul had no apparent qualifications for the position. Teufel previously served as Deputy Solicitor General for the State of Colorado under Attorney General Gale Norton.[24] When Norton was named by President Bush as Secretary of the Interior Department, Teufel followed her to Washington and became an Associate Solicitor at the Department.[25]

The nomination of Teufel to the position sparked some protest.[26] While at the Interior Department, Teufel advised officials in the 2004 dismissal of Teresa Chambers from her position as chief of the U.S. Park Police. Chambers was fired after she complained publicly that she needed more officers and funding, and she was not been granted whistleblower protections.[27] Teufel published *Expanded Use of Nondisclosure Agreements, an Administrative Solution to National Security Leaks* in the Administrative Law Journal in 1990.[28]

B. Activities to Date

---

[23] Office of the Press Secretary, Department of Homeland Security, "Statement by Homeland Security Secretary Michael Chertoff on the Appointment of the Chief Privacy Officer," (July 21, 2006), http://www.dhs.gov/dhspublic/display?content=5752

[24] Anne Broache, *Homeland Security Hires New Privacy Chief*, CNET NEWS.COM, July 21, 2006, available at http://news.com.com/Homeland+Security+hires+new+privacy+chief/2100-7348_3-6097208.html.

[25] *Id.*

[26] *See, e.g.*, David Lazarus, *Privacy Czar Lacks Experience*, SAN FRANCISCO CHRONICLE, July 26, 2006, at C1.

[27] *Homeland Security Taps Teufel as Privacy Chief*, THE WASHINGTON POST, July 22, 2006, available at http://www.washingtonpost.com/wp-dyn/content/article/2006/07/21/AR2006072101427.html.

[28] FindLaw, *supra*.

In testimony to a House subcommittee, Acting CPO Maureen Cooney summarized the efforts of the Privacy Office as "operationalizing privacy."[29] The Privacy Office achieves this by ensuring that the activities of DHS are fully compliant with statutory privacy laws through impact assessments, compliance reviews, and education programs.[30] The primary oversight mechanism of the Privacy Office is the Privacy Impact Assessment ("PIA").[31] The E-Government Act of 2002 requires a PIA whenever DHS procures new information technology systems or substantially modifies existing systems.[32] In addition, DHS has implemented § 222 of the Homeland Security Act to require a PIA for all DHS systems, including national security systems, if they contain personal information.[33] The Privacy Office has required that every PIA must address at least two issues: (1) the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and (2) the protections and alternative processes for handling information to mitigate potential privacy risks.[34] PIAs have been written for systems ranging from the Secure Flight air passenger pre-screening program to the visitor registration and tracking program used at the headquarters of the Transportation Security Administration.[35] The PIAs allow standardized evaluation of privacy issues so that problems can be identified.[36]

---

[29] Hearing before the Subcomm. on Commercial and Administrative Law on the Judiciary, 109th Cong. (2006) (statement of Maureen Cooney, Acting Chief Privacy Officer), available at http://www.dhs.gov/dhspublic/interapp/testimony/testimony_0051.xml.
[30] *Id.*
[31] Joint Hearing before the Subcomm. on Commercial and Administrative Law and Subcomm. on the Constitution on the Judiciary, 109th Cong. (2006) (statement of Maureen Cooney, Acting Chief Privacy Officer), available at http://www.dhs.gov/dhspublic/interapp/testimony/testimony_0047.xml.
[32] 44 U.S.C. § 3501.
[33] Joint Hearing, *supra* (statement of Maureen Cooney, Acting Chief Privacy Officer).
[34] *Id.*
[35] Department of Homeland Security Organization, Department Structure, Privacy Office - Privacy Impact Assessments (PIA), http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0511.xml (last visited July 25, 2006).
[36] Hearing, *supra* (statement of Maureen Cooney, Acting Chief Privacy Officer).

As an example, the United States Visitor and Immigrant Status Indicator Technology ("US-VISIT") Program PIA shows that identifying information is collected on visitors to the United States. It contains a list of information collected and the purposes for that collection.[37] It also notes that, while DHS does not engage in data mining, agencies with which information is shared may data mine.[38] It also contains the length of time for which records are retained,[39] the entities with whom information is shared,[40] and the rights of individuals to decline to provide, to access, and to correct information.[41] This information is reported by the agency in a standard form and posted online for anyone to review.

The Privacy Office also trains all new DHS employees on fair information practices. The training is intended not only to acclimate employees to the PIA mechanism but also to increase awareness and sensitivity to privacy issues.[42] In addition to the basic training, the Privacy Office holds regular workshops to give deeper training on specific issues such as government use of commercial data.[43] The workshops are open to the public.

Since 2003, the Privacy Office has been responsible for responding to FOIA requests for the Department of Homeland Security. As detailed in the 2005 annual report to the Attorney General, the Office responded to 126,126 FOIA requests in 2005, with

---

[37] U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE UNITED STATES VISITOR AND IMMIGRANT STATUS INDICATOR TECHNOLOGY (US-VISIT) PROGRAM 3-4 (2005), available at http://www.dhs.gov/interweb/assetlibrary/privacy_pia_usvisit_update_12-22-2005.pdf.
[38] *Id*. at 7.
[39] *Id*. at 7-8.
[40] *Id*. at 8-11.
[41] *Id*. at 11-15.
[42] Joint Hearing, *supra* (statement of Maureen Cooney, Acting Chief Privacy Officer).
[43] Department of Homeland Security Organization, Department Structure, Privacy Office - Privacy Workshops, http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0830.xml (last visited July 25, 2006).

163,016 requests coming in during that year.[44] In comparison, the Office responded to 152,027 of 168,882 requests in 2004[45] and 160,902 of 161,117 in 2003.[46] Each year the number of requests has increased around 5%, while the number of expedited requests has increased dramatically. At the same time, staffing levels have remained virtually unchanged.

In April 2004, the Privacy Office announced the establishment of the DPIAC, a committee that would be made up of members of the private sector with expertise in privacy, to advise the DHS Secretary and CPO. The Data Privacy and Integrity Advisory Committee (DPIAC) was chartered under the authority of Federal Advisory Committee Act to provide an external and expert perspective to the Secretary and Chief Privacy Officer.[47] The Privacy Office explained that:

> The Committee will advise the Secretary of the Department of Homeland Security (DHS) and the Chief Privacy Office on programmatic, policy, operational, administrative, and technological issues within DHS that affect individual privacy, as well as data integrity and data interoperability and other privacy related issues.[48]

In February 2005, the Department of Homeland Security announced the appointments to the Data Privacy and Integrity Advisory Committee.[49] According to the Department, more than 129 applications were received. The Chief privacy officer stated

---

[44] U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY OFFICE, 2005 ANNUAL FREEDOM OF INFORMATION ACT REPORT TO THE ATTORNEY GENERAL OF THE UNITED STATES 11 (2005), available at http://www.dhs.gov/dhspublic/interweb/assetlibrary/privacy_rpt_foia_2005.pdf.
[45] U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY OFFICE, 2004 ANNUAL FREEDOM OF INFORMATION ACT REPORT TO THE ATTORNEY GENERAL OF THE UNITED STATES 8 (2004), available at http://www.dhs.gov/dhspublic/interweb/assetlibrary/privacy_rpt_foia_2004.pdf.
[46] U.S. DEPARTMENT OF HOMELAND SECURITY, FREEDOM OF INFORMATION ACT ANNUAL REPORT FOR FISCAL YEAR 2003 6 (2003), available at http://www.dhs.gov/dhspublic/interweb/assetlibrary/privacy_rpt_foia_2003.pdf.
[47] Department of Homeland Security, (Apr. 9, 2006), available at http://www.dhs.gov/interweb/assetlibrary/privacy_advcom_notice.pdf
[48] Id.
[49] "Department of Homeland Security, "Department of Homeland Security Announces Appointments to Data Privacy and Integrity Advisory Committee," (Feb. 23, 2006), available at http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0625.xml

that, "The diversity of experience and perspectives represented by this Committee will play an important role in advancing the national discourse on privacy and homeland security."[50] The first meeting of the DPIAC was held in Washington, DC on April 6, 2005.

In May of 2006 DPIAC published a highly publicized report criticizing the use of RFID for identifying people, following many of the comments submitted by EPIC.[51] Specifically, it addressed the e-passport system developed by the State Department as well as the REAL ID Act implementations being developed by DHS.[52] In general, the report found that the risks to privacy and security of RFID were significant enough to render any possible benefits inconsequential.[53] DPIAC has also issued reports on Secure Flight and on government use of commercial data, as well as developing a general framework for analyzing privacy issues.[54]

C. Assessment

1. Assuring that the use of technologies sustain and do not erode privacy protections

The Privacy Office's work to date has been to evaluate privacy issues without correcting them. As described above, one of the tasks on which the Privacy Office spends most of its time is the creation of Privacy Impact Assessments. These PIAs are crafted to bring attention to privacy problems. The assumption in the development of this

---

[50] Id.
[51] See DHS EMERGING APPLICATIONS AND TECHNOLOGY SUBCOMMITTEE, THE USE OF RFID FOR HUMAN IDENTIFICATION (2006), available at http://www.dhs.gov/interweb/assetlibrary/privacy_advcom_rpt_rfid_draft.pdf; EPIC Comments to Data Privacy and Integrity Advisory Committee, http://www.epic.org/privacy/us-visit/comm120605.pdf (last visited July 26, 2006).
[52] *Id.*
[53] *See Id.*
[54] DHS Data Privacy and Integrity Advisory Committee website, *supra*.

system may have been that the agency or responsible party would want to correct privacy problems without outside influence, but publicly available PIAs show that privacy problems are left unresolved.

A key example of an unresolved privacy problem is the possibility of data mining the information collected in the United States Visitor and Immigrant Status Indicator Technology ("US-VISIT") Program. The PIA for that program states, "US-VISIT does not currently have plans to implement data mining technology within the direct program environment. However, US-VISIT shares biographic and biometric information with DHS components, and other federal agencies that make use of data mining for the purposes of both investigative and intelligence gathering purposes."[55] Not only does the PIA ignore the potential for data mining by other agencies, it also allows for future data mining within the US-VISIT program (possibly without a new PIA). This issue is left unresolved, and the only effect of the PIA requirement is that the privacy issue is public.

Similarly, the Privacy Office has programs to train all incoming employees as well as ongoing workshops on privacy issues. These programs undoubtedly increase awareness of privacy issues within the agency, but it is not clear whether the training actually results in better privacy protections for the data subjects; it may be that privacy protections are eroded under revised agency standards that might allow, for example, exemptions to Privacy Act obligations that would be otherwise enforced.

Finally, the Data Privacy and Integrity Advisory Committee ("DPIAC") also increases the information available about privacy by providing advise to the Privacy Office and the Department as a whole. Unfortunately, the agency can choose to ignore

[55] PRIVACY IMPACT ASSESSMENT FOR US-VISIT PROGRAM, *supra*, at 7.

this valuable input. Employees may be aware of issues and problems, but there is no real incentive to solve them.

2. Assuring compliance with the Privacy Act of 1974

The Privacy Impact Assessments discussed above are designed to comply with the reporting requirements of the Privacy Act.[56] In the form, the responsible party must disclose the details of the system including what kinds of information are collected, the reasons for their collection, the intended uses of the information as well as the length of time the information is retained, with whom the information might be shared, and the data subject's rights. The information on the PIA is essential to protecting privacy and required by the Privacy Act of 1974.

Fair Information Practices as set out in the Privacy Act, however, require not only that people be aware of Privacy Act systems but that they be able to access and correct information. The PIA includes information about a data subject's ability to access and correct information, but the Privacy Office does not have the authority to compel compliance with these requirements; under the Privacy Act, only an individual injured by an agency violation may bring a suit against the agency.

[56] The Privacy Impact Assessments required under the EGovernment Act of 2002 and the Homeland Security Act of 2002. Section 208 of the E-Government Act of 2002 requires all Federal government agencies to conduct Privacy Impact Assessments (PIA) for all new or substantially changed technology that collects, maintains, or disseminates personally identifiable information. The Chief Privacy Officer of the Department of Homeland Security is required by Section 222 of the Homeland Security Act to ensure that the technology used by the Department sustains privacy protections. The Privacy Impact Assessment is one mechanism through which the Chief Privacy Officer fulfills this statutory mandate. Privacy Impact Assessments seek to "Minimize intrusiveness into the lives of individuals; Maximize fairness in institutional decisions made about individuals; and Provide individuals with legitimate, enforceable expectations of confidentiality." See generally, Department of Homeland Security, Privacy Impact Assessment Guidance 2006, available at http://www.dhs.gov/interweb/assetlibrary/privacy_pia_guidance_march_v5.pdf.

On June 15, 2005, the Privacy Office announced that it was investigating whether the Transportation Security Administration ("TSA") violated the Privacy Act during the test phase of its Secure Flight program.[57] Days later TSA admitted in a Federal Register notice that it had collected and maintained detailed commercial data about thousands of travelers in violation of an order issued in November 2004 stating it would not do so.[58] The notice said that the agency continued to store commercial data a contractor purchased, combined with information from airlines, and turned over to the agency on CD-ROMs during the testing of Secure Flight. The Privacy Act notification procedure is intended to ensure that the records collection practices of the federal agencies comply with the Act. The Privacy Office has a responsibility to review Privacy Act notices that will be published in the Federal Register and to ensure that the notification is accurate and reflects the agency's actual practices, particularly where a program is under scrutiny because it might create new privacy risks. The failure of the Privacy Office to address this violation at an earlier state of the testing process is clear neglect of statutory responsibilities and raises questions about the reliability of Privacy Act notices published by the Department of Homeland Security.

3. Evaluating legislative and regulatory proposals involving personal information

[57] EPIC Secure Flight Information Page, http://www.epic.org/privacy/airtravel/secureflight.html (last visited July 26, 2006).

[58] The Federal Register notices stated, "TSA is amending the scope of the system of records notice and the PIA to clarify and describe with greater particularity the categories of records and categories of individuals covered by the Secure Flight Test Records system. The category of records include PNRs enhanced with certain elements of commercial data that were provided to TSA for purposes of testing the Secure Flight program and include commercial data purchased and held by a TSA contractor, EagleForce Associates, Inc. (EagleForce), for purposes of the commercial data test." Transportation Security Administration, 70 Fed. Reg. 36,320 (June 22, 2005), available at http://frwebgate4.access.gpo.gov/cgi-bin/waisgate.cgi?WAISdocID=9417424498+30+0+0&WAISaction=retrieve and http://www.epic.org/privacy/airtravel/sf_sorn_pia_062205.pdf.

In cooperation with the Data Privacy and Integrity Advisory Committee ("DPIAC"), the Privacy Office evaluates and reports on proposals. As discussed above, DPIAC has released reports on the use of RFID for human identification and other issues. These reports are publicly available and can be considered by policymakers.

The DPIAC was established on April 9, 2004, and a charter setting out the scope and objectives of the committee was filed on April 26, 2004.[59] The Committee operates under the Federal Advisory Committee Act, which establishes certain obligation for public notice, transparency, and decisionmaking. Initial appointments to the Committee were made on February 23, 2005. Committee members serve staggered terms of two, three, and four years. In announcing the establishment of the Data Privacy and Integrity Advisory Committee, the Chief Privacy Officer said, "meetings will be held on a quarterly basis and will rotate from Washington, DC to forums in other parts of the United States." Four public meetings were held in 2005, two have been held in 2006, and two more are scheduled for the remainder of the year. Although the meetings have been generally well attended and involved the participation of government officials, privacy experts, and technologists, it is unclear at this point what specifically has resulted from the public meetings. For example, at a meeting of the DPIAC in Washington, DC in September 2006, the question of the status of the Passenger Name Record arrangement was raised. This was a significant question, as the European Court of Justice had recently annulled the agreement between the United States and the European Union, negotiated by the Department of Homeland Security that permitted the transfer of personal information on European air travelers to the United States. When the chair of the Advisory

[59] http://www.dhs.gov/interweb/assetlibrary/privacy_advcom_ctr_rev.pdf.

Committee asked the Deputy Secretary about the status of agreement, the Deputy Secretary assured the committee that it would not "turn to dust." There was no indication that the Committee played any role in the original formulation of the agreement or in the subsequent negotiation.

4. Conducting Privacy Impact Assessments

As discussed above, the Privacy Office assists in the completion of Privacy Impact Assessments for any new or substantially revised program. These PIAs include consideration of the type of information collected and its use. The Privacy Office not only trains incoming employees on the PIA process but also holds regular workshops whose topics include PIAs.

The framework developed by the DPIAC may also help with the assessment of new systems. According to the DPIAC, the Framework for Privacy Analysis of Programs:

> sets forth a recommended framework for analyzing programs, technologies, and applications in light of their effects on privacy and related interests. It is intended as guidance for the Data Privacy and Integrity Advisory Committee (the Committee) to the U.S. Department of Homeland Security (DHS) It may also be useful to the DHS Privacy Office, other DHS components, and other governmental entities that are seeking to reconcile personal data-intensive programs and activities with important social and human values.

This 5-part framework is similar to the multi-step analysis done of security systems and provides a systematic way of evaluating not only the privacy risks of a given system but also the efficacy of the system in achieving its intended purpose. The analysis considers the scope of the system, the legal basis of the system, the efficacy of the system, and the effect of the system on privacy interests, and it finally pulls the other data together to help

formulate recommendations for the developer of the system. The Framework was written to be used in analyses by the DHS, but the DPIAC suggests it can be used to analyze privacy issues in other settings as well.[60]

One program to which the Framework can be applied is the implementation of the REAL ID Act.[61] The REAL ID Act provides that any identification card accepted by a federal agency as a form of identification must meet certain standards. Some of these standards are similar to those used for common driver's license designs, such as requiring that the card contain the holder's name, date of birth, home address, and photograph. Other REAL ID requirements, however, are deviations from the usual designs of driver's licenses. These new requirements create possible privacy problems, and analysis under the Framework helps to clarify the problems.

The REAL ID Act § 202(d)(1) requires that "identity source documents" be captured as digital images. Though this is only part of a larger scheme, this single provision can by analyzed under the Framework. In step one of the Framework, the provision's scope is considered; though the precise purpose of this provision is unclear, it is likely an accounting mechanism to allow identification documents to be verified at a later date or to help find employees who may be issuing identity documents fraudulently.

The second step of the Framework asks about the legal basis for the provision; in this case, the provision is part of an act of Congress, so its legal basis is that act. Step two also suggests consideration of other statutes and constitutions, however, so this

---

[60] The DHS Privacy Framework is not as comprehensive or as well known as the popular "Code of Information Practices" that is frequently described in privacy literature. See, e.g., DANIEL J. SOLOVE, MARC ROTENBERG AND PAUL SCHWARTZ, INFORMATION PRIVACY LAW 577-83. But it does share some of the attributes: the Framework provides a set of principles of general applicability, intended to protect privacy, that can be the basis for both legal rules and system design.

[61] Pub. L. No. 109-13, §§ 201-207, 119 Stat. 231, 312 (2005).

provision must be considered in light of the notice requirements of the Privacy Act of 1974 and the implementation must comply with the Privacy Act.[62]

In step three of the Framework, the efficacy of the provision is considered, and the Framework includes a sequence of questions to help evaluate the efficacy. The questions ask what is being protected and from whom or what, what is the likelihood of these threats and the consequences, what the response is to these threats and whether it is appropriate, and, finally, whether the response creates other issues that need to be considered. In this step, the provision should be considered as a possible solution to issuance of fraudulent identification cards, but the response of storing copies of identity documents creates other issues such as securing these copies and preventing unauthorized access.

Step four examines the provision's effect on various kinds of privacy rights, such as anonymity, confidentiality, fairness, accountability, and data security. As with the other steps, detailed questions are provided to help evaluators formulate a response.[63] Here, there is little direct threat to privacy, since the copies will not be publicly accessible, but there are significant risks if the copies are not stored securely, and individuals may not be able to access and correct faulty information. The final step suggests that evaluators consider whether, in light of the other steps, the program is effective and should proceed and whether steps could be taken to mitigate privacy risks. This provision may or may not be worth the effort required for the benefit intended (though here Congress has mandated that it be implemented), but there may be steps that

[62] 5 U.S.C. § 552a.

[63] Unlike the environmental field, where impact assessments incorporate scientific metrics, such as the parts per million of mercury that may be found in a sample of drinking water, privacy assessments typically identify qualitative factors, such as loss of anonymity or the absence of a redress procedure, that might contribute to a better understanding of the consequences of a particular system design.

can be taken to mitigate privacy risks, such as storing only portions of identity documents that are absolutely necessary.

The privacy risks and other possible problems with such provisions may not be immediately visible upon first reading of the provisions, but the Framework is a tool that can be used to analyze and consider the provisions from different perspectives. Analysis of the provisions of the REAL ID Act under this framework highlights some of the severe privacy risks inherent in the mandates of the law.

When REAL ID Act § 202(d)(12), which requires that states make their full motor vehicle database available to other states, is analyzed under the Framework, its flaws also become apparent. When a person applies for a driver's license, the state needs to confirm the person's identity and ensure that the person does not have a valid license from another state. This provision allows states to easily compare information presented by the applicant to information on file in other states, and it allows one state to confirm the status of the applicant's license in other states. These are valid risks to be considered under Step 3. The access provided, however, is broader than necessary, and there could be grave privacy effects under Step 4. While there certainly are efficiency gains in allowing one state to confirm information with another state, the access is not limited to this purpose.

Assuming state law allows it, nothing prevents a police officer from browsing nationwide driving records, selling the information, or using the information for identity theft. For the purposes of the REAL ID Act, all that matters is that the person is who the ID asserts he is. Limiting database access to confirming information the applicant provides in the process of issuing an ID card would restrict its use to this purpose. When

a state needs to verify that a person does not have a valid driver's license in another state, the only information required is a statement that either the person does have a valid driver's license or he does not. As above, allowing a simply confirming query to another state's database would accomplish this purpose. A state has no need to access another state's full record if the only information needed can be presented as a "yes" or "no." As above, there is a serious risk that people will browse information or even use the information for identity theft. Access should be limited to that required for the asserted purpose, and in this case a simple declaration would suffice. Accounting of access could help track down someone who improperly accesses data, but at that point damage has already been done: an identity has been stolen, or the data has been sold. Instead, it is better to limit the data access at the outset. Access should be limited to government entities responsible for confirming information for the issuance of driver's licenses, and for only the purpose of confirming information for the issuance of driver's licenses.

REAL ID Act § 202(d)(5), requiring a check with the Social Security Administration that the correct Social Security Number has been provided by an applicant, presents similar problems that become obvious under a Framework analysis. The legal basis for this provision, examined in step 2 of the Framework, is questionable. In § 7 of the Privacy Act, Congress limited the allowed uses of the Social Security Number ("SSN"). The goal was to prevent use of the SSN as a national identifier, at least for government purposes. In pursuit of that, the Act requires that the government state the statutory basis and intended use for the SSN whenever it is requested. Since the REAL ID Act was passed to ensure accurate identification, use of the SSN seems to be in

violation of the purposes of the Privacy Act. More importantly, though, the intended benefits under Step 3 of checking the SSN are unclear.

The intent seems to be to prevent people from getting a driver's license under an incorrect SSN and to prevent people from getting driver's licenses from multiple states. Each of these purposes is accomplished more effectively through other provisions: the identity information an applicant presents, including SSN, must be verified, and states are required to give other states access to their databases. This additional check with the Social Security Administration accomplishes nothing more. This check requires no additional information from the applicant, but it does require another step in the verification process, implicating data security risks under Step 4. SSNs are sensitive personal information, and they should not be disclosed or transferred unless it is necessary. Requiring it to be sent to the Social Security Administration for an additional check carries an unnecessary risk of disclosure.

The Framework developed by the Department's Data Privacy and Integrity Advisory Committee thus appears to provide a useful technique for evaluating programs that may impact on privacy interests. The analysis is similar to the exercise that is often pursued with the application of Fair Information Practices to record systems, but reflects a somewhat more detailed assessment that mirrors the specific program activities pursued by the Department of Homeland Security.

5. Preparing an annual report to Congress

As required by law, the Privacy Office released a report for 2003 to Congress in June 2004.[64] The report includes an evaluation of the Office's performance in carrying out its statutory and other duties. The office cites among its key achievements:

- "Establishing a Privacy Protection awareness training presented to all newly-hired employees;
- "Establishing a network of Privacy Officers and Freedom of Information Act Officers to respond to the more than 160,000 requests received by the Department in its first year of operation;
- "Building professional partnerships with international privacy councils and workgroups; and
- "Working directly with DHS components and program offices so that privacy protection, compliance, and redress are considered at the front end of security and information systems development."

However, as of the summer 2006, there is still no subsequent report. In 2005, the Office announced the publication of a quarterly newsletter, "Privacy Matters." Only three copies have appeared to date.

6. Ensuring FOIA compliance

The Privacy Office responds to FOIA requests for DHS. As noted above, the percentage of requests to which the Office has responded has dropped significantly over the past few years.

[DISCUSS July 2006 GAO Report on FOIA processing trends.]

[DISCUSS problem of Critical Information statutory exemption.]

[64] U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY OFFICE, REPORT TO CONGRESS (2004), available at http://www.dhs.gov/interweb/assetlibrary/privacy_annualrpt_2004.pdf.

D. Recommendations for Chief Privacy Office

1. Under current statutory scheme

The Privacy Office should take a more active role in enforcing compliance with Fair Information Practices and in protecting privacy. While the Privacy Office currently trains all incoming employees on privacy issues, it should encourage employees to consider actions that may affect privacy with a presumption toward protecting personal privacy and ensuring fairness in decisionmaking based on the information collected by the agency. Entities within the Department of Homeland Security ("DHS") should make a strong effort to comply with Fair Information Practices; the principles help ensure that information is accurate and reliable and will be produce better decisions by the Department. Accurate decisionmaking is particularly important for an agency that plays a central role in safeguarding national security. The principles also provide the basis for the Privacy Act, which the agency obligated to enforce.

The Privacy Act allows a department to exempt programs from compliance with Privacy Act requirements. DHS should commit to refrain from promulgating such exceptions. In order to ensure the personal privacy of all Americans, DHS should exceed the statutory minimums of the Privacy Act. In cases such as the US-VISIT Program whose PIA is discussed above, the Privacy Office should have pressed the responsible party to get an agreement from other parties with whom information may be shared that they will not use the information for another purpose.

The Privacy Office should ensure that problems area addressed at the outset. PIAs that indicate noncompliance, even if theoretical, with the Privacy Act and with Fair Information Practices should be revised. When an entity submits a PIA that shows a

program does not strictly comply or that adequate protections are not in place, the Privacy Office should require that the program be revised to protect privacy rights. Only then should it consider the Privacy Impact Assessment approved.

An example of a program whose PIA should have been rejected is the Homeland Security Information Network Database.[65] The PIA openly states that people whose information is submitted to the system probably will not be aware of that information[66] and because people will generally not know about this information "no procedures will be established to allow for correction of this opinion information."[67] EPIC and other organizations submitted comments to the Privacy Office about this database complaining of these issues and other problems,[68] but as can be seen from the final PIA the issues were never resolved. DHS exempted the database from the requirements of the Privacy Act, but the Privacy Office should have acted to ensure compliance with the Privacy Act than allow the agency to claim exemptions from the law's requirements.

In all of these actions, the Privacy Office should not only seek compliance with the law and with their statutory command to "assur[e] that the use of technologies sustain, and do not erode, privacy protections," but they should work to enhance existing privacy protections.[69] The Privacy Office should encourage DHS to see privacy as a desirable feature of a system rather than as a rule with which they must comply. The aims of the Privacy Act, properly understood, should not be in conflict with the agency's mission. For example, when information collection is not essential to a program, the

[65] U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE HOMELAND SECURITY INFORMATION NETWORK DATABASE (2006), available at http://www.dhs.gov/interweb/assetlibrary/privacy_pia_hsind.pdf.
[66] *Id*. at 9.
[67] *Id*. at 10.
[68] EPIC Comments to Department of Homeeland Security Privacy Office, http://epic.org/privacy/homeland/dhs_hsocd_final.pdf (last viewed July 26, 2006).
[69] 6 U.S.C. § 142.

collection should be narrowed; retaining information under such circumstances creates unnecessary privacy and security risks without any legal basis.

The Privacy Office should also seek to broadly apply the Framework of the Data Privacy and Integrity and Advisory Committee to the various programs, technologies, and applications within its preview. Agency components should be required to publish a public notice describing the program's review under the DPIAC Framework. The Privacy Office should undertake a comprehensive assessment of the REAL ID Act under the DPIAC Framework, similar to the analysis outlined above, prior to the issuance of the regulations to implement the Act.

The Privacy Office needs to complete the 2005 annual report and make that available to Congress and the public as soon as possible. That report is required by statute and provides a critical means of oversight.[70]

The Privacy Office also needs to undertake more formal investigations of agency programs and publish findings. Given the ongoing controversy surrounding the expansion of the US-VISIT program, the Privacy Office should complete an assessment in 2006 of US-VISIT, based on both the DPIAC Framework and complaints received to date.

The Privacy Office has fallen behind in responding to FOIA requests. Though the volume of requests has not risen tremendously, the number of responses is dropping. Though it is unclear why the response rate is dropping, the number of requests received per year is increasing faster than the size of the response staff, and DHS should therefore increase the number of FOIA processors commensurate with the increase in requests.

[70] Section 222 of the Homeland Security Act of 2002 mandates the Secretary shall appoint a senior official in the Department to assume primary responsibility for privacy policy, including: . . . "(5) preparing a report to Congress on an annual basis on activities of the Department that affect privacy including complaints of privacy violations, implementation of the Privacy Act of 1974, internal controls, and other matters."

2. Statutory changes

The Privacy Office has been continually hampered in its investigations by non-cooperation within the DHS. In a 2003 email, then-Chief Privacy Officer Nuala Kelly wrote that the Office was "getting better information from outside than" it had gotten internally.[71] Because of these difficulties, thirteen Members of Congress wrote a letter suggesting that the Privacy Office could be strengthened by giving the CPO subpoena power and broader power to initiate investigations.[72] These changes would give the Privacy Office more power to mandate compliance with privacy protections. These are powers routinely available to an agency Inspector General, and privacy offices in other countries, and should be made available to an office that is expected to undertake independent assessment on behalf of Congress.[73]

---

[71] Email from Carol DiBattiste to Nuala O'Connor Kelly (Nov. 12, 2003), available at http://www.epic.org/privacy/airtravel/jetblue/kelly_email.pdf.

[72] U.S. HOUSE OF REPRESENTATIVES, PROTECTING AMERICA AGAINST TERRORISTS: THE CASE FOR A COMPREHENSIVE REORGANIZATION OF THE DEPARTMENT OF HOMELAND SECURITY 10-11 (2005), available at http://www.epic.org/privacy/us-visit/dhs_review_071405.pdf.

[73] The Inspector General Act of 1978 provides broad powers, including authority "to have access to all records, reports, audits, reviews, documents, papers, recommendations, or other material available to the applicable establishment which relate to programs and operations with respect to which that Inspector General has responsibilities under this Act," sect. 6(1), "to make such investigations and reports relating to the administration of the programs and operations of the applicable establishment as are, in the judgment of the Inspector General, necessary or desirable;" sect. 6(2), "to request such information or assistance as may be necessary for carrying out the duties and responsibilities provided by this Act from any Federal, State, or local governmental agency or unit there," sect. 6(3), to administer to or take from any person an oath, affirmation, or affidavit, whenever necessary in the performance of the functions assigned by this Act, which oath, affirmation, or affidavit when administered or taken by or before an employee of an Office of Inspector General designated by the Inspector General shall have the same force and effect as if administered or taken by or before an officer having a seal;" sect. 6(5). The powers of the federal privacy commissioner in Canada in the investigation of complaints include the authority to:

> (a) summon and enforce the appearance of persons before the Commissioner and compel them to give oral or written evidence on oath and to produce any records and things that the Commissioner considers necessary to investigate the complaint, in the same manner and to the same extent as a superior court of record;
> (b) administer oaths;
> (c) receive and accept any evidence and other information, whether on oath, by affidavit or otherwise, that the Commissioner sees fit, whether or not it is or would be admissible in a court of law;

The Office's effectiveness is also limited because of its dependence on the Department. The Chief Privacy Office is appointed by the Secretary of Homeland Security and reports to him. In the letter from the Members of Congress, they also suggested that the CPO be appointed for a specific term and that he be given the power to report directly to Congress if necessary.[74] Privacy officials in other countries are routinely appointed to their positions for a fixed term, and may not be removed by the executive or an agency head.

These changes would give the Privacy Office greater freedom to act to protect privacy and investigate the Department even when doing so may be unpopular.

V. The President's Civil Liberties and Privacy Oversight Board

The Privacy and Civil Liberties Board ("Board") in the Executive Office of the President was established in December 2004 by legislative action.[75] The Board is intended to advise the executive branch to ensure that privacy and civil liberties are properly considered in the "implementation of all laws, regulations, and executive branch policies related to efforts to protect the Nation against terrorism."[76] Although the intentions with which this Board was established were admirable, the slow formation of

---

> (d) at any reasonable time, enter any premises, other than a dwelling-house, occupied by an organization on satisfying any security requirements of the organization relating to the premises;
> (e) converse in private with any person in any premises entered under paragraph (d) and otherwise carry out in those premises any inquiries that the Commissioner sees fit; and
> (f) examine or obtain copies of or extracts from records found in any premises entered under paragraph (d) that contain any matter relevant to the investigation.

Personal Information Protection and Electronic Documents Act, Section 12(1) ("Powers of Commissioner"), available at http://laws.justice.gc.ca/en/P-8.6/258031.html

[74] *Id.*

[75] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, sec. 1061 (2004) (hereinafter "Act").

[76] Privacy and Civil Liberties Oversight Board, About the Board, http://www.privacyboard.gov/ (last visited July 24, 2006).

the Board has prevented it from being effective thus far. The members have demonstrated an enthusiasm for information gathering. They have organized meetings with experts and administration officials, since being sworn in on March 14, 2006. But there is no indication yet that they have made a substantive contribution to any of the many pending matters on which the executive branch is considering proposals, such as an expansion of warrantless communications surveillance or the expansion of government databases, that may impact privacy and civil liberties interests.

A. Legislative Authority

The Board was established by the Intelligence Reform and Terrorism Prevention Act of 2004 following a recommendation of the 9/11 Commission.[77] In its July 22, 2004 report, the 9/11 Commission emphasized that counter-terrorism efforts must be "accomplished while engendering the people's trust that privacy and other civil liberties are being protected."[78] The report explicitly recommended "[a] board within the executive branch [be created] to oversee adherence to the guidelines we recommend and the commitment the government makes to defend our civil liberties."[79] This board should "[d]etermine, with leadership from the President, guidelines for gathering and sharing information in the new security systems that are needed, guidelines that integrate safeguards for privacy and other essential liberties."[80] The Commission stressed the

[77] Act, *supra*.
[78] 9/11 COMMISSION, THE 9/11 COMMISSION REPORT 419 (2002) (citing Markle Foundation Task Force report, Creating a Trusted Information Network for Homeland Security (Markle Foundation, 2003); Markle Foundation Task Force report, Protecting America's Freedom in the Information Age (Markle Foundation, 2002)).
[79] *Id*. at 395.
[80] 9/11 COMMISSION, 9/11 COMMISSION REPORT, EXECUTIVE SUMMARY 19 (2002).

importance of creating a privacy and civil liberties board under the executive branch, noting that individual privacy offices within federal agencies are limited in scope.

Initial attempts to implement the 9/11 Commission's recommendation for a more comprehensive privacy board contemplated the creation of a civil liberties oversight board with advising, reporting and reviewing functions to oversee the President's adherence to information-sharing guidelines. These first endeavors considered establishing a privacy and civil liberties oversight board as an independent agency within the executive branch rather than the Executive Office of the President.[81] However, the prevailing, and ultimately adopted, view was a board housed within the Executive Office of the President.

The Intelligence Reform and Terrorism Prevention Act of 2004 ("Act") established the Privacy and Civil Liberties Board as an entity within the Executive Office. The Act mandated that the Board's five members be appointed by the President, restricting the chair and vice chair appointments to Senate approval. The Board's authority was confined to review and advice responsibilities – without subpoena power, the Board would have to request the Attorney General's assistance in retrieving information from non-federal department and agency entities. Further, the Act stated that each executive department or agency with law enforcement or antiterrorism responsibilities ought to designate a privacy and civil liberties officer.

The Board advises the President and other senior executive branch officials to ensure that concerns with respect to privacy and civil liberties are appropriately considered in the implementation of all laws, regulations, and executive branch policies

[81] The Protection of Civil Liberties Act, H.R. 1310, 109th Cong., Sess. 2.

related to efforts to protect the Nation against terrorism. This includes advising on whether adequate guidelines, supervision, and oversight exist to protect these important legal rights of all Americans.[82]

In addition, the Board is specifically charged with responsibility for reviewing the terrorism information sharing practices of executive branch departments and agencies to determine whether guidelines designed to appropriately protect privacy and civil liberties are being followed, including those issued by the President on December 16, 2005.[83]

Section 1061 of the Act provides for the creation of the Board. The Board has three chief statutory functions: (1) provide advice to the President or the head of any department or agency of the executive branch on the development and implementation of policy; (2) provide oversight, and; (3) prepare a report at least once a year to Congress on the Board's activities.[84]

The Act authorizes the Board to access all the records, including classified information as permitted by law, of executive branch departments and agencies (and their employees) and Federal officers to carry out its functions.[85] The Act also permits the Board to request assistance from state, local and tribal governments, as well as request entities not affiliated with the executive branch to produce relevant information. In the latter case, IRPTA allows the Board to notify the Attorney General if the recipient of the request does not comply within forty-five days.[86] The Attorney General is then directed to

---

[82] The White House, "Privacy and Civil Liberties Oversight Board," http://www.whitehouse.gov/privacyboard/

[83] George W. Bush, The White House, "Message to the Congress of the United States on Information Sharing," Dec. 16, 2005, http://www.whitehouse.gov/news/releases/2005/12/20051216-9.html; George W. Bush, The White House. "Memorandum for the Heads of Executive Departments and Agencies," Dec. 16, 2005, http://www.whitehouse.gov/news/releases/2005/12/20051216-10.html.

[84] Act, sec. 1061(c).

[85] *Id*. at 1061 (d)(1)(A).

[86] § 1061 (d)(1)(D)(ii).

review the request, provide an opportunity for the subject of the request to explain his reasons for non-compliance, and take appropriate steps to ensure compliance.[87] If the Board deems that the information or assistance requested is unreasonably refused or not provided, the Act directs the Board to report the circumstances to the head of the department or agency concerned, who will ensure compliance in accordance with applicable law.[88] However, these procedures are subject to both the National Intelligence Director and Attorney General's discretion as to whether disclosure of the information sought would thwart national security interests. Further, the Attorney General has the authority to withhold from the Board any information that he determines is sensitive and related to law enforcement or counterterrorism efforts.[89]

For Freedom of Information Act purposes, the Board is to be treated as an agency.[90] The Act explicitly stipulates that the Board will operate within the executive branch "under the general supervision of the President[91] and that each member "shall serve at the pleasure of the President."[92] While Board members must not serve as some other elected official, officer or employee of the Federal Government,[93] both the chairman and vice chairman may serve on a part-time basis.[94] The Act further ensures

[87] § 1061 (d)(2).
[88] § 1061 (d)(3).
[89] § 1061 (d)(4).
[90] § 1061(i)(2). Section 1071 (h) of the Act also facilitates the Board's ability to access information by requiring that executive branch departments and agencies cooperate with Board members and staff to expedite the processing of appropriate security clearances "under applicable procedures and requirements."
[91] § 1061 (k).
[92] § 1061 (e)(1)(E).
[93] § 1061 (e)(2).
[94] § 1061 (e)(1)(D); *see also* § 1061 (f)(1) which sets out the compensation scheme for the part-time and full-time employment of the chairman and vice chairman. It is also worth noting that either the chairman or a majority (3) of members may call and initiate a Board meeting. § 1061(e)(3).

that the Federal Advisory Committee Act[95] does not limit the Board's powers to provide advice to executive branch officers and agencies, or the length of term of its operation.[96]

B. Activities to Date

Although the Board was established in December 2004, President Bush did not send the nominations and appointments to Congress until June 2005.[97] The Committee on the Judiciary held a nomination hearing for Carol Dinkins and Alan Raul, chair and vice-chair respectively, in November 2005 but postponed any confirmation activity due to nomination hearings for the United States Supreme Court. Dinkins and Raul were confirmed February 17, 2006.[98] Dinkins, Raul, and the remaining members—Lanny Davis, Theodore Olson, and Francis Taylor —were sworn in on March 14, 2006.[99][100]

Since that time, the Board has met in person four times, the first meeting occurring on March 14 after the members took their oaths of office.[101] In addition to these meetings, the Board has also "relied on conference calls and other ongoing

---

[95] Pub. L. No. 92-463 (Oct. 6, 1972).
[96] § 1061 (i)(1).
[97] Harold C. Relyea, Congressional Research Service, Library of Congress, Report for Congress, Privacy and Civil Liberties Oversight Board: 109th Congress Proposed Refinements 5 (July 1, 2005) (hereinafter CRS).
[98] About the Board, *supra*.
[99] *Id*.
[100] Carol E. Dinkins is a partner with Vinson & Elkins, where she chairs the administrative and environmental law section. Alan Charles Raul is a partner in Sidley's Washington, D.C., office. Mr. Davis, a partner in Orrick's Washington, D.C. office, is a member of the Litigation Practice Group. Theodore B. Olson is a partner in Gibson, Dunn & Crutcher's Washington, D.C. office; a member of the firm's Executive Committee, Co-Chair of the Appellate and Constitutional Law Practice Group and the firm's Crisis Management Team. Francis X. Taylor was appointed the Chief Security Officer for the General Electric Company on March 7, 2005. He is responsible for overseeing GE's global security operations and crisis management processes. Biographies of the members of the Privacy and Civil Liberties Oversight Board at http://www.privacyboard.gov/index.html.
[101] U.S. House of Representatives, Comm. on Gov't Reform, Subcomm. On Nat'l Security, Emerging Threats, and Internat'l Relations, June 6, 2006 (Statement of Carol E. Dinkins, Chairman, Privacy and Civil Liberties Oversight Board, The White House).

communications to continue to make substantial progress in between formal meetings."[102] The Board has also met with several organizations and individuals in the privacy field, both in government and the private and non-profit sectors. The Chair and Vice-Chair met, via telephone conference, with Governor Thomas Kean, the Chairman of the 9/11 Commission to discuss the efforts of the Board to become active.[103] The Board has also met with several administration officials, including then-White House Chief of Staff Andrew Card; Francis Townsend, Assistant to the President for Homeland Security and Counterterrorism; and Harriet Miers, Counsel to the President.[104]

According to Carol Dinkins, these meetings have helped the Board members "identify several areas of initial interest where [they] believe the Board can play the constructive role envisioned by Congress when it enacted the Intelligence Reform and Terrorism Prevention Act."[105] Meetings are scheduled in the near future with the American Conservative Union, the Markle Foundation, the Board of the National Counterrorism Center, and the National Security Agency.[106]

In addition to these informal sessions, the Board has initiated procedures to assist the executive branch in the implementation of information sharing guidelines, one of its statutorily prescribed obligations.[107] The initial action on this was a meeting with Ambassador Thomas McNamara, Program Manager in the Office of the Director of

---

[102] U.S. House of Representatives, Committee on Gov't Reform, Subcomm. On Nat'l Security, Emerging Threats, and Internat'l Relations, June 6, 2006 (Statement of Carol E. Dinkins, Chairman, Privacy and Civil Liberties Oversight Board, The White House).
[103] *Id*.
[104] *Id*. Additional meetings include Stephen J. Haley, Assistant to the President for National Security; John Negroponte, Director of National Intelligence; General Michael Hayden, then-Deputy Director of National Intelligence. *Id*.
[105] *Id*.
[106] *Id*.
[107] *Id*.

National Intelligence, who is responsible for the drafting and implementation of these guidelines.

The Board has also taken steps to support its administrative functions. It has hired an Executive Director, who is responsible for hiring professional and support staff, and set up personnel security clearances. The Board has set up a suite of offices within the White House complex. And the Board has secured a budget "sufficient to pursue [its] mission."[108]

The Board members have taken the first steps in launching its oversight tenure. The administrative needs are mostly met, and the Board has begun gathering information on the concerns of privacy experts in both government and private and nonprofit sectors. Although, delays in nominations, appointments, and confirmations led to a slow start for the Board, it appears that the members are enthusiastic to meet their statutory responsibilities. However, it does not appear that the Board has engaged its central task.

Under the Information Sharing Environment promoted by the Intelligence Reform and Terrorism Prevention Act of 2004, the Federal Government and the State, local, tribal, and private sector partners that share personal information must "ensure that information privacy and other legal rights of Americans are protected in the development and implementation of the ISE"[109] Specifically, Guideline 5 ("Protect the Information Privacy Rights and Other Legal Rights of Americans") of the President's December 2005 memorandum " Guidelines and Requirements in Support of the Information Sharing Environment" states:

---

[108] *Id.*; *see also* Joint Statement of the Members (May 17, 2006), http://www.privacyboard.gov/press/20060517.html.
[109] Id.

> [T]he Federal Government has a solemn obligation, and must continue fully, to protect the legal rights of all Americans in the effective performance of national security and homeland security functions. Accordingly, in the development and use of the ISE, the information privacy rights and other legal rights of Americans must be protected.
>
> (i) Within 180 days after the date of this memorandum, the Attorney General and the DNI, in coordination with the heads of executive departments and agencies that possess or use intelligence or terrorism information, shall (A) conduct a review of current executive department and agency information sharing policies and procedures regarding the protection of information privacy and other legal rights of Americans, (B) develop guidelines designed to be implemented by executive departments and agencies to ensure that the information privacy and other legal rights of Americans are protected in the development and use of the ISE, including in the acquisition, access, use, and storage of personally identifiable information, and (C) submit such guidelines to the President for approval through the Director of OMB, the APHS-CT, and the APNSA. Such guidelines shall not be inconsistent with Executive Order 12333 and guidance issued pursuant to that order.
>
> (ii) Each head of an executive department or agency that possesses or uses intelligence or terrorism information shall ensure on an ongoing basis that (A) appropriate personnel, structures, training, and technologies are in place to ensure that terrorism information is shared in a manner that protects the information privacy and other legal rights of Americans, and (B) upon approval by the President of the guidelines developed under the preceding subsection (i), such guidelines are fully implemented in such department or agency.

It is unclear at this point whether the President's Board on Civil Liberties and Privacy Oversight has had involvement in this central assignment. The Board should provide a preliminary assessment, available to the public, as soon as possible.

C. Assessment

The Board, although established in December 2004, was not nominated, confirmed, and appointed until March 2006. This delay reflects on the effectiveness of the Executive and Legislative Branches rather than on the Board itself. Since being sworn in, the Board has attended to administrative needs, held informal meetings and testified in

Congress. However, it is unclear what action it has taken assessing the privacy implication of the information sharing policies or assessing emerging privacy issues that should be brought to the attention of the President.

The purpose of the Board is to "provide an enhanced system of checks and balances to protect" privacy and civil liberties.[110] However, the Act provides little mechanism for the Board to "check" any action by the executive branch. The enumerated functions of the Board limit this ability by restricting the Board's activities to review and advise, while providing no method of enforcement or rectification of privacy or civil liberty violations.[111] The Board is further limited by the placement of discretionary power in the office of the Attorney General with regards to compliance with information requests and the Board's ability to access records.[112] This information may be needed for the Board to effectively assess the proposal or implementation of laws, regulations or policies as they implicate privacy and civil liberties.

Not only does the Act not provide any "teeth" for the Board, it explicitly excuses agencies and federal officers, departments, and the executive from consulting the Board prior to implementing "any legislation, law, regulation, policy, or guideline related to efforts to protect the nation from terrorism."[113] In the absence of further action by Congress, unless the board shows significant initiative, it may be able to cite little more than its nice location at a White House as among its key achievements.

D. Recommendations

[110] Pub. L. No. 108-458, Subtitle F, sec. 1061(a)(2).
[111] § 1061(c).
[112] §§ 1061(d)(1)(D)(ii), (d)(2).
[113] *Id*. at (j).

Thus far, the Board has done little to fulfill its statutory mission. Of course, the Board has not had much opportunity to engage in activities related to its purpose, given the short time since its formation. But this does not obviate the importance of the Board's function, particularly considering the alternative proposals that Congress might have pursued.

In protecting civil liberties and privacy, it is important that the Board act in the public eye. Engaging in activities openly will allow the public to fully understand the privacy and civil liberty implications of programs and policies examined by the Board. The Board should hold public hearings to explore law enforcement programs, such as the domestic eavesdropping program and the no-fly lists that raise significant civil liberties concerns for the broad American public. These hearings should specifically probe the potential privacy and civil liberties impacts of these programs.

The current legislation requires that the Board submit an annual report to Congress detailing its actions for the preceding period.[114] However, the Act does not specify the content of that report. The report should contain a review of the Board's authorizing legislation; actions taken by the Board; the status of any ongoing investigations; complaints and reports received by the Board; any recommendations for congressional action; and a report on Freedom of Information Act requests and responses. It is important for the public and the Board to be aware of all such laws, regulations, and policies and the relevant privacy and civil liberty implications. The Board's annual report to Congress also include a listing of all laws, regulations, and executive branch policies

[114] 108 Pub. L. 458 § 1061(c)(4).

proposed and/or implemented during the preceding period, including those that the Board did not address.

The Act does not provide subpoena power to the Board. Chairwoman Dinkins agreed with Congress' assessment, stating "it is incongruous to even consider an office within the White House requiring subpoena power to compel executive branch agencies or officials to provide it with information."[115] This policy relies on the cooperation of the agencies and agency personnel. The Board has no recourse in the event of non-responsive agencies except to notify the Attorney General of such noncompliance.[116] Additionally, the statute provides that the Attorney General and the Directory of National Intelligence can withhold information in the interest of national security and counterterrorism and law enforcement efforts.[117] EPIC recommends that Congress grant subpoena power to the Board. This does not require making materials that the Attorney General determines "sensitive" public. However, providing this information to a board designed for oversight is a necessary step to ensure meaningful review.

Additionally, the statute does not provide the Board with any veto power. Without some enforcement authority, the Board may become a toothless advocate for privacy and civil liberties. The Act provides that the Board "shall … consider" whether there is adequate supervision of the use of the power by the executive branch, whether there are guidelines and oversight of the use of power, whether privacy and civil liberty interests have been balanced against the "need for the power." Additionally, the Board "shall continually review" regulations, laws, and policies and the implementation thereof and information sharing practices "to ensure that privacy and civil liberties are protected."

---

[115] Dinkins, *supra*.
[116] 108 Pub. L. 458, Subtitle F, sec. 1061(d)(1)(D)(ii).
[117] 108 Pub. L. 458, Subtitle F, sec. 1061(d)(4).

However, the statute does not provide for any resulting changes to policies and practices that the Board finds violate privacy and civil liberties. Without any enforcement authority, the Board is helpless to correct any privacy or civil liberty violations it identifies.

Further, the Act explicitly relieves any department or agency from consulting with the Board or observing any waiting period before "developing, proposing, or implementing any legislation, law, regulation, policy, or guideline related to efforts to protect the Nation from terrorism." This provision is incongruent with the purpose of the Board. If the Board is to be effective in ensuring "that concerns with respect to privacy and civil liberties are appropriately considered" the Board must be able to review and comment on such department and agency actions prior to implementation. Congress should amend the language in the Construction provision of the Act to require such consultation and adequate time periods for Board comment.

Although the Act establishes the Board under the authority of the Executive Office of the President, Congress has considered independent status for such a board. Rep. Carolyn Maloney proposed legislation that would "reconstitute" the Board as an Executive Branch independent agency.[118] This legislation would have prohibited the membership comprising of more than three members of the same political party. Further, Maloney's bill would have required Senate confirmation for all members of the Board. Status as an independent would allow the Board to take a more proactive role in protecting privacy and civil liberties, such as vigorously resisting additional exemptions

[118] CRS, *supra*.

to the Privacy Act. Reclassifying the Board as an independent agency to allow for more effective oversight.

The roles of the chairman and vice chairman are crucial to the Board's ability to fulfill its statutory mandate. Full-time commitment to these positions translates into full-time commitment to running a viable checks and balance system that does not sacrifice privacy and civil liberties rights for national security needs. The Act should be revised to make the chairman and vice chairman full-time positions.

VI. The Civil Liberties Protection Officer of the Office of the National Intelligence Director

A. Establishment of Civil Liberties Protection Officer

The Intelligence Reform and Terrorism Prevention Act of 2004[119] established the position of the Civil Liberties Protection Officer – as well as establishing the Office of the Director of National Intelligence itself.[120] The provision of the Act that established this position was originally present in the House version of the bill but not in the Senate version.[121] The Civil Liberties Protection Officer provision made its way into the final bill with minimal legislative history at any point in the process.[122]

The Civil Liberties Protection Officer's responsibilities are to

> **(1)** ensure that the protection of civil liberties and privacy is appropriately incorporated in the policies and procedures developed for and implemented by the Office of the Director of National Intelligence and the

[119] Pub. L. No. 108-458, 118 Stat. 3638 (Dec. 17, 2004) (this provision became effective not later than six months after its enactment, as provided by section 1097 of the Act) (codified at 50 U.S.C. § 403-3d).
[120] *See* 50 U.S.C. § 403 (establishing the Office of the Director of National Intelligence).
[121] *See* CONGRESSIONAL RESEARCH SERVICE, H.R. 10 (9/11 RECOMMENDATIONS IMPLEMENTATION ACT) AND S. 2845 (NATIONAL INTELLIGENCE REFORM ACT OF 2004): A COMPARATIVE ANALYSIS 12 (2004), *available at* http://fpc.state.gov/documents/organization/39304.pdf.
[122] *See, e.g.*, H.R. REP. NO. 108-796, at 241-244 (2004) (Conf. Rep.) (Joint Explanatory Statement of the Committee of the Conference) (making no mention of the Civil Liberties Protection Officer, and including little discussion of civil liberties and privacy officers in general, even in a section entitled "Civil Liberties and Privacy").

> elements of the intelligence community within the National Intelligence Program; **(2)** oversee compliance by the Office and the Director of National Intelligence with requirements under the Constitution and all laws, regulations, Executive orders, and implementing guidelines relating to civil liberties and privacy; **(3)** review and assess complaints and other information indicating possible abuses of civil liberties and privacy in the administration of the programs and operations of the Office and the Director of National Intelligence and, as appropriate, investigate any such complaint or information; **(4)** ensure that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information; **(5)** ensure that personal information contained in a system of records subject to section 552a of Title 5 (popularly referred to as the "Privacy Act"), is handled in full compliance with fair information practices as set out in that section; **(6)** conduct privacy impact assessments when appropriate or as required by law; and **(7)** perform such other duties as may be prescribed by the Director of National Intelligence or specified by law.[123]

"When appropriate, the Civil Liberties Protection Officer may refer complaints to the Office of Inspector General having responsibility for the affected element of the department or agency of the intelligence community to conduct an investigation under paragraph (3) of subsection (b) of this section."[124] However, the Civil Liberties Protection Officer lacks subpoena power and does not report to Congress.[125]

As the 9/11 Commission noted, the Bush administration made minimal progress in fulfilling the privacy protection requirements of this law, failing to appoint a Civil Liberties Protection Officer for nearly a year.[126] The administration waited to appoint a Civil Liberties Protection Officer until only a few days before the NSA domestic wiretapping program was to be revealed by the *New York Times*.[127]

---

[123] 50 U.S.C. § 403-3d(b).
[124] 50 U.S.C. § 403-3d(c).
[125] Anne Marie Squeo, *New U.S. Post Aims to Guard Public's Privacy*, WALL ST. J. ONLINE, April 20, 2006, at B1, *available at* http://online.wsj.com/public/article/SB114549771456130732-fNMKc3AWRNO7Kt58oXWNzzR_pms_20060519.html?mod=tff_main_tff_top.
[126] THOMAS H. KEAN, ET AL., 9/11 COMMISSION, REPORT ON THE STATUS OF 9/11 COMMISSION RECOMMENDATIONS 7 (2005), *available at* http://www.9-11pdp.org/press/2005-10-20_report.pdf.
[127] Ryan Singel, Bush Keeps Privacy Posts Vacant, Wired News, Feb. 2, 2006, *available at* www.wired.com/news/technology/0,70121-0.html.

The first and current Civil Liberties Protection Officer is Mr. Alexander W. Joel.[128] Mr. Joel has held this position, which reports directly to the Director of National Intelligence[129] since his December 7, 2005 appointment by the Director.[130] Before that time, Joel had held the same position on an interim basis beginning in June 2005.[131]

B. Activities to Date

The Civil Liberties Protection Office has yet to produce much, if anything, in the way of tangible privacy protection results, largely because this Office has yet to take much substantive action, at least that has been publicly acknowledged. The Civil Liberties Protection Office has focused on policy, rather than policing, meeting and speaking with some number of government officials, undertaking preliminary consideration of a small number of privacy-related issues, and taking small steps to reach out to the civil society privacy community.

The Civil Liberties Protection Office focuses more on policy than on policing.[132] The Civil Liberties Protection Office oversees privacy protections for "numerous intelligence agencies [that] report up to the [D]irector of National Intelligence,"[133] and

---

[128] Anne Marie Squeo, *New U.S. Post Aims to Guard Public's Privacy*, WALL ST. J. ONLINE, April 20, 2006, at B1, *available at* http://online.wsj.com/public/article/SB114549771456130732-fNMKc3AWRNO7Kt58oXWNzzR_pms_20060519.html?mod=tff_main_tff_top.
[129] 50 U.S.C. § 403-3d(a)(2).
[130] Office of the Director of National Intelligence, Mr. Alexander W. Joel: Civil Liberties Protection Officer, http://www.dni.gov/aboutODNI/bios/joel_bio.htm (last visited July 25, 2006) (discussing Mr. Joel's appointment); *see* 50 U.S.C. § 403-3d(a)(1) (providing that the Civil Liberties Protection Officer is to exist within the Office of the Director of National Intelligence and is to be appointed by the Director of National Intelligence).
[131] Office of the Director of National Intelligence, Mr. Alexander W. Joel: Civil Liberties Protection Officer, http://www.dni.gov/aboutODNI/bios/joel_bio.htm (last visited July 25, 2006).
[132] Anne Marie Squeo, *New U.S. Post Aims to Guard Public's Privacy*, WALL ST. J. ONLINE, April 20, 2006, at B1, *available at* http://online.wsj.com/public/article/SB114549771456130732-fNMKc3AWRNO7Kt58oXWNzzR_pms_20060519.html?mod=tff_main_tff_top.
[133] Anne Marie Squeo, *New U.S. Post Aims to Guard Public's Privacy*, WALL ST. J. ONLINE, April 20, 2006, at B1, *available at* http://online.wsj.com/public/article/SB114549771456130732-fNMKc3AWRNO7Kt58oXWNzzR_pms_20060519.html?mod=tff_main_tff_top.

Mr. Joel says that he works more at "creating a dialogue with government officials, intelligence officers[,] and others" than at looking into complaints.[134] Since March, the Office has also "worked closely" with the Privacy and Civil Liberties Oversight Board.[135]

The Civil Liberties Protection Officer says that he has addressed at least a few privacy issues, including domestic wiretapping, anonymization of data, and increased disclosure of secret government programs. Mr. Joel reviewed the secret NSA domestic wiretapping program and at one point found no problems; he said at the time that he believed the fears about the program to be overblown.[136] More recently, however, Mr. Joel expressed no opinion on the legality of that program, claiming that "[it's] not [his] job to tell the president what the rules are."[137] The Civil Liberties Protection Office is also examining anonymization technologies.[138] In addition, it is looking at methods to disclose more information about secret programs so as to alleviate concerns, while still protecting the "essence" of those programs.[139] No further details seem to be available on any of these inquiries.

Recently, the Civil Liberties Protection Office has taken some steps to reach out to the pro-privacy civil society community. In June, Mr. Joel made waves by hiring former ACLU lobbyist Timothy H. Edgar as his deputy.[140]

---

[134] *Id.*
[135] Scott Shane, *Watching the Watchers: An Intelligence Official Works to Keep Agencies in Bounds*, N.Y. TIMES, July 25, 2006, *available at* http://www.nytimes.com/2006/07/25/washington/25protect.html.
[136] Anne Marie Squeo, *New U.S. Post Aims to Guard Public's Privacy*, WALL ST. J. ONLINE, April 20, 2006, at B1, *available at* http://online.wsj.com/public/article/SB114549771456130732-fNMKc3AWRNO7Kt58oXWNzzR_pms_20060519.html?mod=tff_main_tff_top.
[137] Scott Shane, *Watching the Watchers: An Intelligence Official Works to Keep Agencies in Bounds*, N.Y. TIMES, July 25, 2006, *available at* http://www.nytimes.com/2006/07/25/washington/25protect.html.
[138] Anne Marie Squeo, *New U.S. Post Aims to Guard Public's Privacy*, WALL ST. J. ONLINE, April 20, 2006, at B1, *available at* http://online.wsj.com/public/article/SB114549771456130732-fNMKc3AWRNO7Kt58oXWNzzR_pms_20060519.html?mod=tff_main_tff_top.
[139] *Id.*
[140] *See* Scott Shane, *Watching the Watchers: An Intelligence Official Works to Keep Agencies in Bounds*, N.Y. TIMES, July 25, 2006, *available at* http://www.nytimes.com/2006/07/25/washington/25protect.html;

C. Assessment

Most observers appear to agree that the Civil Liberties Protection Office has been generally ineffective during its brief existence. An evaluation of this question requires the application of standards, and several such standards present themselves. One might reasonably ask whether the Civil Liberties Protection Office has met its congressionally mandated objectives and whether it has met any objectives which may have been set out for it by the President, by the Director of National Intelligence, or in its own statements. In addition to the Congressional requirements, the President and Mr. Joel himself have expressed a purpose to earn the public's trust and soothe the public's privacy concerns.[141] Unfortunately, during his brief time as Civil Liberties Protection Officer, Mr. Joel has not reached these objectives.

Current events continue to raise questions about whether the intelligence community – of which the Director of National Intelligence is the head – is complying with "requirements under the Constitution and all laws . . . relating to civil liberties and privacy."[142] Recent revelations of illegal non-disclosures of secret intelligence programs, even to the chairman of a congressional intelligence committee, show that the

---

Steven Aftergood, ODNI Casts a Wide Net to Hire Staff, Secrecy News, July 14, 2006, http://www.fas.org/blog/secrecy/2006/07/.

[141] *See, e.g.*, Scott Shane, *Watching the Watchers: An Intelligence Official Works to Keep Agencies in Bounds*, N.Y. TIMES, July 25, 2006, *available at* http://www.nytimes.com/2006/07/25/washington/25protect.html; Anne Marie Squeo, *New U.S. Post Aims to Guard Public's Privacy*, WALL ST. J. ONLINE, April 20, 2006, at B1, *available at* http://online.wsj.com/public/article/SB114549771456130732-fNMKc3AWRNO7Kt58oXWNzzR_pms_20060519.html?mod=tff_main_tff_top.

[142] 50 U.S.C. 403-3d(b)(2) (giving the Civil Liberties Protection Officer responsibility for overseeing compliance with these requirements).

administration continues to violate laws and jeopardize privacy and civil liberties by refusing to submit privacy-invasive programs to appropriate legislative oversight.[143]

Mr. Joel's dismissive responses to concerns about the secret NSA wiretapping program further call his performance of his legal compliance responsibilities into question. This program has been the subject of widespread, sustained criticism from a number of sources.[144] As previously noted, the Civil Liberties Protection Officer's first response to this firestorm was to assert that his review of the program found no problems,[145] but Mr. Joel later changed his position to "no opinion," claiming that considering the legality of the program was "not [his] job . . . ."[146] While the former position may have been dubious in the face of so much legal authority taking a contrary view, the latter position can only be seen as a failure of the Civil Liberties Protection Office to do its job. After all, 50 U.S.C. §§ 403-3d(b)(1)-(3) explicitly give the responsibility for such legal oversight to this office.

Nor is there any evidence that the Civil Liberties Protection Office has referred any matters whatsoever to an Inspector General who might be able to pursue matters of

---

[143] *See, e.g.*, Tom Regan, *Another Secret U.S. Intelligence Program?*, Christian Science Monitor, July 10, 2006, *available at* http://www.csmonitor.com/2006/0710/dailyUpdate.html (noting that the Representative Peter Hoekstra, Republican chairman of the House Intelligence Committee, found out about a "significant" secret intelligence program only when alerted by a whistleblower); Charles Babington, *Hoekstra Urges Bush to Impart Intelligence Details*, Wash. Post, July 10, 2006, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/07/09/AR2006070900705.html (discussing Representative Hoekstra's anger at this "'breach of responsibility by the Administration . . . violation of law and . . . direct affront to . . . the Members of this committee,'" noting that the administration may have continued to fall short of its legal obligations with respect to these intelligence programs, and quoting Representative Harman's statement that "vigorous congressional oversight is impossible unless the administration shares critical information with the appropriate committees of Congress").

[144] *See, e.g.*, Wikipedia Contributors, NSA Warrantless Surveillance Controversy, Wikipedia, The Free Encyclopedia, http://en.wikipedia.org/wiki/N.S.A._surveillance_without_warrants_controversy (last visited July 26, 2006) (collecting the mostly-negative third-party legal analyses and other responses to the NSA wireless surveillance program).

[145] Anne Marie Squeo, *New U.S. Post Aims to Guard Public's Privacy*, WALL ST. J. ONLINE, April 20, 2006, at B1, *available at* http://online.wsj.com/public/article/SB114549771456130732-fNMKc3AWRNO7Kt58oXWNzzR_pms_20060519.html?mod=tff_main_tff_top.

[146] Scott Shane, *Watching the Watchers: An Intelligence Official Works to Keep Agencies in Bounds*, N.Y. TIMES, July 25, 2006, *available at* http://www.nytimes.com/2006/07/25/washington/25protect.html.

this sort using subpoena powers that this Office lacks.[147] No privacy impact assessments are known to have been conducted on any of these matters.[148] It is not known what, if any, advice the Civil Liberties Protection Office has supplied to Director of National Intelligence John Negroponte on the privacy status of challenged intelligence programs.

The Civil Liberties Protection Officer has avoided handling complaints and problems relating to privacy, claiming that he prefers to allow other authorities to respond to complaints and handle problems.[149] Certainly, handling of complaints may be seen as "'an additional layer of bureaucracy'" by some interested parties.[150] How much bureaucracy is needed is a delicate policy choice. This choice, however, is not Mr. Joel's to make. 50 U.S.C. § 403-3d(b) explicitly makes this Officer responsible to "review and assess complaints."

The Civil Liberties Protection Office has been equally ineffective regarding the administration's goal of earning the public trust and soothing privacy concerns. Notwithstanding the Office's assurances, recent polls show that the majority of Americans believe that warrantless NSA domestic surveillance "'goes too far in invading people's privacy.'"[151] An even greater percentage of Americans agreed that the current administration has "'gone too far.'"[152] Another poll found similar results, with roughly half of Americans disapproving of the current administration's handling of privacy

[147] *See* 50 U.S.C. § 403-3d(c) (providing for such referrals).
[148] *Cf.* 50 U.S.C. § 403-3d(b)(6) (calling for such assessments to be made where appropriate).
[149] Scott Shane, *Watching the Watchers: An Intelligence Official Works to Keep Agencies in Bounds*, N.Y. TIMES, July 25, 2006, *available at* http://www.nytimes.com/2006/07/25/washington/25protect.html.
[150] *Id.*
[151] David Jefferson, *NEWSWEEK Poll: Americans Wary of NSA Spying*, NEWSWEEK, May 14, 2006, *available at* http://www.msnbc.msn.com/id/12771821/site/newsweek/.
[152] *Id.*

rights.[153] Such concerns about privacy rights have actually risen since the Civil Liberties Protection Office began its work.[154]

There is one area in which the Civil Liberties Protection Office has demonstrated some degree of effectiveness: outreach to civil society privacy groups is a positive step. These actions aid both his congressionally mandated purposes to review privacy complaints and to Americans' protect privacy and his personally asserted purpose to build trust and soothe privacy concerns. They are an important and effective, if incomplete, step in the performance of the Civil Liberties Protection Office's duties.

D. Recommendations

That the Civil Liberties Protection Office has yet to demonstrate meaningful effectiveness in any form of privacy and civil liberties protection is partially attributable to the secrecy with which the intelligence community in general – and this Office in particular – operates. However, it is equally the result of the Office's failure to adequately perform certain congressionally mandated job responsibilities. The long delay in appointing the Civil Liberties Protection Officer and the placement and authority granted to this individual by Congress have no doubt also contributed to the shortcomings of this Office.

Several steps can be taken under the current legal regime to improve the effectiveness of the Civil Liberties Protection Office, and several changes could be made to the legal authority under which that Office operates in order to create further opportunities for improvement.

---

[153] *Washington Post-ABC News Poll*, WASH. POST, May 12, 2006, *available at* http://www.washingtonpost.com/wp-srv/politics/polls/postpoll_nsa_051206.htm.
[154] *See* Gary Langer, Poll: Broader Concern on Privacy Rights, But Terrorism Threat Still Trumps, ABC News, Jan. 10, 2006, http://abcnews.go.com/Politics/story?id=1490715 (last visited July 26, 2006).

1. Reform

There are several steps that the Civil Liberties Protection Office can take to improve its effectiveness. These steps include actively pursuing *all* statutory responsibilities, making more use of available investigatory authority, and improving openness with the public and outreach to civil society.

In light of the nature of the ineffectiveness of this Office, it is most critical that the Civil Liberties Protection Officer fully accepts and works to fulfill *all* of the responsibilities given to him by Congress. In particular, the Civil Liberties Protection Officer should accept that it *is* his job to tell the president when an intelligence program may violate privacy rights;[155] and it *is* his job to handle privacy problems and complaints,[156] even if doing so creates an additional layer of bureaucracy.

In order to satisfy his responsibilities, the Civil Liberties Protection Officer should make better use of the powers he has already been granted. As yet, there is no evidence that Mr. Joel has used his powers to produce any tangible pro-privacy results, and simply using his position to talk to government officials is unlikely to change this fact. This Officer should use his authority to conduct privacy impact assessments and to refer potential privacy problems to Inspectors General who can bring subpoena powers and other resources to bear.

Because the Civil Liberties Protection Office is statutorily accountable only to the Director of National Intelligence, and because earning public trust is a goal of this Office, it is of particular importance that this Office should improve its openness with the public. The Civil Liberties Protection Office should make public the list of specific "government

[155] 50 U.S.C. § 403-3d(b)(2).
[156] 50 U.S.C. § 403-3d(b)(3).

officials, intelligence officers[,] and others" with which it has "creat[ed] a dialogue."[157] The content, or at least the specific subject, of each such meeting should be revealed. In particular, Mr. Joel should disclose how, if at all, he has advised Director of National Intelligence John Negroponte about privacy and civil rights matters related to contentious recent issues like the invocation of the state secrets privilege in the NSA domestic wiretapping cases[158] and the status of executive authority for intelligence programs in light of the recent *Hamdan* ruling.[159]

The Civil Liberties Protection Officer should also continue his encouraging outreach to the civil society privacy community and should continue to seek ways to make more details of government activities public.

2. Additional Authority

Though additional steps by the Civil Liberties Protection Office itself could substantially improve that Office's effectiveness, certain legislative actions would also be helpful. Similar to the privacy officers described above, it would be sensible if the Civil Liberties Protection Officer were granted subpoena power and was also expected to

---

[157] *See* Anne Marie Squeo, *New U.S. Post Aims to Guard Public's Privacy*, WALL ST. J. ONLINE, April 20, 2006, at B1, *available at* http://online.wsj.com/public/article/SB114549771456130732-fNMKc3AWRNO7Kt58oXWNzzR_pms_20060519.html?mod=tff_main_tff_top.

[158] Director of National Intelligence Negroponte has filed both classified and unclassified affidavits asserting the state secrets privilege and seeking dismissal in multiple NSA domestic wiretapping cases. *See, e.g.*, Declaration of John D. Negroponte, Director of National Intelligence, ACLU v. NSA, No. 2:06-CV-10204 (E.D. Mich. May 27, 2006), *available at* http://www.fas.org/sgp/jud/statesec/aclu-negroponte.pdf; Declaration of John D. Negroponte, Director of National Intelligence, Ctr. for Constitutional Rights v. Bush, No. 06-cv-313 (S.D.N.Y. May 26, 2006), *available at* http://www.fas.org/sgp/jud/statesec/ccr-negroponte.pdf. There is no evidence whether the Civil Liberties Protection Officer played any role, including providing any assessment of the legal and/or privacy impacts of the invocation of the state secrets defense, in the process leading up to these filings.

[159] The Supreme Court's decision in Hamdan v. Rumsfeld, 548 U.S. ___, 126 S.Ct. 2749 (2006), cast doubt on the legality of any number of executive branch activities conducted in the name of and on the authority of "fighting the war or terrorism." Again, there is no information on the question of whether the Civil Liberties Protection Officer has provided the Director of National Intelligence with any assessment of the legal and/or privacy policy implications of this issue.

publish an annual report regarding the activities of his office that would be available to the public and Congress. There should also be techniques established to promote public participation and advice. The Office of National Intelligence Director has been given unparallel opportunity to conduct surveillance of the American public. There should be some corresponding means of oversight that helps ensure this authority is not misused.[160]

Each of these suggested changes would be useful. An annual reporting provision would help promote accountability and public trust. Stronger subpoena powers and the power to get expert advisory committees would enable the Civil Liberties Protection Office to form more fully informed opinions and reach better decisions, thus better protecting privacy. In addition to these changes, a provision directing the Civil Liberties Protection Officer to report directly to Congress would alleviate a number of concerns about the Office's independence and relevance.

To date, the Civil Liberties Protection Office has achieved little and failed to meet its mandated goals. The problems it faces, however, are not insurmountable. Simple steps could be taken by the Civil Liberties Protection Officer, possibly supplemented by Congressional grants of additional authority and more extensive staff support, which would create in this position a vital and effective defender of Americans' privacy rights.

VII. Conclusion

Following the events of September 11, the Congress acted to expand the surveillance capability of the federal government through the consolidation of certain government functions, the expansion of legal authority to conduct searches, the development and integration of new data systems, and the promotion of new techniques

[160] See also E-mail from Peter Swire, Senior Fellow, Ctr. for Am. Progress, to Declan McCullagh, Editor, Politech Mailing List (Sept. 27, 2004), http://lists.jammed.com/politech/2004/09/0035.html.

for identification, profiling, tracking, and monitoring. The Congress also chose to create new privacy offices within the federal government to counterbalance some of the new surveillance authorities that were established. To date, two of the three *sui generis* privacy offices have done nothing of consequence. The President's Civil Liberties Oversight Board has seemed more concerned about locating office space than advising the President about a domestic surveillance program that many Americans consider illegal. It has also failed to engage its central responsibility of reviewing the privacy impact of the proposed consolidation of personal information held by federal agencies into an "Information Sharing Environment." The statements from the Civil Liberties Protection Officer for the Director of National Intelligence offer little more in the way of comfort. Although the office was given a broad mandate by the Congress to protect privacy and pursue active engagement across the intelligence community, there is little indication that any of this has occurred.

The one office where it is possible to say that some meaningful oversight has occurred is the Chief Privacy Officer for the Department of Homeland Security. Through public reporting, active outreach, the participation of an external advisory board, the development of a good framework for privacy evaluation, and the issuance of significant reports on the unlawful transfers of personal information of American citizens and the risks of RFID-enabled identity documents, the DHS Privacy Office suggests both the structural attributes and record of achievement that could make a successful agency-specific privacy office. But the office's future remains unclear with the appointment of a political official lacking in any privacy expertise, a delayed annual report, and real

challenges ahead resulting from the expansion of US-VISIT and the implementation of REAL ID.

The intuition of the 9/11 Commission and the work of Congress to establish corresponding means of oversight for the new surveillance authority that was granted to the executive branch after 9/11 was probably correct. But the results to date do not bode well. It is too easy for the President to frustrate meaningful oversight through delay or through reluctance to grant appropriate legal authorities. Where agencies have had some success limiting the activities of the executive, political appointments may bring an end to necessary oversight. And the creation of agency-specific privacy officials may obscure larger challenges to the protection of privacy in the United States, such as the enforcement of the Privacy Act and the limitations on the profiling of American citizens that the Congress effectively prohibited in 1974.

In the absence of effective oversight within federal agencies for the new powers created after September 11, the checks and balances are likely to best be found where the Constitution intended: the Congress, established by Article I, and the Judiciary, established by Article III.