AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

PRIVACY IN THE HANDS OF THE GOVERNMENT: THE PRIVACY OFFICER FOR THE DEPARTMENT OF HOMELAND SECURITY AND THE PRIVACY OFFICER FOR THE DEPARTMENT OF JUSTICE

HEARING

BEFORE THE

SUBCOMMITTEE ON
COMMERCIAL AND ADMINISTRATIVE LAW

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

MAY 17, 2006

Serial No. 109–155

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://judiciary.house.gov

U.S. GOVERNMENT PRINTING OFFICE

27–606 PDF WASHINGTON : 2006

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

F. JAMES SENSENBRENNER, JR., Wisconsin, *Chairman*

HENRY J. HYDE, Illinois
HOWARD COBLE, North Carolina
LAMAR SMITH, Texas
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
STEVE CHABOT, Ohio
DANIEL E. LUNGREN, California
WILLIAM L. JENKINS, Tennessee
CHRIS CANNON, Utah
SPENCER BACHUS, Alabama
BOB INGLIS, South Carolina
JOHN N. HOSTETTLER, Indiana
MARK GREEN, Wisconsin
RIC KELLER, Florida
DARRELL ISSA, California
JEFF FLAKE, Arizona
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TOM FEENEY, Florida
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas

JOHN CONYERS, JR., Michigan
HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
MARTIN T. MEEHAN, Massachusetts
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
ANTHONY D. WEINER, New York
ADAM B. SCHIFF, California
LINDA T. SÁNCHEZ, California
CHRIS VAN HOLLEN, Maryland
DEBBIE WASSERMAN SCHULTZ, Florida

PHILIP G. KIKO, *Chief of Staff-General Counsel*
PERRY H. APELBAUM, *Minority Chief Counsel*

SUBCOMMITTEE ON COMMERCIAL AND ADMINISTRATIVE LAW

CHRIS CANNON, Utah *Chairman*

HOWARD COBLE, North Carolina
TRENT FRANKS, Arizona
STEVE CHABOT, Ohio
MARK GREEN, Wisconsin
J. RANDY FORBES, Virginia
LOUIE GOHMERT, Texas

MELVIN L. WATT, North Carolina
WILLIAM D. DELAHUNT, Massachusetts
CHRIS VAN HOLLEN, Maryland
JERROLD NADLER, New York
DEBBIE WASSERMAN SCHULTZ, Florida

RAYMOND V. SMIETANKA, *Chief Counsel*
SUSAN A. JENSEN, *Counsel*
BRENDA HANKINS, *Counsel*
MIKE LENN, *Full Committee Counsel*
STEPHANIE MOORE, *Minority Counsel*

CONTENTS

MAY 17, 2006

OPENING STATEMENT

	Page
The Honorable Chris Cannon, a Representative in Congress from the State of Utah, and Chairman, Subcommittee on Commercial and Administrative Law	1
The Honorable Melvin L. Watt, a Representative in Congress from the State of North Carolina, and Ranking Member, Subcommittee on Commercial and Administrative Law	6

WITNESSES

Ms. Maureen Cooney, Acting Chief Privacy Officer, U.S. Department of Homeland Security, Washington, DC	
Oral Testimony	9
Prepared Statement	11
Ms. Jane C. Horvath, Chief Privacy and Civil Liberties Officer, U.S. Department of Justice, Washington, DC	
Oral Testimony	15
Prepared Statement	17
Ms. Sally Katzen, Professor, George Mason University Law School, Arlington, VA	
Oral Testimony	25
Prepared Statement	26
Ms. Linda D. Koontz, Director, Information Management Issues, U.S. Government Accountability Office, Washington, DC	
Oral Testimony	31
Prepared Statement	33

LETTERS, STATEMENTS, ETC., SUBMITTED FOR THE HEARING

Prepared Statement of the Honorable Chris Cannon, a Representative in Congress from the State of Utah, and Chairman, Subcommittee on Commercial and Administrative Law	2
Prepared Statement of the Honorable Melvin L. Watt, a Representative in Congress from the State of North Carolina, and Ranking Member, Subcommittee on Commercial and Administrative Law	4

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Response to Post-Hearing Questions from Maureen Cooney, Acting Chief Privacy Officer, U.S. Department of Homeland Security, Washington, DC	64
Response to Post-Hearing Questions from Sally Katzen, Professor, George Mason University Law School, Arlington, VA	68
Response to Post-Hearing Questions from Linda D. Koontz, Director, Information Management Issues, U.S. Government Accountability Office, Washington, DC	70

PRIVACY IN THE HANDS OF THE GOVERNMENT: THE PRIVACY OFFICER FOR THE DEPARTMENT OF HOMELAND SECURITY AND THE PRIVACY OFFICER FOR THE DEPARTMENT OF JUSTICE

WEDNESDAY, MAY 17, 2006

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COMMERCIAL
AND ADMINISTRATIVE LAW,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:06 p.m., in Room 2141, Rayburn House Office Building, the Honorable Chris Cannon (Chairman of the Subcommittee) presiding.

Mr. CANNON. The Subcommittee will please come to order.

At the outset I want to note that immediately following the hearing, we have scheduled the markup of H.R. 2840, the "Federal Agency Protection of Privacy Act."

Let me begin this hearing with an observation written in 1787 by Alexander Hamilton, one of our Founding Fathers, and one of the more interesting of them. He wrote: "Safety from external danger is the most powerful director of national conduct. Even the ardent love of liberty will, after a time, give way to its dictates. The violent destruction of life and property incident to war, the continual effort and alarm attendant on a state of continual danger, will compel nations the most attached to liberty to resort for repose and security to institutions which have a tendency to destroy their civil and political rights. To be more safe, they at length become willing to run the risk of being less free."

Mr. Hamilton's comments are as insightful today as they were when he wrote them more than two centuries ago.

In this post-9/11 world, it is no easy task to balance the competing goals of keeping our Nation secure while at the same time protecting the privacy rights of our Nation's citizens.

As many of you know, the protection of personal information in the hands of the Federal Government has long been a top priority for my Subcommittee, the Subcommittee on Commercial and Administrative Law. Under the leadership of House Judiciary Committee Chairman Sensenbrenner, our Subcommittee has played a major role in protecting personal privacy and civil liberties.

Our accomplishments to date include the establishment of the first statutorily created privacy office in a Federal agency, namely, the Department of Homeland Security. That office has since earned

plaudits from both the private and public sectors, including the GAO.

Just this week, the DHS Privacy Office submitted to Congress a comprehensive assessment of the impact of automatic selectee and so-called no-fly lists for airline passengers on privacy and civil liberties. While these lists can be useful tools for preventing terrorist activity endangering the safety of airline passengers and others, the collection of personal information to create these tools could raise concerns about their impact on privacy and civil liberties. I think we will be interested to hear Ms. Cooney's summary of this report as part of today's hearing.

Inspired by the successes of the DHS Privacy Office, our Subcommittee also spearheaded the creation of a similar function in the Justice Department, which was signed into law in January of this year. Ms. Horvath, another of our witnesses, was appointed to fill this important position on February 21. We also look forward to hearing from Ms. Horvath about her views and goals as the Chief Privacy and Civil Liberties Officer for the Justice Department.

To supplement these efforts, our Subcommittee has also conducted oversight hearings on the subject of the Government's use of personal information. These include a hearing held on the 9/11 Commission's privacy-related recommendations as well as a hearing held just last month on the respective roles that the Federal Government and information resellers have with respect to personal information collected in commercial databases.

As technological devices increasingly facilitate the collection, use, and dissemination of personally identifiable information, the potential for misuse of such information escalates. Five years ago, the GAO warned: "Our Nation has an increasing ability to accumulate, store, retrieve, cross-reference, analyze, and link vast numbers of electronic records in an ever faster and more cost-efficient manner. These advances bring substantial Federal information benefits as well as increasing responsibilities and concerns."

Unfortunately, the GAO continues to find, as we learned from our hearing last month, that Federal agencies' compliance with the Privacy Act and other requirements is, to quote, "uneven."

It is against this complex but exceedingly interesting backdrop that we are holding this hearing today.

I now turn to my colleague, Mr. Watt, the Ranking Member of the Subcommittee, and ask him if he has any opening remarks. But before I recognize him, I just want to say that we appreciate working with Mr. Watt on these issues. He has been a—this Committee has worked well together, and he has been a great support and addition. And with that, Mr. Watt, I recognize you for an opening statement for 5 minutes.

[The prepared statement of Mr. Cannon follows:]

PREPARED STATEMENT OF THE HONORABLE CHRIS CANNON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF UTAH, AND CHAIRMAN, SUBCOMMITTEE ON COMMERCIAL AND ADMINISTRATIVE LAW

Let me begin this hearing with an observation written in 1787 by Alexander Hamilton, one of our Founding Fathers. He wrote:

> "Safety from external danger is the most powerful director of national conduct. Even the ardent love of liberty will, after a time, give way to its dictates. The

> violent destruction of life and property incident to war, the continual effort and alarm attendant on a state of continual danger, will compel nations the most attached to liberty to resort for repose and security to institutions which have a tendency to destroy their civil and political rights. To be more safe, they at length become willing to run the risk of being less free."

Mr. Hamilton's comments are as insightful today as they were when he wrote them more than two centuries ago.

In this post-September 11th world, it is no easy task to balance the competing goals of keeping our nation secure while at the same time protecting the privacy rights of our nation's citizens.

As many of you know, the protection of personal information in the hands of the federal government has long been a top priority for my Subcommittee—the Subcommittee on Commercial and Administrative Law. Under the leadership of House Judiciary Committee Chairman Sensenbrenner, our Subcommittee has played a major role in protecting personal privacy and civil liberties.

Our accomplishments to date include the establishment of the first statutorily-created privacy office in a federal agency, namely the Department of Homeland Security. That office has since earned plaudits from both the private and public sectors, including the GAO.

Just this week, the DHS Privacy Office submitted to Congress a comprehensive assessment of the impact of automatic selectee and so-called "no-fly" lists for airline passengers on privacy and civil liberties. While these lists can be useful tools for preventing terrorist activity endangering the safety of airline passengers and others, the collection of personal information to create these tools could raise concerns about their impact on privacy and civil liberties. I think we will be very interested to hear Ms. Cooney's summary of this report as part of today's hearing.

Inspired by the successes of the DHS Privacy Office, our Subcommittee also spearheaded the creation of a similar function in the Justice Department, which was signed into law in January of this year. Ms. Horvath, another of our witnesses, was appointed to fill this important position on February 21st. We also look forward to hearing from Ms. Horvath about her views and goals as the Chief Privacy and Civil Liberties Officer for the Justice Department.

To supplement these efforts, our Subcommittee has also conducted oversight hearings on the subject of the government's use of personal information. These include a hearing held on the 9/11 Commission's privacy-related recommendations as well as a hearing held just last month on the respective roles that the federal government and information resellers have with respect to personal information collected in commercial databases.

As technological developments increasingly facilitate the collection, use, and dissemination of personally identifiable information, the potential for misuse of such information escalates. Five years ago, the GAO warned:

> "Our nation has an increasing ability to accumulate, store, retrieve, cross-reference, analyze, and link vast numbers of electronic records in an ever faster and more cost-efficient manner. These advances bring substantial federal information benefits as well as increasing responsibilities and concerns."

Unfortunately, the GAO continues to find—as we learned from our hearing last month—that federal agencies' compliance with the Privacy Act and other requirements is "uneven."

It is against this complex, but exceedingly interesting backdrop that we are holding this hearing today.

Mr. WATT. Thank you, Mr. Chairman, and I am going to ask that my civil written statement be put in the record.

Mr. CANNON. Without objection, so ordered.

[The prepared statement of Mr. Watt follows:]

PREPARED STATEMENT OF THE HONORABLE MELVIN L. WATT, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NORTH CAROLINA, AND RANKING MEMBER, SUBCOMMITTEE ON COMMERCIAL AND ADMINISTRATIVE LAW

STATEMENT OF REP. MELVIN L. WATT
Ranking Member, House Judiciary Subcommittee on Commercial and Administrative Law

Hearing on "Privacy in the Hands of the Government: The Privacy Officer for the Department of Homeland Security and the Privacy Officer for the Department of Justice; Markup, H.R. 2840, the "Federal Agency Protection of Privacy Act of 2005"

May 17, 2006
2141 Rayburn House Office Building

Thank you, Mr. Chairman, and thank you for convening this very important hearing.

The privacy issues that confront our country as a result of extraordinary technological advances are significant. The ramification of how we treat the privacy of personally identifiable information is heightened in a post 9/11 world. As a Member of both the Financial Services and Judiciary Committees, I have heard testimony from numerous witnesses on the enhanced concerns with the government's acquisition, maintenance and dissemination of personal information and the opportunities for identity theft and other abuse and misuse of personal details created by the massive data-mining of this information.

One of the main recommendations of the 9/11 Commission was the establishment of a government wide watchdog to safeguard civil liberties. The Commission found that currently "there is no office within the government whose job it is to look across the government at the actions we are taking to protect ourselves to ensure that liberty concerns are appropriately considered." I believed

then, and I continue to believe that a strong Privacy and Civil Liberties Oversight Board –with appropriate subpoena power– is essential to the preservation of the rights of American citizens to some level of personal privacy.

A weaker version of the Privacy Oversight Board was established and I understand the Members of the board have been empaneled. With the creation of this Board, the question arises about how the procedures mandated by the H.R. 2840 (which we will mark-up following this hearing, and on which I was an original co-sponsor 2 terms ago) will complement, duplicate or undermine the work of the Board. Does H.R. 2840 impose an additional layer of process on overburdened agencies? Will the bill be effective in reaching its intended results or give the false appearance to the American public that every measure is being taken prevent government abuse of personal information obtained from whatever source.

I am happy to see some of our witnesses back with us today. I am looking forward to your expertise on what I believe to the shared goal of preserving a sphere of individual privacy while permitting the government the opportunity to do its job. I look forward to your testimony.

Mr. WATT. Thank you, sir, and then I'm going to stray to make some less civil remarks, so you might have bragged too early because I'm feeling a sense of frustration here.

I'm reflecting back to a point several terms ago when eyebrows were raised by the fact that Representative Bob Barr, one of the, quote-unquote, more conservative Members of this Committee, and Representative Mel Watt, quote-unquote, one of the more liberal Members of this Committee, met out here in front of the Capitol and had a press conference about a bill that is this bill.

Well, we marked it up, and Mr. Barr is now gone on into the private sector. The year after he left, we marked it up again. And, you know, at some point we're going to have to do something on this issue more than mark up this bill in the Subcommittee if we are going to begin to be serious about doing what we need to do, it seems to me.

And so it is from that that I am feeling this great sense of frustration that I am beginning to get the feeling that any time some of my colleagues want to feel like they want to say publicly that they are doing oversight over our Government or interested in protecting privacy rights, the way to do that is to put this bill back on for another hearing and another markup, and then next term of Congress we'll be back doing the same thing over and over again as we now have been doing—what?—two or three, maybe—I don't know how many terms of Congress we've marked this bill up and had hearings on it.

So if I'm feeling a little frustrated, it's not because I don't think this is something important. It is more important today than it was when we started three or four terms of Congress ago.

Yeah, we thought the Government was doing some things to invade the privacy rights of individuals, but we certainly—our Government wasn't getting a list of everybody's phone numbers and monitoring phone calls within the United States. So this has gone to a level that is so far beyond what we anticipated or thought about or thought we were addressing at the time we originally introduced this bill. And yet here we are having another hearing, marking up the bill in our Subcommittee, and so I guess maybe I should make a commitment not to be back here next term of Congress doing the same thing that we've done now several times. Unless we are going to be serious about pushing this legislation and getting it considered in the full Committee in the House, in the Senate, this may be just another show that some of our Members think is time to make another public demonstration that we are concerned about the privacy rights of our citizens and the possibility that the Government—the probability—the reality that the Government is way over there beyond where they ought to be on invading those privacy rights.

So I will—I've put my civilized statement in the record, Mr. Chairman. I've made my uncivilized statement. But believe me, I'm just frustrated about where we are on this issue because we've had hearing after hearing, we've had markup after markup, but we still don't have any real results to show for it.

So, with that, I yield back.

Mr. CANNON. The record of this hearing should reflect the Chairman's view that even when Mr. Watt intends to be uncivil, he is an awfully civil human being.

I hope that the gentleman is not suggesting that there is any lack of commitment on my part to this bill, and I point out that actually we've changed the rules recently that allows us now on this side of the Hill to criticize the other side of the Hill for its lack of action. We've actually passed this bill on the House side from the whole—the House of Representatives has passed it out. It has not been acted on by the Senate. The Senate is a complicated body, and we hope that by passing this again, and maybe again and again—we actually passed the Bankruptcy Act eight times before they passed it on the other side. So I agree with the gentleman and his concerns and wish that this issue were actually behind us. And hopefully we'll take that step today to do that.

I just might also point out that there's a difference between monitoring phone calls and comparing numbers that people are calling to connect those phone calls to our enemies outside the country, without arguing for the rightness of any of that, just to make the distinction on the record here.

Without objection, all Members may place their statements in the record at this point. Hearing no objection, so ordered.

Without objection, the Chair will be authorized to declare recesses of the hearing at any point. Hearing no objection, so ordered.

I ask unanimous consent that the Members have 5 legislative days to submit written statements for inclusion in today's record. Hearing no objection, so ordered.

I'm now pleased to introduce the witnesses for today's hearing, three of whom have previously testified before our Subcommittee. We welcome you back and appreciate your continued assistance to our Subcommittee.

Our first witness is Maureen Cooney, the Acting Chief Privacy Officer for the Department of Homeland Security. As I previously noted, the Subcommittee played a major role in establishing Ms. Cooney's office at DHS. The legislation creating her office not only mandated the appointment of a Privacy Officer, but specified the officer's responsibilities.

One of the principal responsibilities of the DHS Privacy Officer as set out by statute is the duty to assure that "the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information." In addition, the Privacy Officer must assure that personal information is handled in full compliance with the Privacy Act and assess the privacy impact of the Department's proposed rules.

Before joining DHS' Privacy Office, Ms. Cooney worked on international privacy and security issues at the U.S. Federal Trade Commission where she served as a principal liaison to the European Commission for privacy issues, a very difficult and burdensome task, I'm sure, especially eating in French restaurants on occasion. I hope you had that opportunity. You don't need to—no incriminating statement is due on that.

She also played a major role in the revision of the guidelines for information systems and networks for the Organization of Economic Cooperation and Development. Prior to that assignment, Ms.

Cooney worked on privacy and security issues with the Treasury Department and at the Office of the Comptroller of the Currency. Ms. Cooney received her bachelor's degree in American Studies from Georgetown University and her law degree from Georgetown University Law Center.

Our next witness is Jane Horvath, the recently appointed Chief Privacy Officer and Civil Liberties Officer for the Department of Justice. In this capacity, Ms. Horvath is responsible for reviewing the Justice Department's compliance with the privacy laws and with developing the Department's privacy policies. In addition to safeguarding privacy, Ms. Horvath oversees the Department's policies relating to the protection of individual civil liberties, specifically in the context of DOJ's counterterrorism and law enforcement efforts. These are really awesome responsibilities. Before joining the Justice Department, Ms. Horvath was the Director of the Washington, D.C., Office of Privacy Laws and Business, a privacy consulting firm. While there, she focused on advising U.S. companies on international privacy trends among other matters. Ms. Horvath received her undergraduate degree from the College of William and Mary and her law degree from the University of Virginia.

Professor Sally Katzen is our next witness. Ms. Katzen is a visiting professor at George Mason University Law School as well as the Sachs Scholar at Johns Hopkins University. Next year, she will be a Public Interest, Public Service Faculty Fellow at the University of Michigan Law School. Prior to joining academia in 2001, Professor Katzen was responsible for developing privacy policy for the Clinton administration for nearly a decade. As the Administrator of the Office of Information and Regulatory Affairs at the Office of Management and Budget, she was effectively the chief information office—policy official for the Federal Government. Her responsibilities included developing Federal privacy policies. Professor Katzen later served as the Deputy Assistant to the President for Economic Policy and Deputy Director of the National Economic Council in the White House. Thereafter, she became the Deputy Director for Management at OMB. Before embarking on her public service career, Professor Katzen was a partner in the Washington, DC, law firm of Wilmer, Cutler and Pickering, where she specialized in regulatory and legislative matters. Professor Katzen graduated *magna cum laude* from Smith College and *magna cum laude* from the University of Michigan Law School, where she was editor in chief of the Law Review. Following her graduation from law school, she clerked for Judge J. Skelly Wright of the United States Court of Appeals for the District of Columbia Circuit.

Our final witness is Linda Koontz, who is the Director of GAO's Information Management Issues Division. In that capacity, she is responsible for issues regarding the collection and use and dissemination of Government information. Ms. Koontz has led GAO's investigations into the Government's data-mining activities as well as e-Government initiatives. In addition to obtaining her bachelor's degree from Michigan State University, Ms. Koontz received certification as a Government financial manager.

I extend to each of you my warm regards and appreciation for your willingness to participate in today's hearing. In light of the

fact that your written statements will be included in the hearing record, I request that you limit your oral remarks to 5 minutes. Accordingly, please feel free to summarize highlights of your—or highlight the salient points of your testimony. You will note that we have a lighting system that starts with a green light. After 4 minutes, it turns to a yellow light, and then at 5 minutes, it turns to a red light. It is my habit to tap the gavel at 5 minutes. We'd appreciate it if you'd finish up your thoughts within that time frame. We don't like to cut people off in their thinking, but I find that it works much better if everybody knows that 5 minutes is 5 minutes. So if you could wrap it up by that time, the time we get there, I would appreciate that, and I will try to be consistent in my tapping, and that includes for other Members of the Committee, who are given 5 minutes to ask questions. This is not like an ironclad rule, by the way. Just we actually are interested in what you have to say, not in the clock.

After you've presented your remarks, the Subcommittee Members, in the order they arrived, will be permitted to ask questions of the witnesses, subject to the 5-minute limit.

Pursuant to the direction of the Chairman of the Judiciary Committee, I ask the witnesses to please stand and raise your right hand to take the oath.

[Witnesses sworn.]

Mr. CANNON. The record should reflect that each of the witnesses answered in the affirmative, and you may be seated.

Ms. Cooney, would you now please proceed with your testimony?

TESTIMONY OF MAUREEN COONEY, ACTING CHIEF PRIVACY OFFICER, U.S. DEPARTMENT OF HOMELAND SECURITY, WASHINGTON, DC

Ms. COONEY. Thank you. Chairman Cannon, Ranking Member Watt, and Members of the Committee, good afternoon. Thank you for the opportunity to speak to the issue of privacy in the hands of the Federal Government and most specifically on activities at the Department of Homeland Security, the role of the Chief Privacy Officer, and initiatives led by the Department's Privacy Office.

As the Subcommittee well knows, the Department of Homeland Security was the first Federal agency to have a statutorily required Privacy Officer. We appreciate the support of this Committee. The inclusion of a senior official accountable for privacy policy and protections honors the value placed on privacy as an underpinning of our American freedoms and democracy. It also reflects Congress' understanding of the growing sensitivity and awareness of the ubiquitous nature of personal data, flows in both private and public sectors, and a recognition of the impact of those data flows upon our citizens' lives.

At the most recent meeting of the Department's Data Privacy and Integrity Advisory Committee, which was created to advise the Secretary and the Chief Privacy Officer on significant privacy issues, Secretary Chertoff noted that the Department has the opportunity to build into the sinews of this organization respect for privacy and a thoughtful approach to privacy.

Secretary Chertoff expressed a belief that I share. We want the Government to be a protector of privacy, and we want to build se-

curity regimes that maximize privacy protection and that do it in a thoughtful and meaningful way. If done right, it will be not only a long-lasting ingredient of what we do in Homeland Security but a very good template for what Government ought to do in general when it comes to protecting people's personal autonomy and privacy.

The Chief Privacy Officer and the DHS Privacy Office have a special role working in partnership and collaboration across the Department to integrate privacy into the consideration of the ways in which the Department assesses its programs and uses technologies, handles information, and carries out our protective mission.

The Privacy Office has oversight of privacy policy matters and information disclosure policy, including compliance with the Privacy Act of 1974, the Freedom of Information Act, and the completion of privacy impact assessments on all new programs or new collections of personal information as required by the E-Government Act of 2002 and section 222 of the Homeland Security Act of 2002.

The Privacy Office also evaluates new technologies used by the Department for their impact on personal privacy. Further, the Chief Privacy Officer reports directly to the Secretary and is required to report to Congress on these matters, as well as on complaints about possible privacy violations.

At this point, if I may, I would like to amplify my written testimony by speaking for a few minutes about the U.S. privacy framework that applies to the Federal space. In tandem, the Privacy Act of 1974, the Freedom of Information Act that promotes transparency of Government operations and accountability, a significant privacy principle, and the E-Government Act of 2002 that augmented the Privacy Act by operationalizing privacy reviews for all new major data collection systems or significant changes to information systems provide a robust umbrella of privacy protections for which the United States can be proud and which I believe is second to none in the Government space. Notice, transparency, and accountability are key to our work in the privacy area.

Today, I'm very happy to address our efforts in this regard with respect to the activities of the Department of Homeland Security from a seat at the table during the investment review process at DHS for technology acquisitions and program funding, through all steps of the technology and program lifecycle development process, the use of PIAs to integrate privacy considerations into standards, strategic planning for programs at the Department, and notice to the public through systems of record notices, to audits and oversight and the development of policy guidance and implementation on key data issues.

I thank you again for the opportunity to share the accomplishments of the DHS Privacy Office, which I have noted in our written testimony, and hope to demonstrate through both the written and oral testimony the importance of privacy in the hands of the Department of Homeland Security and how important it is as a part of our culture. We appreciate the support this Subcommittee has given to our office and look forward to working with you on matters of mutual interest and concern.

Thank you again.

[The prepared statement of Ms. Cooney follows:]

PREPARED STATEMENT OF MAUREEN COONEY

Chairman Cannon, Ranking Member Watt, and Members of the Subcommittee, I am delighted to be back before you today to discuss Privacy in the Hands of the Government as it pertains to activities of the Department of Homeland Security and the efforts of the Privacy Office. Building privacy attentiveness into the very sinews of our still young agency is a responsibility that we take seriously at DHS.

In the eight months that I have served as Acting Chief Privacy Officer, within the Privacy Office we have continued to develop and operationalize privacy policy for the Department, consistent with our statutory mission in Section 222 of the Homeland Security Act and with support and partnership throughout the Department. And as I hope the following testimony will demonstrate, we have been actively implementing our statutory responsibilities as part of the larger mission of the Department. By ensuring that the Department's programs, policies, personnel, and technologies account for and embrace fair information principles—the use of personal information for legitimate, tailored, and sound purposes—the Privacy Office has worked to enhance public trust in the Department and to ensure the protection of an essential right of our people.

My predecessor, Nuala O'Connor Kelly, testified before this Subcommittee in February 2004, and outlined the first year activities of the DHS Privacy Office. I would like to update the Subcommittee on our continued work since that time and our plans for future initiatives.

The Privacy Office has focused on making privacy an integral part of DHS operations. We often use the phrase "operationalizing privacy" to describe these efforts. We want DHS personnel to think about privacy every time they consider the collection, use, maintenance or disclosure of personally identifiable information. Our efforts to operationalize privacy have encompassed a number of activities.

OPERATIONALIZING PRIVACY THROUGH COMPLIANCE

One way to operationalize privacy is to ensure that DHS is fully compliant with statutory privacy requirements and the DHS Privacy Office has been actively engaged in this effort.

In my previous appearance before the Subcommittee, which focused on the use by the government of data from information resellers, I outlined for the Subcommittee how we have used the E-Government Act of 2002's requirement that Privacy Impact Assessments be conducted for new or substantially revised information systems to make sure that privacy is built into DHS programs and that there is transparency about the types of information used by DHS as well as the purposes for which the information is used. PIAs are fundamental in making privacy an operational element within the Department and we have fully utilized this tool to embed privacy as part of DHS operations.

To do this, we have updated and refined our guidance on conducting Privacy Impact Assessments and have distributed it widely both internally to DHS offices and programs and externally to other agencies. Along with the guidance, we also have issued a template for DHS offices to follow in drafting Privacy Impact Assessments. We have fully utilized our Privacy Office website for transparency purposes and have posted these documents so that the public is also aware of our guidance.

"Imitation is the sincerest form of flattery," according to an old expression, and I am happy to report that the DHS Privacy Office's PIA Guidance has served as the basis for other agencies' PIA activities. For example, our PIA template served as the basis for a model PIA for HSPD-12 (Common Identification Standards for Federal Employees) implementation, which was distributed by the Office of Management and Budget through its Interagency Privacy Committee. In addition, other federal agencies have requested to liberally borrow the guidance and we are happy to be able to share it and to add to government efficiency and harmonization of approaches to privacy in the government space.

In addition to requiring that DHS programs conduct Privacy Impact Assessments for new or substantially revised programs, privacy is one of the issues that must be addressed before funding is awarded to a program that involves the collection, use and maintenance of personally identifiable information. The Privacy Office provides significant support to the DHS Office of the Chief Information Officer (OCIO) in the budget process by ensuring that all proposed spending on information technology investments that involve personally identifiable information meets privacy requirements. Not only are our programs required to complete a Privacy Threshold Analysis, which helps us to determine whether a full Privacy Impact Assessment is necessary, but funding for DHS programs through the budget process cannot go forward without program compliance with privacy mandates. The DHS Privacy Of-

fice therefore has a strong "stick" to accompany the "carrot" of funding to ensure that privacy becomes operationalized in DHS programs.

Privacy compliance reviews are another important tool for operationalizing privacy into DHS programs, and during this past year, the Privacy Office undertook the first privacy review of what we expect to be many when we analyzed compliance by the U.S. Customs and Border Protection (CBP) with its Passenger Name Record (PNR) Undertakings. These Undertakings were provided by CBP to the European Commission in order to demonstrate that CBP has adequate privacy protocols in place to protect personally identifiable information as a condition precedent to receiving PNR information about European airline passengers. Based on the Undertakings, the EU agreed to share passenger name record information with CBP in order to fight terrorism and other serious crimes as well as to facilitate transatlantic travel.

The Privacy Office's compliance review consisted of a full analysis of CBP policies and procedures, interviews with key managers and staff who handle PNR, and a technical review of CBP systems and documentation. This compliance review occurred over a several-month period and as a result of changes recommended by the Privacy Office or made unilaterally by CBP, we were able to conclude that CBP achieved full compliance with the representations it had made in the Undertakings. This finding was the primary factor in the ability of the Privacy Office to conclude a successful joint review, with representatives of the EU, of CBP's compliance with the US-EU PNR Agreement.

We conducted a different kind of compliance review when we examined the use of commercial data by the Transportation Security Administration (TSA) in connection with the Secure Flight Program after privacy concerns were raised by the Government Accountability Office. We analyzed whether TSA's public notices about this use of commercial data for testing purposes matched the actual test protocols and made recommendations, as a result of this review. The Privacy Office continues to work closely with TSA to implement privacy statutory requirements and best practices in the design and implementation of this as well as other TSA screening programs.

In compliance with the requirements of the Computer Matching and Privacy Protection Act, as amended, the Privacy Office established a Privacy and Data Integrity Board to approve matching agreements undertaken by DHS components, as required by law, and to weigh in on privacy policy issues of interest and concern to the Department. Our Board held several meetings at which we discussed ideas for responsible information handling, and the Board was instrumental in assisting the Privacy Office in completing several required reports.

Ensuring publication of appropriate Privacy Act systems of records notices (SORNs) rounded out the Privacy Office's compliance activities. These notices, in fact, necessarily are a regular and ongoing part of the Privacy Office's work and of our statutory obligation to ensure that the Department maintains personally identifiable information in conformity with the requirements of the Privacy Act.

OPERATIONALIZING PRIVACY THROUGH EDUCATION

A significant way to increase privacy awareness and ensure that it is embedded in DHS is through education and training. The Privacy Office trains all new DHS employees as part of their overall orientation to the Department. We continue to develop, moreover, more robust training courses to be provided to all DHS employees and contractors to augment their privacy background and to raise awareness and sensitivity about the importance of the respectful use of personal information by the Department. And we have conducted training on Privacy Impact Assessment requirements for individual DHS offices, information technology managers, business managers, and systems analysts. Establishing the lines of communication between DHS personnel and our office through these training programs helps us to get our message across and helps employees to be sensitized to proper information handling techniques.

Our component privacy officers also make sure that employees in our components and offices are provided robust privacy training. I would be remiss, in fact, if I didn't emphasize the close collaboration and rapport our office has with other privacy officers in the Department, who were installed at our urging and who help the DHS Privacy Office carry out our important work

In addition to our general education and training programs, the Privacy Office has conducted two workshops intended to raise privacy awareness among DHS personnel as well as the public. These workshops have drawn subject matter experts together to discuss privacy issues raised by homeland security programs. The issues

we have explored are both relevant and topical. We have posted both transcripts and summaries of our activities on our website.

I mentioned in my April 4, 2006 testimony before this Subcommittee that we had conducted a workshop on the government's use of commercial data for homeland security purposes. The objective of that workshop was to look at the policy, legal and technology issues associated with the government's use of commercial data in homeland security programs. Just last week our Privacy and Data Integrity Board held preliminary discussions on development of a policy regarding the use of commercial data by DHS, and the information we gleaned from our workshop will be helpful as we move forward on this vital issue.

Last month, we conducted another workshop on the use of personal information by the government and how we can achieve transparency and accountability. This workshop sparked discussions about the utility of privacy notices to accomplish transparency and how those notices can be written in a way that is comprehensible while it is also comprehensive. We also discussed the utility of the Freedom of Information Act for fostering accountability through access to information about individuals that is maintained by the government. We were fortunate to have several panel members from other nations who could contribute a global perspective on this issue. Again, the workshop complemented our internal training efforts to raise privacy awareness and also served an important educational function to improve public understanding of DHS programs.

INFORMATION SHARING AND OUTREACH

Information sharing has become a significant focus of the DHS Privacy Office. The Intelligence Reform and Terrorism Prevention Act established requirements for an information sharing environment. This legislative mandate augmented Executive Orders and Homeland Security Directives issued by President Bush all aimed at fostering a climate of robust exchanges of terrorism related information in a privacy sensitive manner. Executive Order 13356, for example, directed all departments and agencies to enhance the interchange of terrorism-related information within the Federal government and between the Federal government and appropriate authorities of state and local governments. The DHS Privacy Office led the effort to integrate privacy protections into the planning process supporting the implementation of this Executive Order.

Similarly, the DHS Privacy Office led the effort within DHS to integrate privacy protections at the earliest stages of implementing HSPD-11, a Presidential directive that concerns terrorist-related screening procedures. Within DHS, moreover, the Privacy Office has supported the work of the Information Sharing and Collaboration Office (ISCO), which was established to lead the creation of a DHS information sharing environment. The Privacy Office provided both resources and guidance to ISCO to help create a set of business rules for sharing personal information in a way that minimizes privacy intrusions while maximizing use of the data for homeland security purposes.

The Privacy Office also participated in a number of interagency activities designed to foster inter-agency exchanges of information on privacy technologies and other privacy issues. We chair, for example, the Social, Legal and Privacy Subgroup of the National Science and Technology Council's (NSTC) Subcommittee on Biometrics. Established by Executive Order, NSTC is the principal means by which the President coordinates science, space, and technology policy across the government. NSTC's Subcommittee on Biometrics has examined issues related to the development and use of biometric technologies in the Federal government and the Social, Legal and Privacy Subgroup was responsible for developing a rich, centralized repository of information about the social history of biometrics, the legal framework that applies to the collection and use of biometrics, and the privacy principles that should govern the responsible use of this technology. Analysis of this repository and actual implementations resulted in a paper that connects privacy and biometrics at a structural level so that both fields can be understood within a common framework, thus enabling federal agencies and public entities to implement privacy-protective biometric systems.

We have also begun coordinating with the White House's Privacy and Civil Liberties Oversight Board on information sharing and other relevant issues. Through this work, the DHS Privacy Office is able to foster interagency cooperation, coordination and collaboration on privacy matters.

The Privacy Office has also reached out to experts in the private sector to help us understand programmatic, policy, operational and technology issues that affect privacy, data integrity, and data interoperability. To that end, in April 2004, the Department chartered the Data Privacy and Integrity Advisory Committee (DPIAC)

under the authority of Federal Advisory Committee Act to provide an external and expert perspective to the Secretary and Chief Privacy Officer. The DHS Privacy Office provides administrative and managerial support to the DPIAC. In return, the Committee has provided significant advice to the Chief Privacy Officer and the Secretary on important privacy considerations. The Committee offered its recommendations on TSA's Secure Flight Program, which have helped the DHS Privacy Office to formulate its own advice on this significant initiative. The Committee also provided guidance on the *Use of Commercial Data to Reduce False Positives in Screening Programs,* which will help inform any final policy that the Privacy Office recommends on this important topic. We expect to continue to get advice from the Committee on other issues of interest to the Department.

INTERNATIONAL INITIATIVES

Because the work of the Department is both national and international in scope, the work of the DHS Privacy Office is equally broad. The primary goal of the DHS Privacy Office's international activities has been to convey to the global community the importance of fair information practices to our office, the Department and the nation. We have devoted significant resources to working with programs in multilateral global forums, such as the OECD, as well region-centric international organizations such as the Asian Pacific Economic Cooperation forum (APEC). In addition, of course, the Privacy Office works with the European Union and on issues raised by the Joint Supervisory Body representatives of Europol and Eurojust.

We have had substantial input on a number of international privacy initiatives, including the Enhanced International Travel Security Initiative (EITS), under the leadership of DHS's Science and Technology Directorate and US-VISIT, and real-time sharing of lost and stolen passports in a way that properly protects privacy, through an APEC-sponsored initiative known as the Regional Movement Alert List. The Privacy Office also works more generally within international organizations to shift the international privacy dialogue away from conflicting laws to compatible privacy principles in order to foster information sharing for homeland security and other necessary purposes. Our work has been helpful in improving international opinion regarding the United States Government's attention to privacy principles in the design and operation of information systems.

FUTURE ACTIVITIES

As I hope the foregoing demonstrates, the DHS Privacy Office takes a comprehensive approach to its statutory mission and has worked on a wide range of initiatives to ensure that privacy policy concerns are part of the necessary dialogue on the development and implementation of homeland security programs. We have been fortunate that Congress has provided funding to allow us to expand our staff of dedicated privacy professionals whose credentials rival those of anyone in the government or the private sector. And we are energized as we look ahead to some future activities.

We recently completed a draft of a report on data mining, which is required by the 2005 DHS Appropriations Act, and we expect to continue our study of data mining programs at the Department in the coming year. Data mining can be a useful and important tool in the war against terrorism, and we are committed to ensuring that this technique is used responsibly and appropriately at DHS.

We have already planned our next privacy workshop to focus on Privacy Impact Assessments. This timely session will enable DHS program officers to comply with the privacy requirements necessary for approval of their funding requests. We are also finalizing arrangements for the next DPIAC meeting, which will be held in California, and which will focus on expectations of privacy in public spaces and the use of RFID technology, two issues that have significant ramifications for Departmental activities.

We plan to work closely with the OCIO to build privacy protections into every system across DHS, and we intend to collaborate with the Science and Technology Directorate to add privacy protections to the approval process for new homeland security research initiatives.

Because they are our "bread and butter" issues, the DHS Privacy Office will also continue to work to ensure that individual programs sustain and enhance privacy protections through strict compliance with the PIA and SORN requirements of federal law. We will continue to refine our privacy guidance and enhance our privacy training initiatives to foster a culture of privacy awareness within the agency.

We expect to complete development of a policy for the respectful and appropriate use of commercial data for homeland security purposes. And we anticipate that in the international arena, we will continue to be an important voice for the development of privacy-appropriate cross-border information sharing policies.

Thank you for the opportunity to share the accomplishments of the DHS Privacy Office and to demonstrate, through this testimony, the importance of privacy "in the hands" of the Department of Homeland Security. We appreciate the support this Subcommittee has given to our office and look forward to working with you on matters of mutual interest and concern.

Mr. CANNON. Thank you, Ms. Cooney.

Ms. Horvath, you are recognized for 5 minutes.

TESTIMONY OF JANE C. HORVATH, CHIEF PRIVACY AND CIVIL LIBERTIES OFFICER, U.S. DEPARTMENT OF JUSTICE, WASHINGTON, DC

Ms. HORVATH. Mr. Chairman and Members of the Subcommittee, thank you for inviting me to testify regarding the Department of Justice Privacy and Civil Liberties Office in connection with the Committee's hearing.

I started as the Department of Justice's Chief Privacy and Civil Liberties Officer on February 21, 2006. I am responsible for Department-wide protection of privacy and civil liberties. During my first 30 days at the Department of Justice, we assessed the existing privacy and civil liberties functions at the Department. I met with senior officials of the DOJ components that had either privacy or civil liberties responsibilities within the Department. At all of these meetings, I was welcomed with enthusiasm. I received detailed briefings regarding their privacy and civil liberties efforts. From those meetings, we were able to determine priorities for the Office of Privacy and Civil Liberties.

After meeting with the Chief Information Officer, we decided to centralize the privacy impact assessment process. We determined that the PIA process within the Department would be much more effective if all the components were working from a standard template with standard guidance. Utilizing some of the aspects of the DHS model, we drafted official PIA guidance, a privacy threshold analysis to determine whether a PIA is required, and a new PIA template. Next month, we're going to hold a 1-day training session on PIA preparation and Privacy Act issues with members of the CIO staff and persons within the components who are responsible for Privacy Act issues.

In furtherance of our civil liberties missions, we set up and launched a DOJ Privacy and Civil Liberties Board on April 17, 2006. Representatives of the law enforcement, national security, and other relevant components are represented on the Board. We have subdivided the Board into three separate committees: an Outreach Committee, focusing on outreach to the Arab, Muslim, and other ethnic or religious minority communities; a Data Committee, examining issues related to information privacy within the Department; and a Law Enforcement Committee, providing a forum for law enforcement to discuss effort that might have an impact on civil liberties or privacy.

Shortly after I arrived, we started to reach out to privacy advocacy and public policy groups. We've met with representatives from the ACLU, Center for Democracy and Technology, Cato Institute, Heritage Foundation, the Center for Information Policy Leadership at Hunton and Williams, and Peter Swire, the former Chief Counselor for Privacy in the U.S. Office of Management and Budget.

We've also been active in intergovernmental groups and efforts. We believe that by working together as a group, privacy officers within the Government can utilize each other's collective experience.

Our office has also been active in advising the Department of information-sharing initiatives. While information sharing is an incredibly important initiative for our security, it also involves important privacy and civil liberties issues. We are pleased that the Administration and the Attorney General has recognized the importance of addressing these issues at the inception of information-sharing programs.

Since my arrival, I have co-chaired the President's Information Sharing Environment Guideline 5 Working Group with Alex Joel, the Director of National Intelligence Civil Liberties Protection Officer. Guideline 5 of the December 16th memorandum from President George W. Bush requires, in relevant part, that the Attorney General and the Director of National Intelligence 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. We also look forward to working with the President's Privacy and Civil Liberties Oversight Board on the guidelines.

The Privacy and Civil Liberties Office also oversees the Department's compliance with the Privacy Act of 1974 and plays an active role in ensuring that the Department's law enforcement, litigation, and anti-terrorism missions are carried out in accordance with its provisions. We also provide Privacy Act guidance within the Department, both in response to specific inquiries raised by the components and through training programs.

Although I have only been at DOJ a short while, my arrival has been greeted with enthusiasm. We have been consulted on numerous initiatives. In the coming year, we hope to launch new efforts, such as more extensive privacy and civil liberties training, that will further the office's mission of protecting the privacy and civil liberties of those who interact with the Department of Justice.

Thank you for the opportunity to speak today.

[The prepared statement of Ms. Horvath follows:]

PREPARED STATEMENT OF JANE C. HORVATH

Department of Justice

STATEMENT

OF

JANE C. HORVATH
CHIEF PRIVACY AND CIVIL LIBERTIES OFFICER

BEFORE THE

SUBCOMMITTEE ON COMMERICAL AND ADMINISTRATIVE LAW
COMMITTEE ON THE JUDICIARY
UNITED STATES HOUSE OF REPRESENTATIVES

CONCERNING

THE PRIVACY AND CIVIL LIBERTIES OFFICE

PRESENTED ON

MAY 17, 2006

Mr. Chairman and Members of the Subcommittee: Thank you for inviting me to testify regarding the Privacy and Civil Liberties Office in connection with the Committee's hearing.

I. THE CHIEF PRIVACY AND CIVIL LIBERTIES OFFICER

In February 2006, the Department created a senior position in the Office of the Deputy Attorney General for a new official who will serve as the Department's Chief Privacy and Civil Liberties Officer. DOJ was well into the hiring process for this position in January when Congress passed the Department of Justice Reauthorization Act of 2005 calling for the Attorney General to designate a senior official in the Department of Justice to assume primary responsibility for privacy policy. The Act provided that the responsibilities of such official shall include advising the Attorney General regarding (1) appropriate privacy protections, relating to the collection, storage, use, disclosure, and security of personally identifiable information, with respect to the Department's existing or proposed information technology and information systems; (2) privacy implications of legislative and regulatory proposals affecting the Department and involving the collection, storage, use, disclosure, and security of personally identifiable information; (3) implementation of policies and procedures, including appropriate training and auditing, to ensure the Department's compliance with privacy-related laws and policies, including the Privacy Act and the E-Government Act of 2002; (4) ensuring that adequate resources and staff are devoted to meeting the Department's privacy-related functions and obligations; (5) appropriate notifications regarding the Department's privacy policies and privacy-related inquiry and complaint procedures; and (6) privacy-related reports from the Department to Congress and the President.

After much discussion within the Department, the decision was made to combine the information privacy and civil liberties protection responsibilities into one position. This is a combination that the Department believes makes sense operationally. I started at the DOJ as the Chief Privacy and Civil Liberties Officer on February 21, 2006. As the Chief Privacy and Civil Liberties Officer, I am responsible for Department wide protection of privacy and civil liberties.

I think it might be helpful to you for me to provide you with a little of my background. Prior to my appointment at DOJ, I started the Washington, D.C. office of Privacy Laws & Business, a privacy consulting firm based in the United Kingdom. My responsibilities focused on advising U.S. companies on conducting their business in Europe in light of the EU Data Protection Directive. I spent six years at America Online, Inc. where I was Assistant General Counsel of America Online, Inc. and General Counsel of Digital City, Inc., a subsidiary of America Online, Inc. I helped draft the first privacy policy for the America Online Service, also one of the first in the industry. In 1996, I was a guest lecturer on protecting the privacy of AOL members at the Association of Attorneys' General Meeting. Prior to working at America Online, I was an Associate at Hogan & Hartson, where my focus was on the representation of high technology clients. I started my legal career at Gibson, Dunn & Crutcher.

Currently the Privacy and Civil Liberties Office is made up of two Senior Counsel from the Office of the Deputy Attorney General, and three experienced Privacy Act attorneys who were formerly with the Office of Information and Privacy. We are in the process of hiring additional staff.

II. RESPONSIBILITIES OF THE PRIVACY AND CIVIL LIBERTIES OFFICE

During my first thirty days at DOJ, we assessed the existing privacy and civil liberties functions at the Department. I met with the Inspector General; the Assistant Attorney General, Office of Legal Policy; Assistant Attorney General, Civil Division; the Chief Information Officer; and the Privacy Officer of the Federal Bureau of Investigation; and many others that had either privacy or civil liberties responsibilities within the Department. At all of these meetings I was welcomed with enthusiasm. I received detailed briefings regarding their privacy and civil liberties efforts. From those meetings we were able to develop an action plan for the Office of Privacy and Civil Liberties.

After meeting with the Chief Information Officer, we decided to centralize the Privacy Impact Assessment (PIA) process. PIAs are required by Section 208 of the E-Government Act for all Federal government agencies that develop or procure new technology involving the collection, maintenance, or dissemination of personally identifiable information; or that make substantial changes to existing technology for managing information in identifiable form. A PIA is an analysis of how personally identifiable information is collected, stored, protected, shared, and managed. (We note that although they are excluded from the statute, we do require PIAs for our national security systems.)

We determined that the PIA process within the Department would be much more effective if all components were working from a standard template with standard guidance. Utilizing some of the aspects of the DHS model, we drafted Official PIA Guidance; a Privacy

Threshold Analysis to determine whether a PIA is required; and a new PIA Template. Next month, we are going to hold a one day training session on PIA preparation and Privacy Act issues with members of the CIO staff and persons within the components who are responsible for Privacy Act issues.

In furtherance of our civil liberties missions, we set up and launched a DOJ Privacy and Civil Liberties Board on April 17, 2006. Representatives of the law enforcement, national security, and other relevant components are represented on the Board. We have subdivided the board into three separate committees: Outreach Committee, Data Committee and the Law Enforcement Committee.

The function of the Outreach Committee is to survey and coordinate existing Departmental outreach efforts with respect to the Arab, Muslim and other ethnic or religious minorities which may be affected by the War on Terrorism. We will also implement additional outreach to these communities as needed. The Data Committee will examine issues related to information privacy within the Department. Its first task will be to respond to recommendations in the April 2006 GAO report entitled *Personal Information Agency and Reseller Adherence to Key Privacy Principles*. Specifically, the committee will analyze the Department's use of information reseller data and propose Departmental policy with regard to such use. Information resellers are companies that collect information, including personal information about consumers, from a wide variety of sources for the purpose of reselling such information to their customers, which includes the Government. The Law Enforcement Committee will focus on law enforcement efforts that might have an impact on civil liberties or privacy. Some members of

the Board sit on multiple committees. The committees will meet once a month, with the entire Board meeting at least twice a year or more often as needed to approve Committee initiatives.

Shortly after I arrived, we started to reach out to privacy advocacy and public policy groups. We have met with representatives from the ACLU, Center for Democracy and Technology, Cato Institute and Heritage Foundation. We have also met with Peter Swire, the former Chief Counselor for Privacy in the U.S. Office of Management and Budget and the Center for Information Policy Leadership at Hunton & Williams LLP. Through these meetings we hope to keep up a dialog with the privacy community.

We have also been active in intergovernmental groups and efforts. We believe that by working together as a group, privacy officers within the Government can utilize each others collective experience. Last week Daniel Suthlerland, Officer for Civil Rights and Civil Liberties at the Department of Homeland Security, hosted an event for privacy and civil liberties officers working in the national security and law enforcement agencies. We are planning to continue these meetings on a monthly basis in order for us to share experiences and ideas. Maureen Cooney, DHS acting Chief Privacy Officer, has asked me to participate at a DHS privacy office workshop in June on Privacy Impact Assessments.

Our office has also been active in advising the Department on information sharing initiatives. While information sharing is an incredibly important initiative for our security, it also involves important privacy and civil liberties issues. We are pleased that the Administration

and the Attorney General has recognized the importance of addressing these issues at the inception of information sharing programs.

Since my arrival, I have co-chaired the President's Information Sharing Environment Guideline 5 Working Group with Alex Joel, the Director of National Intelligence Civil Liberties Protection Officer. The Guideline 5 initiative is in response to the December 16, 2005 Memorandum from President George W. Bush to the Heads of Executive Departments and Agencies, Subject: *Guidelines and Requirements in Support of the Information Sharing Environment*. Guideline 5 of the Memorandum requires, in relevant part, that the Attorney General and the Director of National Intelligence: "(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" and "(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." The working group was comprised of representatives of all of the agencies participating in the ISE. The working group is working to develop the guidelines required under the statute. We also look forward to working with the President's Privacy and Civil Liberties Oversight Board on the guidelines.

The Privacy and Civil Liberties Office also oversees the Department's compliance with the Privacy Act of 1974 and plays an active role in ensuring that the Department's law enforcement, litigation, and anti-terrorism missions are carried out in

accordance with its provisions. This is especially evident in our participation in the Department's Law Enforcement Information Sharing Program, in which we serve a vital role in ensuring that information sharing initiatives carried out in our effort to enforce the law are made in a manner that is consistent with the law. We also provide Privacy Act guidance within the Department, both in response to specific inquiries raised by the components and through training programs, drawing on the expertise in Privacy Act case law and analysis that my staff brought to this Office

III. CONCLUSION

Although I have been at DOJ only a short while, my arrival has been greeted with enthusiasm. We have been consulted on numerous initiatives. In the coming year, we hope to launch new efforts, such as more extensive privacy and civil liberties training, that will further the office's mission of protecting the privacy and civil liberties of those who interact with the Department of Justice.

Mr. CANNON. Thank you, Ms. Horvath.
Professor Katzen?

TESTIMONY OF SALLY KATZEN, PROFESSOR, GEORGE MASON UNIVERSITY LAW SCHOOL, ARLINGTON, VA

Ms. KATZEN. Thank you, Mr. Chairman, Ranking Member Watt, other Members of the Committee. I appreciate the invitation for me to testify today, as I did several years ago, about Government policies and practices that implicate privacy.

As the Chairman noted, privacy is one of the hallmarks of our country—cherished, protected, defended throughout our history. Since September 11, 2001, the debate has changed somewhat as the commitment to privacy has often been spoken in the context of national security and the need for combating terrorism. But protecting our privacy and protecting our Nation are not mutually exclusive goals, and our challenge is to protect and defend our country in a way that promotes our core values.

Now, I belabor this point because in the 2 years since I appeared before this Committee, the concern for privacy and what many Americans believe to be invasions of their privacy by the Government has increased rather than decreased. More articles about privacy policies and practices appear more frequently in the press. There are more stories on radio and television, and there is significantly more attention paid to privacy on the Internet than ever before. The time devoted over the last several weeks or months in public discourse to the warrantless wiretaps by the National Security Agency and the decision of some common carriers to release to the Government information about calls made by millions of Americans is a clear indication of Americans' commitment to and concern about privacy.

Given the importance of privacy and its persistence in the national debate, it's somewhat surprising that this Administration has seemed so reluctant to take even minimal steps to address these concerns. For example, one of the subjects of today's hearing is the Privacy Officer at DHS. When I last testified, I spoke in highly favorable terms of the appointment of Ms. Kelly as the first statutorily required privacy official at DHS. I stressed both the beneficial attention that was being paid to privacy concerns and the fact that having a privacy officer at DHS in no way diminished the capacity of the Department to pursue its mission.

Ms. Kelly resigned from DHS last September, and with respect to Ms. Cooney, we have in place an Acting Privacy Officer. The job is hard enough. To be heard in policy decision meetings, to be listened to when red flags are raised about a proposal's privacy implications, to be supported when a hand goes up and says, "Maybe we should reconsider, maybe we should do it differently," that job is not easy even for a tenured employee. It is so much harder for an acting.

There may well be legitimate reasons that there has been a delay in finding and installing Ms. Kelly's replacement, but the unexpected and unexplained delay raises unfortunate questions. Is it a lack of interest? Is it a lack of support by the Secretary of DHS or by the White House?

In the same vein, I would mention that it has taken a very long time for the White House to nominate and have the Senate confirm the members of the Privacy and Civil Liberties Board which Ms. Horvath spoke about. That, too, was set up by an Act of Congress which was responding to legitimate questions and concerns about Government policies.

In light of these examples, I would call for more oversight by Congress and, equally more important, more legislation concerning and empowering officials in the Government. In my written testimony, I remind the Committee that I had urged that there be statutory privacy officers at all major departments. I am pleased that the Department of Justice now has one. I hope that you will work with other Members of Congress and other Committees to expand that base. And without being too pushy, I would again renew my suggestion that the Committee support establishing at OMB a statutory office headed by a Chief Counselor for Privacy. Such an office was created and staffed during the Clinton administration, and it served us well. The current Administration chose not to fill that position when they took office or since. As a result, there is no senior official in the Executive Office of the President who has privacy in his or her title or who is charged with oversight of Federal privacy policies. Yet it's so much better to have privacy considered at the outset rather than after the plans are implemented and the stories appear on the front pages.

My time is running. I have comments about the markup. Otherwise, I think it's a great bill in many respects. I support the concept. And maybe during the questions and answers I could speak to that.

I want to thank you again for asking me to participate.

[The prepared statement of Ms. Katzen follows:]

PREPARED STATEMENT OF SALLY KATZEN

Mr. Chairman and other Members of the Committee. Thank you for inviting me to testify today on a subject—"Privacy in the Hands of the Government"—that is exceedingly important to the American public and on which this Committee has commendably been actively engaged.

This hearing is a follow on to one at which I testified on February 10, 2004. With the permission of the Committee, I would request that the written testimony that I prepared then be appended to my submission for this hearing; much of the background and analysis presented in that document remain pertinent today and incorporating it by reference will enable me to better focus on more recent developments.

I have been involved in privacy policy and practices for well over a decade, having served as the Administrator of the Office of Information and Regulatory Affairs (OIRA) in the Office of Management and Budget (OMB) from 1993 to 1998 and as the Chair of the Information Policy Committee of the National Information Infrastructure Task Force, which produced, among other things, a revision of the 1973 Code of Fair Information Practices, entitled "Principles for Providing and Using Personal Information." During my later tenure as Deputy Director of the National Economic Council and then as Deputy Director for Management at OMB, I was involved in a series of privacy issues, any my interest in the subject has continued during my years in academics.

My earlier testimony spoke to the importance of privacy in our history and culture, and why I believe that privacy is one of the hallmarks of America—cherished, protected and defended throughout our country and throughout the years.

The arrival of the Information Age raised privacy concerns to a new level, although after September 11, 2001, this was tempered by a clear recognition of the importance of security and the need for combating terrorism. But protecting our privacy and protecting our nation are not mutually exclusive goals. Rather, the challenge for all of us is to protect and defend our country in a way that preserves and promotes our core values.

I belabor this point because in the two years since I appeared before this Committee, the concern for privacy (and what many Americans believe to be invasions of their privacy) has increased rather than decreased. More articles about privacy policies and practices appear more frequently in the press, there are more stories on the radio and television, and there is significantly more attention paid to privacy on the Internet than ever before. The time devoted over the last several weeks/months in public discourse to the warrantless wiretaps by the National Security Agency and the decision of some common carriers to release to the government information about calls made by millions of Americans is a clear indication of Americans' continued commitment to, and concern about, privacy.

Given the importance of privacy and its persistence in the national debate, it is somewhat surprising that this Administration has seemed to be so reluctant to take even minimal steps to address these concerns. For example, when I last testified, I spoke of the generally highly favorable reactions to the tenure of Nuala O'Connor Kelly as the first statutorily required privacy official at the Department of Homeland Security (DHS). I stressed both the beneficial attention that was paid to privacy concerns and the fact that having a privacy officer at DHS in no way diminished the capacity of the Department to pursue its mission. Ms. Kelly resigned from DHS many months ago, and regrettably there is only an Acting privacy officer in place. Is it a lack of interest or a lack of support for the position by the current Secretary of DHS? Or by the White House? There may well be legitimate problems in finding and installing Ms. Kelly's replacement, but the unexplained delay sends a very bad signal to those who follow these developments as an indication of the Administration's commitment to privacy. In that same vein, it is worth noting that it took the longest time for the White House to nominate and have the Senate confirm the members of the Privacy and Civil Liberties Board, which is a committee established by another act of Congress designed to respond to what were perceived as legitimate questions and concerns about government policies with respect to privacy.

In light of these examples, I would call for more oversight by the Congress and, equally important, more legislation creating and empowering officials in the government with responsibility for privacy policy. I had urged in my earlier testimony that the Committee consider expanding the number of statutory privacy offices from one to 24, covering all major Departments (the so-called Chief Financial Officers Act agencies) or at least a handful of critical agencies, including the Department of Justice, the Department of the Treasury (and the Internal Revenue Service), the Department of Defense and the Veterans Administration, the Social Security Administration, and the Department of Health and Human Services. I was pleased when Congress enacted legislation establishing a privacy officer at the Department of Justice. With respect, I would again urge this Committee to work with others in the Congress to expand on this base. OMB guidance from two administrations (issued first during the Clinton Administration and repeated several years ago by the Bush Administration) has called for the creation of such offices in Executive Branch agencies. The imprimatur of Congress would enhance the influence and respect that these officers have within their Departments. Equally important, by establishing statutory privacy offices, the Congress would be able to engage in systematic oversight of the attention paid to this important value in the federal government.

I would also renew my suggestion that Congress establish at OMB a statutory office headed by a Chief Counselor for Privacy. Such an office was created and staffed during the Clinton Administration, and it served us well. The current Administration chose not to fill the position when they took office or since. As a result, there is no senior official in the Executive Office of the President who has "privacy" in his/her title or who is charged with oversight of federal privacy practices, monitoring of interagency processes where privacy is implicated, or developing national privacy polices. Yet it is so much better to have privacy implications considered beforehand—in the formulation of program or projects—rather than after the plans are implemented and the stories about them begin to appear on the front pages of the national newspapers. And apart from damage control, having someone on the "inside" addressing these issues may provide some brakes on the runaway train of surveillance.

Finally, I understand that after this hearing, the Committee will move to mark up H.R. 2840, the "Federal Agency Protection of Privacy Act of 2005." That bill reflects a commendable desire to ensure that privacy impact statements are prepared by federal agencies as they develop regulations that involve the collection of personal information. Several thoughts occurred to me as I was rereading the text for today's hearing.

First, Subsection (c) provides that an agency head may waive the requirements for a privacy impact statement "for national security reasons, or to protect from dis-

closure classified information, confidential commercial information, or information the disclosure of which may adversely affect a law enforcement effort . . ." Apart from the fact that the basis for a waiver goes well beyond national security, I recalled that there is a similar provision in the E-Government Act of 2002, which requires a privacy impact assessment for new federal government computer systems, but instead of giving an essentially free pass for national security concerns, Section 208 (b) (1) (D) of that Act requires the agency to provide the privacy impact assessment to the Director of OMB. I would recommend that such a provision be included in H.R. 2840 and, in addition, that the bill provide that a copy of the analysis be sent to the Congressional Intelligence Committees in the case of national security waivers and the Congressional Judiciary Committees in the case of law enforcement related waivers. In that way, there could be government-wide Executive Branch oversight and, equally important, Congressional oversight over agency decision-making in this area.

Second, the provisions of H.R. 2840 requiring an agency to prepare a plan for, and carry out, a periodic review of existing regulations that have a significant privacy impact on individuals or a privacy impact on a significant number of individuals are quire detailed and quite prescriptive. Rather than specifying all of the factors to be considered, and the timetable and procedures for each element of the review, it might be preferable to set forth un the bill the objectives of a periodic review and task OMB with providing guidance for the agencies as to how they should proceed. In this way, the terms are not cast in concrete but can be more readily adjusted as changes occur, either with respect to content or with respect to technology.

With those modest suggestions, I would endorse the bill and once again commend this Committee for its effective and persistent leadership on these very important issues.

Again, thank you for inviting me to testify today. I would be pleased to elaborate on these comments or answer any questions that you may have.

ATTACHMENT

PREPARED STATEMENT OF SALLY KATZEN BEFORE THE COMMITTEE ON THE JUDICIARY, SUBCOMMITTEE ON COMMERCIAL AND ADMINISTRATIVE LAW, ON FEBRUARY 10, 2004 ON "PRIVACY IN THE HANDS OF THE GOVERNMENT: THE PRIVACY OFFICER FOR THE DEPARTMENT OF HOMELAND SECURITY"

Thank you for inviting me to testify today on a vitally important subject—"Privacy in the Hands of the Government." This Committee is to be congratulated, not only for its leadership in creating a statutory Privacy Officer in the Department of Homeland Security (DHS), but also for being vigilant in its oversight of that office.

I am currently a Visiting Professor at the University of Michigan Law School, where one of my courses is a seminar on "Technology Policy in the Information Age"—a significant portion of which is devoted to examining both the government and the private sector's privacy policies and practices. I have been involved in privacy policy for over a decade. In early 1993, I began serving as the Administrator of the Office of Information and Regulatory Affairs (OIRA) in the Office of Management and Budget (OMB); the "I" in OIRA signaled that I was, in effect, the chief information policy official for the federal government. Among other responsibilities, my office was charged with developing federal privacy policies, including implementation of the 1974 Privacy Act. Later in 1993, I was asked to chair the Information Policy Committee of the National Information Infrastructure Task Force, which had been convened by the Vice President and chaired by then Secretary of Commerce Ronald Brown. One of the first deliverables we produced was from my committee's Privacy Working Group—a revision of the 1973 Code of Fair Information Practices, entitled "Principles for Providing and Using Personal Information." During President Clinton's second term, I worked with the Vice President's Domestic Policy Advisor to create a highly visible and effective office for privacy advocacy in OMB; we selected Peter Swire to head that office and be the first Chief Counselor for Privacy, and I worked closely with him when I served as Deputy Director for Management at OMB during the last two years of the Clinton Administration. Since leaving government, I have, as indicated earlier, been teaching both at the graduate and undergraduate level.

Given the Committee's extensive work in this area, it is not necessary to speak at length on the importance of privacy in the history and culture of our country. Nonetheless, to provide context for the comments that follow, I want to be clear that, from my perspective, privacy is one of the core values of what we are as Americans. Whether you trace its roots from the first settlers and the "frontier" mentality

of the early pioneers, or from the legal doctrines that flowed from Justice Brandeis' oft-quoted recognition in the late 19th century of "the right to be let alone," privacy has been one of the hallmarks of America—cherished, prized, protected and defended throughout our country and throughout our history.

The "Information Age" has brought new opportunities to benefit from the free flow of information, but at the same time it has also raised privacy concerns to a new level. Computers and networks can assemble, organize and analyze data from disparate sources at a speed (and with an accuracy) that was unimaginable only a few decades ago. And as the capacity—of both the government and the private sector—to obtain and mine data has increased, Americans have felt more threatened—indeed, alarmed—at the potential for invasion (and exploitation) of their privacy.

Before September 11, 2001, privacy concerns polled off the charts. Since then, there has been a recognition of the importance of security and the need for combating terrorism. But, as the Pew Internet surveys (and others) have found, Americans' commitment to privacy has not diminished, and some would argue (with much force) that if, in protecting our nation, we are not able to preserve a free and open society for our public lives, with commensurate respect for the privacy of our private lives, then the terrorists will have won. For that reason, it was both necessary and desirable in creating a Department of Homeland Security to statutorily require the Secretary to appoint a senior official with primary responsibility for privacy policy. Ms. Kelly was selected for that position and took office about six months ago.

We thus have some—albeit limited—operational experience with the statutory scheme, and it is therefore timely to see what we have learned and what more could (and should) be done by this Committee to be responsive to privacy concerns.

I would draw two lessons from Ms. Kelly's tenure to date at DHS.

First, the existence of a Privacy Officer at DHS, especially someone who comes to the position with extensive knowledge of the issues and practical experience with the federal government, is highly beneficial. We know that some attention is now being paid to privacy concerns and that steps are being taken to advance this important value that might otherwise not have occurred.

Consider the CAPPS II project, in which Ms. Kelly has recently been involved. She inherited a Privacy Act Notice issued last winter that was dreadful. She produced a Second Privacy Act Notice that reflected much more careful thought about citizens' rights and provided more transparency about the process. Regrettably, there was some backsliding: the initial concept was that the information would be used only to combat terrorism, whereas the second Notice indicated that the information would be used not only for terrorism but also for any violation of criminal or immigration law. Also, the document was vague (at best) on an individual's ability to access the data and to have corrections made. And there was more that should have been said about the manner in which the information is processed through the various data bases. But there is no question that the Second Notice was greatly improved from the first.

Ms. Kelly was also involved with the US VISIT program, where she produced a Privacy Impact Analysis (PIA). Some had argued that a PIA was not required because the program did not directly affect American citizens or permanent residents. Nonetheless, to her credit, she prepared and issued a PIA that was quite thoughtful and was well received. Whether one agrees or disagrees with the underlying program, at least we know that someone was engaged in the issues that deserve attention and the product of that effort was released to the public.

As someone outside the government, it is hard to know how influential Ms. Kelly will be if—and it inevitably will happen—there is a direct conflict between what a program office within DHS wants to do and what the Privacy Officer would counsel against for privacy reasons. Effectiveness in this type of position depends on autonomy and authority—that is, on the aggressiveness of the office holder to call attention to potential problems and on support from the top. We may take some comfort from Secretary Ridge's comments; he has said all the right things about supporting the Privacy Officer. But we cannot now know what will happen when the "rubber meets the road."

This Committee, however, can further empower the Privacy Officer, and lay the foundation for remedying any problems that may arise, by maintaining its oversight and inquiring pointedly into how the Department operates. For example, Ms. Kelly (and Secretary Ridge) should be asked at what stage she is alerted to or brought into new initiatives; what avenues are open for her to raise any questions or concerns; and whether the Secretary will be personally involved in resolving any dispute in which she is involved. The timing of the release of the PIA for the US VISIT program suggests that Ms. Kelly may not always be consulted on a timely basis. As I read the E-Government Act of 2002, an agency is to issue a PIA *before it develops or procures* information technology that collects, maintains or disseminates in-

formation that is in an identifiable form. In this instance, the PIA was released much further down the road, when the program was about to go on line. Anything that helps the Privacy Officer become involved in new initiatives at the outset, before there is substantial staff (let alone money) invested in a project, would be highly salutary.

The second lesson that I take from the experience to date with the Privacy Officer at DHS is that there has been no diminution in the capacity of the Department to pursue its mission. Or as a political wag would say, the existence of a Privacy Officer in DHS has not caused the collapse of western civilization as we know it. This is wholly consistent with what most Americans think—that national security and privacy are compatible and are not intrinsically mutually exclusive.

The fact that there is no evidence that the existence, or any activity, of the Privacy Officer has caused DHS to falter leads me to suggest that the Committee consider expanding the number of statutory privacy offices from one to 24, covering all major Departments (the so-called Chief Financial Officers Act agencies) or at least a handful of critical agencies. Imagine the salutary effect that a statutory privacy office could have at the Department of Justice, the Department of the Treasury (and the Internal Revenue Service), the Department of Defense and the Veterans Administration, the Social Security Administration, and the Department of Health and Human Services. All of these agencies already have some form of privacy office in place, although many simply process Privacy Act complaints, requests, notices, etc. and do not involve themselves in the privacy implications of activities undertaken by their agencies. It is significant, I believe, that OMB guidance from two administrations (issued first during the Clinton Administration and repeated recently by the Bush Administration) has called for the creation of such offices in Executive Branch agencies. With the imprimatur of Congress, these offices can achieve the status (and increased influence) and gain the respect that the Privacy Officer has enjoyed at DHS. Equally important, by establishing statutory privacy offices, the Congress will be able to engage in systematic oversight of the attention paid to this important value in the federal government—something which has not occurred before this hearing today.

I hope I do not seem presumptuous to suggest—indeed, strongly urge—one further step: establishing at OMB a statutory office headed by a Chief Counselor for Privacy. As noted above, we had created such a position during the Clinton Administration, and it served us well. Peter Swire, the person we selected to head that office, was able to bring his knowledge, insights, and sensitivity to privacy concerns to a wide range of subjects. In his two years as Chief Counselor, he worked on a number of difficult issues, including privacy policies (and the role of cookies) on government websites, encryption, medical records privacy regulations, use and abuse of social security numbers, and genetic discrimination in federal hiring and promotion decisions, to name just some of the subjects that came from various federal agencies. He was also instrumental in helping us formulate national privacy policies that arose in connection with such matters as the financial modernization bill, proposed legislation to regulate internet privacy, and the European Union's Data Protection Directive.

I believe it is unfortunate that the current Administration has chosen not to fill that position. As a result, there is no senior official in the Executive Office of the President who has "privacy" in his/her title or who is charged with oversight of federal privacy practices, monitoring of interagency processes where privacy is implicated, or developing national privacy polices. Perhaps it was the absence of such a person that led to the Bush Administration's initial lack of support for the designation of a Privacy Officer at the Department of Homeland Security. Perhaps if someone had been appointed to that position, the Administration would not have appeared to be so tone deaf to privacy concerns in connection with the Patriot Act or any number of law enforcement issues that have made headlines over the past several years. An "insider" can provide both institutional memory and sensitivity to counterbalance the unfortunate tendency of some within the government to surveil first and think later. At the least, the appointment of a highly qualified privacy guru at OMB would mean that someone in a senior position, with visibility, would be thinking about these issues before—rather than after—policies are announced.

Finally, I understand that after this Hearing, the Committee will move to mark up H.R. 338, "The Defense of Privacy Act." That bill reflects a commendable desire to ensure that privacy impact statements are prepared by federal agencies as they develop regulations which may have a significant privacy impact on an individual or have a privacy impact on a substantial number of individuals. I was struck in reviewing the E-Government Act of 2002 for this testimony that it requires an agency to prepare a PIA not only before it develops or procures information technology that implicates privacy concerns, but also before the agency initiates a new collec-

tion of information that will use information technology to collect, maintain or disseminate any information in an identifiable form. This law has gone into effect, OMB has already issued guidance on how to prepare the requisite PIAs, and the agencies are learning how to prepare these PIAs using that model. Rather than impose another regime on agencies when they are developing regulations (which are frequently the basis for the information collection requests referenced in the E-Government Act of 2002), it might be preferable to amend the E-Government Act to expand its requirements to apply to regulations that implicate privacy concerns. That approach would have the added benefit of eliminating the inevitable debate over the judicial review provisions of H.R. 338, which go significantly beyond the judicial review provisions of any of the comparable acts (e.g., Reg.Flex., NEPA, Unfunded Mandates, etc.). Lastly, if you were to amend the E-Government Act to include privacy-related regulations, you might also consider including privacy-related legislative proposals from the Administration. As you know, Executive Branch proposals for legislation are reviewed by OMB before they are submitted to the Congress. If there were a Chief Counselor for Privacy at OMB, s/he would be able to provide input for the benefit of the Administration, the Congress and the American people.

Again, thank you for inviting me to testify today. This Committee has been an effective leader on privacy issues, and it is encouraging that you are continuing the effort. I would be pleased to elaborate on these comments or answer any questions that you may have.

Mr. CANNON. Thank you, Professor.

Ms. Koontz?

TESTIMONY OF LINDA KOONTZ, DIRECTOR, INFORMATION MANAGEMENT ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE, WASHINGTON, DC

Ms. KOONTZ. Mr. Chairman and Members of the Subcommittee, I appreciate the opportunity to be here today to discuss key challenges facing Federal privacy officers. As you know, advances in information technology make it easier than ever for the Federal Government to acquire data on individuals, analyze it for a variety of purposes, and share it with other governmental and nongovernmental entities. Further, the demands of the war on terror put additional pressure on agencies to extract as much value as possible from the information available to them, adding to the potential for compromising privacy.

This is the context in which agencies must carry out their critical responsibilities for protecting the privacy rights of individuals in accordance with current law. To do so, many agencies have designated privacy officers to act as focal points. Recently, these positions have gained greater prominence. In response to rising concerns about privacy rights in our electronic age, both legislation and guidance have directed agencies to establish chief privacy officers or to ensure that a senior official takes overall responsibility for information privacy.

Privacy issues have also been at the heart of several studies that the Congress has asked us to perform over the past few years. Our results highlight some of the challenges faced by agencies and privacy officials.

First, compliance with current law has posed challenges. In 2003, we reported that agency compliance with the requirements of the Privacy Act was uneven. Agencies reviewed generally did well with certain aspects of the requirements, such as issuing public notices about systems containing personal information. However, they did less well at others, such as ensuring that information was complete, accurate, relevant, and timely before it was disclosed to a non-Federal organization.

Agency officials told us that they needed more leadership and guidance from the Office of Management and Budget to help them with implementation in a rapidly changing environment. Similarly, agencies have not always complied with the E-Government Act requirement that agencies perform privacy impact assessments, or PIAs, on certain systems containing personal information. Such assessments are important to ensure that information is handled in a way that protects privacy.

Although we have not yet done a comprehensive assessment of agencies' implementation of PIAs, we did determine in recent work on commercial data resellers that many agencies did not perform PIAs on systems that used reseller information because they believe that a PIA was not required.

Privacy officers also face the challenge of ensuring that privacy protections are not compromised by advances in technology. For example, Federal agencies are increasingly using data mining, that is, analyzing large amounts of data to uncover hidden patterns. Initially, this tool was used mostly to detect financial fraud and abuse, but its use has expanded to include purposes such as detecting terrorist threats.

In 2005, in a review of five different data-mining efforts at selected agencies, we reported that these agencies did take many of the steps needed to protect privacy. However, none followed all key procedures. For instance, although they did issue public notices, these notices did not always describe the intended uses of personal information as required.

Another new technology presenting privacy challenges is radio frequency identification, or RFID. This technology uses wireless communications to transmit data and electronically track and store information on tags attached to or embedded in objects. As we reported in 2005, Federal agencies use or propose to use RFID for physical access controls and to track access. For example, DOD uses it to track shipments. Although this kind of inventory control application is not likely to generate privacy concerns, RFID use could raise issues if, for example, people were not aware that the technology is being used and that it could be embedded in items they are carrying and be used to track them.

Agency privacy offices will play a key role in addressing the challenges I have described. They will be instrumental in ensuring that agencies comply with legislative requirements and in ensuring that privacy is fully addressed in agency approaches to new technologies. In addition, chief privacy officers are in a position to work with OMB and other agencies to identify ambiguities and clarify the applicability of privacy requirements. Not least, they can work to increase agency awareness and raise the priority of privacy issues.

That concludes my statement. I would be happy to answer questions at the appropriate time.

[The prepared statement of Ms. Koontz follows:]

PREPARED STATEMENT OF LINDA D. KOONTZ

United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Commercial and Administrative Law, Committee on the Judiciary, House of Representatives

For Release on Delivery
Expected at 2 p.m. EDT
Wednesday, May 17, 2006

PRIVACY

Key Challenges Facing Federal Agencies

Statement of Linda D. Koontz
Director, Information Management Issues

GAO-06-777T

May 17, 2006

GAO
Accountability•Integrity•Reliability

Highlights

Highlights of GAO-06-777T, a testimony before the Subcommittee on Commercial and Administrative Law, Committee on the Judiciary, House of Representatives

PRIVACY

Key Challenges Facing Federal Agencies

Why GAO Did This Study

Advances in information technology make it easier than ever for the federal government to obtain and process personal information about citizens and residents in many ways and for many purposes. To ensure that the privacy rights of individuals are respected, this information must be properly protected in accordance with current law, particularly the Privacy Act and the E-Government Act of 2002. These laws prescribe specific activities that agencies must perform to protect privacy, and the Office of Management and Budget (OMB) has developed guidance on how and in what circumstances agencies are to carry out these activities.

Many agencies designate officials as focal points for privacy-related matters, and increasingly, many have created senior positions, such as chief privacy officer, to assume primary responsibility for privacy policy, as well as dedicated privacy offices.

GAO was asked to testify on key challenges facing agency privacy officers. To address this issue, GAO identified and summarized issues raised in its previous reports on privacy.

What GAO Recommends

Because GAO has already made privacy-related recommendations in the earlier reports described here, it is making no further recommendations at this time.

www.gao.gov/cgi-bin/getrpt?GAO-06-777T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Linda Koontz at (202) 512-6240 or koontzl@gao.gov.

What GAO Found

Agencies and their privacy officers face growing demands in addressing privacy challenges. For example, as GAO reported in 2003, agency compliance with Privacy Act requirements was uneven, owing to ambiguities in guidance, lack of awareness, and lack of priority. While agencies generally did well with certain aspects of the Privacy Act's requirements—such as issuing notices concerning certain systems containing collections of personal information—they did less well at others, such as ensuring that information is complete, accurate, relevant, and timely before it is disclosed to a nonfederal organization. In addition, the E-Gov Act requires that agencies perform privacy impact assessments (PIA) on such information collections. Such assessments are important to ensure, among other things, that information is handled in a way that conforms to privacy requirements. However, in work on commercial data resellers, GAO determined in 2006 that many agencies did not perform PIAs on systems that used reseller information, believing that these were not required. In addition, in public notices on these systems, agencies did not always reveal that information resellers were among the sources to be used. To address such challenges, chief privacy officers can work with officials from OMB and other agencies to identify ambiguities and provide clarifications about the applicability of privacy provisions, such as in situations involving the use of reseller information. In addition, as senior officials, they can increase agency awareness and raise the priority of privacy issues.

Agencies and privacy officers will also face the challenge of ensuring that privacy protections are not compromised by advances in technology. For example, federal agency use of data mining—the analysis of large amounts of data to uncover hidden patterns and relationships—was initially aimed at detecting financial fraud and abuse. Increasingly, however, the use of this tool has expanded to include purposes such as detecting terrorist threats. GAO found in 2005 that agencies employing data mining took many steps needed to protect privacy (such as issuing public notices), but none followed all key procedures (such as including in these notices the intended uses of personal information). Another new technology development presenting privacy challenges is radio frequency identification (RFID), which uses wireless communication to transmit data and thus electronically identify, track, and store information on tags attached to or embedded in objects. GAO reported in 2005 that federal agencies use or propose to use the technology for physical access controls and tracking assets, documents, or materials. For example, the Department of Defense was using RFID to track shipments. Although such applications are not likely to generate privacy concerns, others could, such as the use of RFIDs by the federal government to track the movement of individuals traveling within the United States. Agency privacy offices can serve as a key mechanism for ensuring that privacy is fully addressed in agency approaches to new technologies such as data mining and RFID.

Mr. Chairman and Members of the Subcommittee:

I appreciate the opportunity to be here today to discuss key challenges facing federal agency privacy officers. As the federal government obtains and processes personal information[1] about citizens and residents in increasingly diverse ways and for increasingly sophisticated purposes, it remains critically important that this information be properly protected and the privacy rights of individuals respected. Advances in information technology make it easier than ever for agencies to acquire data on individuals, analyze it for a variety of purposes, and share it with other governmental and nongovernmental entities. Further, the demands of the war on terror put additional pressure on agencies to extract as much value as possible from the information available to them, adding to the potential for compromising privacy. It is in this context that agency privacy officers must continually strive to ensure that the privacy rights of individuals remain adequately respected.

As requested, my statement will focus on key privacy challenges facing agency privacy officers, including those at the Departments of Homeland Security (DHS) and Justice. After a brief summary and discussion of the federal laws and guidance that apply to agency use of personal information, I will discuss the evolution of the role of privacy officials in federal agencies and then highlight key issues they are currently facing.

To address key challenges faced by privacy officers, we identified and summarized issues raised in our previous reports on privacy, including our recent work regarding the federal government's use of personal information from companies known as information resellers.[2] We conducted the work for these reports in accordance

[1] For purposes of this testimony, the term *personal information* encompasses all information associated with an individual, including both identifying and nonidentifying information. *Personally identifying information*, which can be used to locate or identify an individual, includes such things as names, aliases, and agency-assigned case numbers. *Nonidentifying personal information* includes such things as age, education, finances, criminal history, physical attributes, and gender.

[2] GAO, *Personal Information: Agency and Reseller Adherence to Key Privacy Principles*, GAO-06-421, (Washington: D.C.: Apr. 4, 2006).

with generally accepted government auditing standards. To provide additional information on our previous privacy-related work, I have included, as an attachment, a list of pertinent GAO publications.

Results in Brief

Many agencies have designated officials as focal points for privacy-related matters, including, in some agencies, chief privacy officers. Recently, however, these positions have gained greater prominence, as legislation and guidance have directed agencies to establish chief privacy officers or to designate a senior official with overall agencywide responsibility for information privacy issues.

The elevation of privacy officers to senior positions reflects the growing demands that these individuals face in addressing privacy challenges on a day-to-day basis. These challenges include the following:

- Complying with the Privacy Act and the E-Government Act of 2002. These laws prescribe specific activities that agencies must perform to protect privacy, such as such as issuing notices concerning certain systems containing collections of personal information and performing privacy impact assessments. Agency compliance with these requirements has been uneven in the past, owing to ambiguities in guidance, lack of awareness, and lack of priority.
- Ensuring that data mining efforts do not compromise privacy protections. Increased use by federal agencies of data mining—the analysis of large amounts of data to uncover hidden patterns and relationships—has been accompanied by uncertainty regarding privacy requirements and oversight of such systems. As we reported in previous work, the result was that although agencies employing data mining took many steps needed to protect privacy (such as issuing public notices), none followed all key procedures (such as including in these notices the intended uses of personal information).
- Controlling the collection and use of personal information obtained from commercial sources—"information resellers." A major task confronting federal agencies, especially those engaged in antiterrorism tasks, is to ensure that information obtained from

resellers is being appropriately used and protected. In previous work, we reported that agencies were uncertain about the applicability of privacy requirements to this information, which led to inconsistencies in how it was treated.

- Addressing concerns about radio frequency identification technology. This technology uses wireless communication to transmit data and thus electronically identify, track, and store information on tags attached to or embedded in objects. In previous work, we reported that although common applications of this technology (such as inventory control) are not likely to generate privacy concerns, others could, such as its potential use to track the movement of individuals traveling within the United States.

We have made recommendations previously to OMB and agencies to ensure they are adequately addressing privacy issues. As agencies take action, their privacy offices can serve as key mechanisms for ensuring that privacy is fully addressed in agency approaches to collecting, storing, and using personal information, including in new techniques and technologies, such as data mining and others.

Background: Federal Laws and Guidance Govern Use of Personal Information in Federal Agencies

A core function of privacy officers is to ensure that their agencies are in compliance with federal laws. The major requirements for the protection of personal privacy by federal agencies come from two laws, the Privacy Act of 1974 and the E-Government Act of 2002. The Federal Information Security Management Act of 2002 (FISMA) also addresses the protection of personal information in the context of securing federal agency information and information systems.

The Privacy Act places limitations on agencies' collection, disclosure, and use of personal information maintained in systems of records. The act describes a "record" as any item, collection, or grouping of information about an individual that is maintained by an agency and contains his or her name or another personal identifier. It also defines "system of records" as a group of records under the control of any agency from which information is retrieved by the

name of the individual or by an individual identifier. The Privacy Act requires that when agencies establish or make changes to a system of records, they must notify the public by a "system-of-records notice": that is, a notice in the *Federal Register* identifying, among other things, the type of data collected, the types of individuals about whom information is collected, the intended "routine" uses of data, and procedures that individuals can use to review and correct personal information.[3] Among other provisions, the act also requires agencies to define and limit themselves to specific predefined purposes. For example, the act requires that to the greatest extent practicable, personal information should be collected directly from the subject individual when it may affect an individual's rights or benefits under a federal program.

The provisions of the Privacy Act are largely based on a set of principles for protecting the privacy and security of personal information, known as the Fair Information Practices, which were first proposed in 1973 by a U.S. government advisory committee;[4] these principles were intended to address what the committee termed a poor level of protection afforded to privacy under contemporary law. Since that time, the Fair Information Practices have been widely adopted as a standard benchmark for evaluating the adequacy of privacy protections. Attachment 2 contains a summary of the widely used version of the Fair Information Practices adopted by the Organization for Economic Cooperation and Development in 1980.

The E-Government Act of 2002 strives to enhance protection for personal information in government information systems or information collections by requiring that agencies conduct privacy impact assessments (PIA). A PIA is an analysis of how personal information is collected, stored, shared, and managed in a federal

[3] Under the Privacy Act of 1974, the term "routine use" means (with respect to the disclosure of a record) the use of such a record for a purpose that is compatible with the purpose for which it was collected. 5 U.S.C. § 552a(a)(7).

[4] Congress used the committee's final report as a basis for crafting the Privacy Act of 1974. See U.S. Department of Health, Education, and Welfare, *Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (Washington, D.C.: July 1973).

system. More specifically, according to Office of Management and Budget (OMB) guidance,[6] a PIA is an analysis of how information is handled. Specifically, a PIA is to (1) ensure that handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (2) determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (3) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Agencies must conduct PIAs (1) before developing or procuring information technology that collects, maintains, or disseminates information that is in a personally identifiable form; or (2) before initiating any new data collections involving personal information that will be collected, maintained, or disseminated using information technology if the same questions are asked of 10 or more people. To the extent that PIAs are made publicly available,[8] they provide explanations to the public about such things as the information that will be collected, why it is being collected, how it is to be used, and how the system and data will be maintained and protected.

FISMA also addresses the protection of personal information. FISMA defines federal requirements for securing information and information systems that support federal agency operations and assets; it requires agencies to develop agencywide information security programs that extend to contractors and other providers of federal data and systems.[7] Under FISMA, information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction, including controls necessary to preserve authorized

[6] Office of Management and Budget, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, M-03-22 (Sept. 26, 2003).

[8] The E-Government Act requires agencies, if practicable, to make privacy impact assessments publicly available through agency Web sites, publication in the *Federal Register*, or by other means. Pub. L. 107-347, § 208(b)(1)(B)(iii).

[7] FISMA, Title III, E-Government Act of 2002, Pub. L. 107-347 (Dec. 17, 2002).

restrictions on access and disclosure to protect personal privacy, among other things.

OMB is tasked with providing guidance to agencies on how to implement the provisions of the Privacy Act and the E-Government Act and has done so, beginning with guidance on the Privacy Act, issued in 1975.[8] The guidance provides explanations for the various provisions of the law as well as detailed instructions for how to comply. OMB's guidance on implementing the privacy provisions of the E-Government Act of 2002 identifies circumstances under which agencies must conduct PIAs and explains how to conduct them. OMB has also issued guidance on implementing the provisions of FISMA.

Privacy Officers Have Gained Prominence at Several Federal Agencies

While many agencies have had officials designated as focal points for privacy-related matters for some time, these positions have recently gained greater prominence at a number of agencies. A long-standing requirement has been in place for agency chief information officers to be responsible for implementing and enforcing privacy policies, procedures, standards, and guidelines, and for compliance with the Privacy Act.[9] In 2004, we reported that of the 27 major agency chief information officers, 17 were responsible for privacy and 10 were not. In those 10 agencies, privacy was most often the responsibility of the Office of General Counsel and/or various

[8] OMB, "Privacy Act Implementation: Guidelines and Responsibilities," *Federal Register*, Volume 40, Number 132, Part III, pp. 28948–28978 (Washington, D.C.: July 9, 1975). Since the initial Privacy Act guidance of 1975, OMB periodically has published additional guidance. Further information regarding OMB Privacy Act guidance can be found on the OMB Web site at http://www.whitehouse.gov/omb/inforeg/infopoltech.html.

[9] The Paperwork Reduction Act (Pub. L. 96-511), as amended (44 U.S. C. 3506(a)(2) and (3) and 44 U.S.C. 3506(g)).

offices focusing on compliance with the Freedom of Information Act and the Privacy Act.[10]

Steps have been taken recently to highlight the importance of privacy officers in federal agencies. For example, the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act of 2005[11] required each agency covered by the act to have a chief privacy officer responsible for, among other things, "assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of information in identifiable form." Subsequently, in February 2005, OMB issued a memorandum[12] to federal agencies requiring them to designate a senior official with overall agencywide responsibility for information privacy issues. This senior official was to have overall responsibility and accountability for ensuring the agency's implementation of information privacy protections and play a central policy-making role in the agency's development and evaluation of policy proposals relating to the agency's collection, use, sharing, and disclosure of personal information.

Prior to the OMB guidance, several agencies had already designated privacy officials at higher levels. The Internal Revenue Service had been one of the first, establishing its privacy advocate in 1993. In 2001, the Postal Service established a Chief Privacy Officer. More recently, as you know, Section 222 of the Homeland Security Act of 2002 had created the first statutorily required senior privacy official at any federal agency.[13] This law mandated the appointment of a senior official at DHS to assume primary responsibility for privacy policy, including, among other things, assuring that the use of technologies sustains, and does not erode, privacy protections

[10] GAO, *Federal Chief Information Officers: Responsibilities, Reporting Relationships, Tenure, and Challenges*, GAO-04-823 (Washington, D.C.: July 21, 2004).

[11] The Transportation, Treasury, Independent Agencies, and General Government Appropriations Act of 2005, Sec. 552, Division H, Consolidated Appropriations Act of 2005 (Pub. L. 108-447; 118 Stat 3268; 5 U.S.C. 552a note).

[12] OMB, *Designation of Senior Agency Officials for Privacy*, Memorandum M-05-08 (Feb. 11, 2005).

[13] Homeland Security Act of 2002, Pub. L. 107-296, § 222, 116 Stat. 2155.

relating to the use, collection, and disclosure of personal information. Since being established, the DHS Privacy Office created a Data Privacy and Integrity Advisory Committee, made up of experts from the private and non-profit sectors and the academic community, to advise it on issues within DHS that affect individual privacy, as well as data integrity, interoperability, and other privacy-related issues.

Through the Intelligence Reform Act in 2004, Congress expressed more broadly the sense that agencies with law enforcement or anti-terrorism functions should have a privacy and civil liberties officer.[14] In keeping with that, Justice recently announced the appointment of a Chief Privacy and Civil Liberties Officer responsible for reviewing and overseeing the department's privacy operations and complying with privacy laws. Justice has also announced plans to establish an internal Privacy and Civil Liberties Board made up of senior Justice officials to assist in ensuring that the department's activities are carried out in a way that fully protects the privacy and civil liberties of Americans.

Agency Privacy Officers Face a Number of Challenges

The elevation of privacy officers at federal agencies reflects the growing demands that these individuals face in addressing privacy challenges on a day-to-day basis. Among these challenges, several that are prominent include (1) complying with the Privacy Act and the E-Government Act of 2002, (2) ensuring that data mining efforts do not compromise privacy protections, (3) controlling the collection and use of personal information obtained from commercial sources, and (4) addressing concerns about radio frequency identification technology.

[14] P.L. 108-458, sec. 1062 (Dec. 17, 2004).

Complying with the Privacy Act and the E-Government Act of 2002

Although it has been on the books for more than 30 years, the Privacy Act of 1974 continues to pose challenges for federal agencies. In 2003, we reported[15] that agencies generally did well with certain aspects of the Privacy Act's requirements—such as issuing system-of-records notices when required—but did less well at other requirements, such as ensuring that information is complete, accurate, relevant, and timely before it is disclosed to a nonfederal organization. In discussing this uneven compliance, agency officials reported the need for additional OMB leadership and guidance to assist in difficult implementation issues in a rapidly changing environment. For example, officials had questions about the act's applicability to electronic records. Additional issues included the low agency priority given to implementing the act and insufficient employee training on the act.

These are all issues that chief privacy officers could be in a position to address. For example, working in concert with officials from OMB and other agencies, they are in a position to identify ambiguities in guidance and provide clarifications about the applicability of the Privacy Act. Further, the establishment of a chief privacy officer position and its relative seniority within an agency's organizational structure could indicate that an agency places priority on implementing the act. Finally, a chief privacy officer could also serve as a champion for privacy awareness and education across an agency.

The E-Government Act's requirement that agencies conduct PIAs is relatively recent, and we have not yet made a comprehensive assessment of agencies' implementation of this important provision. However, our previous work has highlighted challenges with respect to conduct of these assessments for certain applications. For example, in our work on federal agency use of information resellers,[16] we found that few agency components reported

[15] GAO, *Privacy Act: OMB Leadership Needed to Improve Agency Compliance*, GAO-03-304 (Washington, D.C.; June 30, 2003).

[16] GAO-05-421, p. 59-61.

developing PIAs for their systems or programs that make use of information reseller data. These agencies often did not conduct PIAs because officials did not believe they were required. Current OMB guidance on conducting PIAs is not always clear about when they should be conducted. We concluded that until PIAs are conducted more thoroughly and consistently, the public is likely to remain incompletely informed about the purposes and uses for the information agencies obtain from resellers. We recommended that OMB revise its guidance to clarify the applicability of the E-Gov Act's PIA requirement (as well as Privacy Act requirements) to the use of personal information from resellers.

Compliance with OMB's PIA guidance was also an issue in our review of selected data mining efforts at federal agencies.[17] In that review, although three of the five data mining efforts we assessed had conducted PIAs, none of these assessments fully complied with OMB guidance. Complete assessments are an important tool for agencies to identify areas of noncompliance with federal privacy laws, evaluate risks arising from electronic collection and maintenance of information about individuals, and evaluate protections or alternative processes needed to mitigate the risks identified. Agencies that do not take all the steps required to protect the privacy of personal information limit the ability of individuals to participate in decisions that affect them, as required by law, and risk the improper exposure or alteration of personal information. We recommended that the agencies responsible for the data mining efforts complete or revise PIAs as needed and make them available to the public.

The DHS Privacy Office recently issued detailed guidance on conducting PIAs[18] that may be helpful to departmental components as they develop and implement systems that involved personal information. The guidance notes that PIAs can be one of the most

[17] GAO, *Data Mining: Agencies Have Taken Key Steps to Protect Privacy in Selected Efforts, but Significant Compliance Issues Remain*, GAO-05-866 (Washington, D.C.: Aug. 15, 2005).

[18] Department of Homeland Security Privacy Office, *Privacy Impact Assessments: Official Guidance* (March 2006).

important instruments in establishing trust between the department and the public. As agencies develop or make changes to existing systems that collect personally identifiable information, it will continue to be critical for privacy officers to monitor agency activities and help ensure that PIAs are properly conducted so that their benefits can be realized.

Ensuring that Data Mining Efforts Do Not Compromise Privacy Protections

Many concerns have been raised about the potential for data mining programs at federal agencies to compromise personal privacy. In our May 2004[19] report on federal data mining efforts, we defined data mining as the application of database technology and techniques—such as statistical analysis and modeling—to uncover hidden patterns and subtle relationships in data and to infer rules that allow for the prediction of future results. We based this definition on the most commonly used terms found in a survey of the technical literature. As we noted in our report, mining government and private databases containing personal information raises a range of privacy concerns.

In the government, data mining was initially used to detect financial fraud and abuse. However, its use has greatly expanded. Among other purposes, data mining has been used increasingly as a tool to help detect terrorist threats through the collection and analysis of public and private sector data. Through data mining, agencies can quickly and efficiently obtain information on individuals or groups by exploiting large databases containing personal information aggregated from public and private records. Information can be developed about a specific individual or a group of individuals whose behavior or characteristics fit a specific pattern. The ease with which organizations can use automated systems to gather and analyze large amounts of previously isolated information raises concerns about the impact on personal privacy. Before data aggregation and data mining came into use, personal information contained in paper records stored at widely dispersed locations,

[19] GAO, *Data Mining: Federal Efforts Cover a Wide Range of Uses*, GAO-04-548, (Washington, D.C.: May 4, 2004).

such as courthouses or other government offices, was relatively difficult to gather and analyze.

In August 2005, we reported on five different data mining efforts at selected federal agencies, noting that although the agencies responsible for these data mining efforts took many of the steps needed to protect the privacy and security of personal information used in the efforts, none followed all key procedures.[20] Most of the agencies provided a general public notice about the collection and use of the personal information used in their data mining efforts. However, fewer followed other required steps, such as notifying individuals about the intended uses of their personal information when it was collected or ensuring the security and accuracy of the information used in their data mining efforts. In addition, as I previously mentioned, although three of the five agencies completed privacy impact assessments of their data mining efforts, none fully complied with OMB guidance. We made recommendations to the agencies responsible for the five data mining efforts to ensure that their efforts included adequate privacy and security protections.

In March 2004, an advisory committee chartered by the Department of Defense issued a comprehensive report on privacy concerns regarding data mining in the fight against terrorism.[21] The report made numerous recommendations to better ensure that privacy requirements are clear and stressed that proper oversight be in place when agencies engage in data mining that could include personal information. Agency privacy offices can provide a degree of internal oversight to help ensure that privacy is fully addressed in agency data mining activities.

Controlling the Collection and Use of Personal Information Obtained from Commercial Sources

Recent security breaches at large information resellers, such as ChoicePoint and LexisNexis, have highlighted the extent to which

[20] GAO-05-866.

[21] Technology and Privacy Advisory Committee, *Safeguarding Privacy in the Fight Against Terrorism* (Washington, D.C.: Mar. 1, 2004).

such companies collect and disseminate personal information. Information resellers are companies that collect information, including personal information about consumers, from a wide variety of sources for the purpose of reselling such information to their customers, which include both private-sector businesses and government agencies. Before advanced computerized techniques made aggregating and disseminating such information relatively easy, much personal information was less accessible, being stored in paper-based public records at courthouses and other government offices or in the files of nonpublic businesses. However, information resellers have now amassed extensive amounts of personal information about large numbers of Americans, and federal agencies access this information for a variety of reasons.

A major task confronting federal agencies, especially those engaged in antiterrorism tasks, has been to ensure that information obtained from resellers is being appropriately used and protected. To this end, in September 2005, the DHS Privacy Office held a public workshop to examine the policy, legal, and technology issues associated with the government's use of reseller data for homeland security. Participants provided suggestions on how the government can ensure that privacy is protected while enabling the agencies to analyze reseller data.

We recently testified before this subcommittee on critical issues surrounding the federal government's acquisition and use of personal information from information resellers.[32] In our review of the acquisition of personal information from resellers by DHS, Justice, the Department of State, and the Social Security Administration, agency practices for handling this information did not always reflect the Fair Information Practices. For example, although agencies issued public notices on information collections, these did not always notify the public that information resellers were among the sources to be used, a practice inconsistent with the principle that individuals should be informed about privacy policies and the collection of information. And again, a contributing factor

[32] GAO, *Personal Information: Agencies and Resellers Vary in Providing Protections*, GAO-06-609T (Washington, D.C.: Apr. 4, 2006).

was ambiguities in guidance from OMB regarding the applicability of privacy requirements in this situation. As I mentioned previously, we recommended that OMB revise its guidance to clarify the applicability of governing laws—both the Privacy Act and the E-Gov Act—to the use of personal information from resellers.

In July 2005, we reported on shortcomings at DHS's Transportation Security Administration (TSA) in connection with its test of the use of reseller data for the Secure Flight airline passenger screening program.[28] TSA did not fully disclose to the public its use of personal information in its fall 2004 privacy notices, as required by the Privacy Act. In particular, the public was not made fully aware of, nor had the opportunity to comment on, TSA's use of personal information drawn from commercial sources to test aspects of the Secure Flight program. In September 2004 and November 2004, TSA issued privacy notices in the *Federal Register* that included descriptions of how such information would be used. However, these notices did not fully inform the public before testing began about the procedures that TSA and its contractors would follow for collecting, using, and storing commercial data. In addition, the scope of the data used during commercial data testing was not fully disclosed in the notices. Specifically, a TSA contractor, acting on behalf of the agency, collected more than 100 million commercial data records containing personal information such as name, date of birth, and telephone number without informing the public. As a result of TSA's actions, the public did not receive the full protections of the Privacy Act. In its comments on our findings, DHS stated that it recognized the merits of the issues we raised, and that TSA acted immediately to address them.

In our report on information resellers, we recommended that the Director, OMB, revise privacy guidance to clarify the applicability of requirements for public notices and privacy impact assessments to agency use of personal information from resellers and direct

[28] GAO, *Aviation Security: Transportation Security Administration Did Not Fully Disclose Uses of Personal Information during Secure Flight Program Testing in Initial Privacy Notices, but Has Recently Taken Steps to More Fully Inform the Public*, GAO-05-864R (Washington, D.C.: July 22, 2005).

agencies to review their uses of such information to ensure it is explicitly referenced in privacy notices and assessments. Further, we recommended that agencies develop specific policies for the use of personal information from resellers. Until privacy requirements are better defined and broadly understood, agency privacy officers are likely to continue to face challenges in helping ensure that their agencies are providing appropriate privacy protections.

Addressing Concerns about Radio Frequency Identification Technology

Specific issues about the design and content of identity cards also raise broader privacy concerns associated with the adoption of new technologies such as radio frequency identification (RFID). RFID is an automated data-capture technology that can be used to electronically identify, track, and store information contained on a tag. The tag can be attached to or embedded in the object to be identified, such as a product, case, or pallet. RFID technology provides identification and tracking capabilities by using wireless communication to transmit data. In May 2005, we reported that major initiatives at federal agencies that use or propose to use the technology included physical access controls and tracking assets, documents, or materials.[24] For example, DHS was using RFID to track and identify assets, weapons, and baggage on flights. The Department of Defense was also using it to track shipments.

In our May 2005 report we identified several privacy issues related to both commercial and federal use of RFID technology. Among these privacy issues are notifying individuals of the existence or use of the technology; tracking an individual's movements; profiling an individual's habits, tastes, or predilections; and allowing for secondary uses of information.[25] The extent and nature of the privacy issues depends on the specific proposed use. For example, using the technology for generic inventory control would not likely generate substantial privacy concerns. However, the use of RFIDs

[24] GAO, *Information Security: Radio Frequency Identification Technology in the Federal Government*, GAO-05-551 (Washington, D.C.: May 27, 2005).

[25] For information on the practices and tools to mitigate these privacy issues, see GAO-05-551, pp. 22–24.

by the federal government to track the movement of individuals traveling within the United States could generate concern by the affected parties.

A number of specific privacy issues can arise from RFID use. For example, individuals may not be aware that the technology is being used and that it could be embedded in items they are carrying and thus used to track them. Three agencies indicated to us that employing the technology would allow for the tracking of employees' movements. Tracking is real-time or near-real-time surveillance in which a person's movements are followed through RFID scanning. Media reports have described concerns about ways in which anonymity is likely to be undermined by surveillance. Further, public surveys have identified a distinct unease with the potential ability of the federal government to monitor individuals' movements and transactions.[26] Like tracking, profiling—the reconstruction of a person's movements or transactions over a specific period of time, usually to ascertain something about the individual's habits, tastes, or predilections—could also be undertaken through the use of RFID technology. Because tags can contain unique identifiers, once a tagged item is associated with a particular individual, personally identifiable information can be obtained and then aggregated to develop a profile of the individual. Both tracking and profiling can compromise an individual's privacy and anonymity.

Concerns also have been raised that organizations could develop secondary uses for the information gleaned through RFID technology; this has been referred to as "mission-" or "function-creep." The history of the Social Security number, for example, gives ample evidence of how an identifier developed for one specific use has become a mainstay of identification for many other purposes, governmental and nongovernmental.[27] Secondary uses of the Social

[26] GAO, *Technology Assessment: Using Biometrics for Border Security*, GAO-03-174 (Washington, D.C.: Nov. 15, 2002).

[27] GAO, *Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards*, GAO-02-352 (Washington, D.C.: May 31, 2002).

Security number have been a matter not of technical controls but rather of changing policy and administrative priorities.

As agencies take advantage of the benefits of RFID technology and implement it more widely, it will be critical for privacy officers to help ensure that a full consideration is made of potential privacy issues, both short-term and long-term, as the technology is implemented.

In summary, privacy officers at federal agencies face a range of challenges in working to ensure that individual privacy is protected, and today I have discussed several of them. It is clear that advances in technology can present both opportunities for greater agency efficiency and effectiveness as well as the danger, if unaddressed, of eroding important privacy protections. Technological advances also mean there is a need to keep governmentwide privacy guidance up-to-date, and agency privacy officers will depend on OMB for leadership in this area. Even without a consideration of technological evolution, privacy officers need to be vigilant to ensure that agency officials are continually mindful of their privacy responsibilities. Fortunately, tools are available—including the requirements for PIAs and Privacy Act public notices—that can help ensure that the right operational decisions are made about the acquisition, use, and storage of personal information. By using these tools effectively, agencies have the opportunity to gain greater public confidence that their actions are in the best interests of all Americans.

Mr. Chairman, this concludes my testimony today. I would happy to answer any questions you or other members of the subcommittee may have.

Contacts and Acknowledgements

If you have any questions concerning this testimony, please contact Linda Koontz, Director, Information Management, at (202) 512-6240, or koontzl@gao.gov. Other individuals who made key contributions

include Barbara Collier, John de Ferrari, David Plocher, and Jamie Pressman.

Attachment I: Selected GAO Products Related to Privacy Issues

Personal Information: Agencies and Resellers Vary in Providing Privacy Protections. GAO-06-609T. Washington, D.C.: April 4, 2006.

Personal Information: Agency and Reseller Adherence to Key Privacy Principles. GAO-06-421. Washington, D.C.: April 4, 2006.

Data Mining: Agencies Have Taken Key Steps to Protect Privacy in Selected Efforts, but Significant Compliance Issues Remain. GAO-05-866. Washington, D.C.: August 15, 2005.

Aviation Security: Transportation Security Administration Did Not Fully Disclose Uses of Personal Information during Secure Flight Program Testing in Initial Privacy Notices, but Has Recently Taken Steps to More Fully Inform the Public. GAO-05-864R. Washington, D.C.: July 22, 2005.

Identity Theft: Some Outreach Efforts to Promote Awareness of New Consumer Rights are Under Way. GAO-05-710. Washington, D.C.: June 30, 2005.

Information Security: Radio Frequency Identification Technology in the Federal Government. GAO-05-551. Washington, D.C.: May 27, 2005.

Aviation Security: Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System is Further Developed. GAO-05-356. Washington, D.C.: March 28, 2005.

Electronic Government: Federal Agencies Have Made Progress Implementing the E-Government Act of 2002. GAO-05-12. Washington, D.C.: December 10, 2004.

Social Security Numbers: Governments Could Do More to Reduce Display in Public Records and on Identity Cards. GAO-05-59. Washington, D.C.: November 9, 2004.

Federal Chief Information Officers: Responsibilities, Reporting Relationships, Tenure, and Challenges, GAO-04-823. Washington, D.C.: July 21, 2004.

Data Mining: Federal Efforts Cover a Wide Range of Uses, GAO-04-548. Washington, D.C.: May 4, 2004.

Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges. GAO-04-385. Washington, D.C.: February 12, 2004.

Privacy Act: OMB Leadership Needed to Improve Agency Compliance. GAO-03-304. Washington, D.C.: June 30, 2003.

Data Mining: Results and Challenges for Government Programs, Audits, and Investigations. GAO-03-591T. Washington, D.C.: March 25, 2003.

Technology Assessment: Using Biometrics for Border Security. GAO-03-174. Washington, D.C.: November 15, 2002.

Information Management: Selected Agencies' Handling of Personal Information. GAO-02-1058. Washington, D.C.: September 30, 2002.

Identity Theft: Greater Awareness and Use of Existing Data Are Needed. GAO-02-766. Washington, D.C.: June 28, 2002.

Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards. GAO-02-352. Washington, D.C.: May 31, 2002.

Attachment 2: The Fair Information Practices

The Fair Information Practices are not precise legal requirements. Rather, they provide a framework of principles for balancing the need for privacy with other public policy interests, such as national security, law enforcement, and administrative efficiency. Ways to strike that balance vary among countries and according to the type of information under consideration. The version of the Fair Information Practices shown in table 1 was issued by the Organization for Economic Cooperation and Development (OECD) in 1980[28] and has been widely adopted.

Table 1: The Fair Information Practices

Principle	Description
Collection limitation	The collection of personal information should be limited, should be obtained by lawful and fair means, and, where appropriate, with the knowledge or consent of the individual.
Data quality	Personal information should be relevant to the purpose for which it is collected, and should be accurate, complete, and current as needed for that purpose.
Purpose specification	The purposes for the collection of personal information should be disclosed before collection and upon any change to that purpose, and its use should be limited to those purposes and compatible purposes.
Use limitation	Personal information should not be disclosed or otherwise used for other than a specified purpose without consent of the individual or legal authority.
Security safeguards	Personal information should be protected with reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification, or disclosure.
Openness	The public should be informed about privacy policies and practices, and individuals should have ready means of learning about the use of personal information.

[28] OECD, *Guidelines on the Protection of Privacy and Transborder Flow of Personal Data* (Sept. 23, 1980). The OECD plays a prominent role in fostering good governance in the public service and in corporate activity among its 30 member countries. It produces internationally agreed-upon instruments, decisions, and recommendations to promote rules in areas where multilateral agreement is necessary for individual countries to make progress in the global economy.

Principle	Description
Individual participation	Individuals should have the following rights: to know about the collection of personal information, to access that information, to request correction, and to challenge the denial of those rights.
Accountability	Individuals controlling the collection or use of personal information should be accountable for taking steps to ensure the implementation of these principles.

Source: Organization for Economic Cooperation and Development.

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON RECYCLED PAPER

Mr. CANNON. Thank you, Ms. Koontz.

I just need to point out that we just had a panel of four participants who all finished within seconds of the 5 minutes. I have never seen that before in my life. Obviously, we have some well-experienced panelists.

We have a significant problem here. We are going to try and mark this bill up today, and we have six votes probably between 2:45 and 3:15. And so—yeah, we'll have six votes, so that means that—let me just suggest that I'm not going to ask questions, and all the Members of the panel can ask written questions.

Professor, I suspect you have your comments already written, and if you could submit those. You suggested you had more that you wanted to say. Do you have that in written form already?

Ms. KATZEN. Yes, Mr. Chairman. My written testimony includes two modest suggestions, one of which relates to the national security issue, and I think it is important.

Mr. CANNON. Thank you. And if any of the panelists have other things you would like to make part of the record, we'll leave the record open for 5 days.

So I ask unanimous consent that the Members of the panel—that we limit questioning to 3 minutes for the panel. Hearing no objection, so ordered.

Mr. WATT. That is per Member?

Mr. CANNON. That is per Member, yes. Pardon me. Hearing no objection, but with that clarification, so ordered. And we'll keep the legislative record open for 5 days for questions. Without objection, so ordered.

Thank you, and, Mr. Watt, you are recognized for 5 minutes.

Mr. WATT. For 3 minutes—3 minutes, I presume. Thank you, sir.

Since we're going on to the markup of H.R. 2840 and all of the witnesses heard my opening comments, I guess the most appropriate question I could ask in my short period of time is to Ms. Cooney and Ms. Horvath, since you all are here representing the Administration, or at least your respective Departments.

Do you have a clue whether the Administration really supports and wants this bill? Because they haven't done anything to try to get it passed that I'm aware of on the Senate side, and we're engaging in a futile gesture here passing it out of here without the Administration injecting itself and saying it wants it.

So does either of you know whether the Administration really wants this bill?

Ms. COONEY. Mr. Watt, I'd be happy to answer. I don't know of a formal position that the Administration has taken on this bill. I'm not aware of one. I think in our last appearance I did mention that under section 222 we have very similar requirements at DHS to do PIAs on rulemakings, and we've been able to tackle that effort and can improve on it as we——

Mr. WATT. But this is a systemwide, governmentwide bill, not a DHS bill. So I guess the question I'm asking is: Is the Administration committed to having this done systemwide, or are they not? If you don't know, I mean, just say you don't know.

Ms. COONEY. I know of no formal position on it.

Mr. WATT. Okay. I assume you don't know either, Ms. Koontz. You're not here—you're kind of in a different position with respect

to the Administration. I understand that. Have you heard anything through the grapevine about whether the Administration wants it, Professor Katzen?

Ms. KATZEN. No.

Mr. WATT. Okay. All right. I just keep pointing out that, you know, we've marked this bill up several times. It's gone. The Chairman indicated it went out of the House. Without the Administration doing something to lift a finger to get it, it ain't going to happen. So we might be back here again next term of Congress doing the same thing.

I yield back.

Mr. CANNON. Thank you.

I think Mr. Franks—the gentleman is recognized for 3 minutes.

Mr. FRANKS. Mr. Chairman, I have no questions at this time.

Mr. CANNON. Thank you, Mr. Franks. We appreciate that candor and directness, and I think—the gentleman from Massachusetts, Mr. Delahunt, is recognized for 3 minutes.

Mr. DELAHUNT. Yes, thank you, Mr. Chairman. I'm going to make an effort to answer Mr. Watt's question. I think it's clear to me that the Administration—this is not a priority, I think it's fair to say, for the Administration. Otherwise, this bill would have been enacted into law last year. And I think it's time, particularly given the context of recent revelations concerning the NSA in particular that the Administration weigh in in a very significant way. If this bill is to pass, the Administration has to make it a priority. And I don't think any of us—and I think I speak for all of us on this panel right now—have not seen evidence of the Administration making it the kind of priority that I think it deserves.

As my colleagues would remember, myself and Mr. Berman had an amendment to the PATRIOT Act involving data mining, and there was great resistance from the Department of Justice regarding that particular amendment, which I believed to be somewhat innocuous. Well, now I understand better, after reading the USA Today and other revelations that occurred prior to that why there would be such resistance. This is simply an opportunity for the American people to find out what their Government was doing.

I have to agree with you, Professor Katzen. You know, when there's a lack of privacy afforded the individual citizen, we're on our way to eroding democracy and living I a totalitarian society. It's absolutely essential that this bill becomes a priority.

Mr. CANNON. Would the gentleman yield?

Mr. DELAHUNT. I yield.

Mr. CANNON. Because I agree with the gentleman. Let me just point out that it is our obligation as the Legislature to set the limits and set the priorities here, and we have to do that as Republicans and Democrats and as the House and the Senate. That's sometimes hard. This Administration—no Administration is going to focus on these issues like we do because our perspective is different, and so I pledge to the gentleman that we will——

Mr. DELAHUNT. I appreciate that, and I would even request—the flip side, Mr. Chairman, is the lack of transparency, secrecy, if you will, that I would suggest has been an earmark of this Administration. We've had the National Archivist, Mr. Leonard, complain about the ubiquitous classification of public documents that is

going on. And I would hope that you would consider having a hearing into that particular issue. I think that is something that is warranted, particularly given——

Mr. CANNON. I'd be happy to speak with the gentleman, whose time has expired.

May I ask unanimous consent that we not continue with questions, since we just had a vote called, and that we move over to the markup of this bill? Thank you.

[Whereupon, at 2:48 p.m., the Subcommittee proceeded to other business.]

APPENDIX

Material Submitted for the Hearing Record

RESPONSE TO POST-HEARING QUESTIONS FROM MAUREEN COONEY, ACTING CHIEF PRIVACY OFFICER, U.S. DEPARTMENT OF HOMELAND SECURITY, WASHINGTON, DC

Questions for the Record
House Judiciary Commercial and Administrative Law Subcommittee
Privacy in the Hands of the Government: The Privacy Officer for the Department of Homeland Security
May 17, 2006
Acting Chief Privacy Officer Maureen Cooney

Questions from Representative Chris Cannon

1. According to your testimony, you have been serving as the Acting Chief Privacy Officer for the past eight months.

   - What accounts for the apparent delay in finding a permanent Chief Privacy Officer?

Response: The Department has made a decision to fill the position. In the interim, the Privacy Office and the broader network of component privacy officers and privacy and Freedom of Information Act specialists, some 430 strong, have continued conducting business as usual with the full support of DHS leadership.

   - When is it likely that a permanent replacement will be named to your position?

Response: The Department made an announcement on July 21, 2006.

2. Section 222 of the Homeland Security Act of 2002[1] requires your office to file an annual report with Congress. To date, however, it appears that only one report has submitted to Congress. Please explain.

Response: During the transition, I concluded that it might be best to cover as many of our activities as possible and to incorporate those that have occurred to date. To do that, we have expanded our coverage to encompass the past 24 months of our work. I hope that the final result will be worth the wait, as the Privacy Office has undertaken many initiatives to inculcate a culture of privacy within the agency and to work with our partners, both at home and abroad, to foster the respectful use of personally identifiable information for homeland security purposes. We will work to ensure future reports are submitted annually. Separately, we have published a quarterly newsletter, *Privacy Matters*, and distributed it to Congress for current updates on Privacy Office and DHS privacy-related activities.

3. What are the major achievements of the Department of Homeland Security Privacy Office to date?

Response: I highlighted some of these in my testimony before the Subcommittee and they will be covered in detail in our annual report, but they include a successful audit of DHS compliance with the requirements of the Passenger Name Record Agreement that was negotiated with the European Union, several highly successful and well-attended public workshops on current privacy issues, active participation in the development of privacy protocols for the Information Sharing Environment, collaboration within DHS to help build privacy into our programs, such as Secure Flight and other screening efforts, outreach to international partners through participation in working groups and assistance in developing appropriate international information sharing

[1] Pub. L. No. 107-296, § 222, 116 Stat. 2135, 2155 (2002).

agreements, establishment and administrative participation in the work of the Data Privacy and Integrity Advisory Committee, which advises our office and the Secretary on privacy issues, and analysis and reporting on data mining projects, the MATRIX Program, and the privacy and civil liberties implications of the "No-Fly" lists.

4. Does your office have sufficient funding and workforce resources?

Response: It takes a significant amount of resources to conduct any successful privacy program, and the Privacy Office has fully utilized its funding and workforce resources. Additionally, we have leveraged DHS resources and partnerships throughout the Department's components to ensure privacy policies and procedures are incorporated into DHS programs and systems.

- Are all positions filled?

Response: We have interviewed for the four new positions created as a result of the 2006 appropriations. Three of the positions are filled – a Senior Advisor for Privacy Technology, a job-share between two individuals who will be International Privacy Specialists, and a Privacy Compliance Specialist with an emphasis on Privacy Impact Assessment coordination. We have a current offer outstanding for another Privacy Compliance Specialist whose work will focus on privacy audits.

- How many employees does your office currently have?

Response: We have 16 FTEs, 12 of which are filled, and 13 contractors.

5. What are some of the biggest challenges that the Department of Homeland Security Privacy Office has encountered?

Response: Perhaps our biggest challenge is to build a culture of privacy into the entirety of the Department; however, I cannot overstate the importance of the oversight function of the Privacy Office in ensuring consistent and uniform implementation of privacy policy throughout the Department. So, although this may be our biggest challenge it is one that we are working on successfully. We believe that the Privacy Office's standardized operational approach to privacy allows the Department to respond to citizens' concerns about Department activities and creates real tangible results in the protection of our citizens' privacy.

6. Has your office encountered any lack of cooperation or recalcitrance from other components in the Department of Homeland Security?

Response: The Privacy Office works hard to be a good partner to all DHS programs and component offices, to assist our colleagues in building privacy into their initiatives. In general, we enjoy good relations across the agency.

Questions for the Record
House Judiciary Commercial and Administrative Law Subcommittee
Privacy in the Hands of the Government: The Privacy Officer for the Department of Homeland Security
May 17, 2006
Acting Chief Privacy Officer Maureen Cooney

7. What is your response to those who question your office's independence?

Response: The DHS Privacy Office's status as a direct report to the Secretary permits it to be a committed partner but one unafraid to cast a critical eye on initiatives if we believe that further steps should be taken to assure that the use of technologies sustain and do not erode privacy protections. I believe our published reports demonstrate the success we have had in achieving our mission.

8. How do you respond to those who believe that privacy protections may undermine law enforcement and antiterrorism endeavors?

Response: Privacy and security are not mutually exclusive goals, and the overall message that our office works to convey, internally as well as externally, is that we can and must achieve both if we are to preserve our way of life. This is a message that resonates with the Secretary, who has said that "we want to build security regimes that maximize privacy protection and that do it in a thoughtful and intelligent way," that is reflected in our strategic goals as an agency, and that is at the heart of our mission. No less an authority than the National Commission on Terrorists Attacks Upon the United States has opined that "the choice between security and liberty is a false choice," and this is a message that must guide all of us as we pursue our homeland security mission.

9. Does the statute that created your position provide sufficient guidance and direction?

Response: Yes. Our enabling statute, which includes reporting requirements on privacy violations, implementation of the Privacy Act, internal controls and other matters, ensures that we have the opportunity to work on the full range of privacy issues at DHS. The office has sufficient guidance and direction.

10. To what extent do you coordinate with privacy officers in other agencies? Are there shared problems/solutions?

Response: Since its inception, our office has been the leader on privacy matters and we coordinate with privacy officers in other agencies on a regular basis, through formal meetings, our workshops and through individual contacts. Because privacy requirements for federal agencies are consistent across agencies, we have been able to share our expertise and insights with privacy officers in many other departments, and, in turn, have benefited in our own work from their experiences. In particular, I am pleased to have developed a strong working relationship with the Privacy and Civil Liberties Offices for the Department of Justice and the Director of National Intelligence, along with the White House Privacy and Civil Liberties Oversight Board. We plan to work closely together as an executive branch-wide structure to ensure that privacy and civil liberties are adequately considered in the design, implementation and management of policy and programs.

Questions for the Record
House Judiciary Commercial and Administrative Law Subcommittee
Privacy in the Hands of the Government: The Privacy Officer for the Department of Homeland Security
May 17, 2006
Acting Chief Privacy Officer Maureen Cooney

RESPONSE TO POST-HEARING QUESTIONS FROM SALLY KATZEN, PROFESSOR, GEORGE MASON UNIVERSITY LAW SCHOOL, ARLINGTON, VA

Responses to Questions Submitted to Professor Sally Katzen by Subcommittee Members

1. What are the biggest challenges that federal privacy officers must address?

The biggest challenges that agency privacy officers face are first, getting a seat at the table with senior agency policy officials as policies or programs are being formulated, and second, being heard (and supported) when they raise privacy implications about high priority proposals. Too often, privacy officers are seen as simply administrators of the Privacy Act and other pertinent laws, whereas they are a source of expertise and experience which the agency should take advantage of when establishing and implementing all agency activities.

2. Please describe the pros and cons of having a chief privacy officer appointed within the Office of Management and Budget.

As I mentioned in my testimony, appointing a chief privacy officer in OMB would not only be an official recognition of the importance of privacy concerns in national policy debates, but also there would be someone in the Executive Office of the President with "privacy" in his or her title who would be charged with oversight of federal privacy practices, developing national privacy polices, and monitoring of interagency processes where privacy is implicated. In a world of information sharing, many privacy issues affect multiple federal agencies. As you know, OMB plays a critical role in clearance of Executive Branch actions – e.g., executive orders, regulations, proposed legislation, etc. – and a chief privacy officer within OMB would be able to be involved in all of these multi-agency activities. In addition, a chief privacy officer within OMB would serve as a natural focus for government-wide coordination, expertise, and training, as well as being an identifiable point of contact for industry, privacy advocates, international privacy officers and other interested persons.

I can think of no disadvantages to appointing a chief privacy officer within OMB.

3. You argue that every agency should have statutory privacy officer. Is there an economic price tag that would accompany such a sweeping mandate?

The additional cost of creating statutory privacy officers is virtually nil, whereas the cost of not adopting the suggestion may be huge.

To explain, I have urged the Subcommittee to consider expanding the number of statutory privacy offices from 2 (namely, the Department of Homeland Security (DHS) and the Department of Justice(DOJ)) to 24 (covering all major Departments -- the so-called Chief Financial Officers Act agencies). The vast majority of these agencies are Cabinet Departments, such as the Department of the Treasury (and the

Responses to Questions Submitted to Professor Sally Katzen by Subcommittee Members

1. What are the biggest challenges that federal privacy officers must address?

The biggest challenges that agency privacy officers face are first, getting a seat at the table with senior agency policy officials as policies or programs are being formulated, and second, being heard (and supported) when they raise privacy implications about high priority proposals. Too often, privacy officers are seen as simply administrators of the Privacy Act and other pertinent laws, whereas they are a source of expertise and experience which the agency should take advantage of when establishing and implementing all agency activities.

2. Please describe the pros and cons of having a chief privacy officer appointed within the Office of Management and Budget.

As I mentioned in my testimony, appointing a chief privacy officer in OMB would not only be an official recognition of the importance of privacy concerns in national policy debates, but also there would be someone in the Executive Office of the President with "privacy" in his or her title who would be charged with oversight of federal privacy practices, developing national privacy polices, and monitoring of interagency processes where privacy is implicated. In a world of information sharing, many privacy issues affect multiple federal agencies. As you know, OMB plays a critical role in clearance of Executive Branch actions – e.g., executive orders, regulations, proposed legislation, etc. – and a chief privacy officer within OMB would be able to be involved in all of these multi-agency activities. In addition, a chief privacy officer within OMB would serve as a natural focus for government-wide coordination, expertise, and training, as well as being an identifiable point of contact for industry, privacy advocates, international privacy officers and other interested persons.

I can think of no disadvantages to appointing a chief privacy officer within OMB.

3. You argue that every agency should have statutory privacy officer. Is there an economic price tag that would accompany such a sweeping mandate?

The additional cost of creating statutory privacy officers is virtually nil, whereas the cost of not adopting the suggestion may be huge.

To explain, I have urged the Subcommittee to consider expanding the number of statutory privacy offices from 2 (namely, the Department of Homeland Security (DHS) and the Department of Justice(DOJ)) to 24 (covering all major Departments -- the so-called Chief Financial Officers Act agencies). The vast majority of these agencies are Cabinet Departments, such as the Department of the Treasury (and the

RESPONSE TO POST-HEARING QUESTIONS FROM LINDA D. KOONTZ, DIRECTOR, INFORMATION MANAGEMENT ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE, WASHINGTON, DC

United States Government Accountability Office
Washington, DC 20548

June 7, 2006

The Honorable Chris Cannon
Chairman, Subcommittee on Commercial and Administrative Law
Committee on the Judiciary
House of Representatives

Subject: *Privacy: Subcommittee Questions Concerning Legislatively-Created Privacy Officers*

Dear Mr. Chairman:

This letter responds to your May 25, 2006 letter that we provide answers to questions relating to your May 17, 2006 hearing. At that hearing, we testified on key challenges facing agency privacy officers, including those at the Departments of Homeland Security and Justice.[1] Your questions, along with our responses, follow.

1. What are the arguments in favor of and against a legislatively-created privacy officer?

A significant argument in favor of a legislatively-created privacy officer is the potential of such a position to raise the visibility of privacy issues within a federal agency, as witnessed through the creation of a privacy officer at the Department of Homeland Security (DHS). Specifically, section 222 of the Homeland Security Act of 2002 directed the appointment of a senior official at DHS to assume primary responsibility for privacy policy, including, among other things, assuring that the use of technologies sustains, and does not erode, privacy protections relating to the use, collection, and disclosure of personal information.[2] This was the first statutorily required senior privacy official at any federal agency. While we have not yet conducted a review of the effectiveness of the DHS Privacy Office, the office has taken steps to raise the visibility of privacy issues within the department. For example, the office chartered an advisory committee—the Data Privacy and Integrity Advisory Committee—consisting of experts from business, non-profit organizations, and the academic community, to advise it on issues that affect individual privacy within DHS, as well as data integrity, interoperability, and other privacy-related issues. In addition, the DHS Privacy Office has initiated a series of public workshops to share information and discuss current issues related to privacy, including the use

[1] Government Accountability Office, *Privacy: Key Challenges Facing Federal Agencies*, GAO-06-777T, (Washington, D.C.: May 17, 2006).

[2] Homeland Security Act of 2002, Pub. L. 107-296, § 222, 116 Stat. 2155.

of data from commercial sources for homeland security, and the use of personal information in the federal government. Finally, the privacy office recently published detailed guidance on conducting privacy impact assessments, aspects of which were used to draft similar guidance at the Department of Justice.

Nevertheless, arguments can also be made against creating additional legislative requirements for privacy officers. Virtually all major federal agencies already have senior officials designated to address privacy issues, and a new legislatively created privacy officer may not be needed in every agency. A long-standing requirement under the Paperwork Reduction Act has been in place for agency chief information officers to be responsible for implementing and enforcing privacy policies, procedures, standards, and guidelines for compliance with the Privacy Act.[3] A further argument against setting new legislative requirements for privacy officers is that the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act of 2005[4] already requires each agency covered by the act to have a chief privacy officer responsible for, among other things, "assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of information in identifiable form." Subsequently, in February 2005, OMB issued a memorandum[5] to federal agencies requiring them to designate a senior official with overall agencywide responsibility for information privacy issues. This senior official was to have overall responsibility and accountability for ensuring the agency's implementation of information privacy protections and play a central policy-making role in the agency's development and evaluation of policy proposals relating to the agency's collection, use, sharing, and disclosure of personal information. OMB has subsequently reported that all major agencies have designated senior privacy officials as required. In addition, prior to the OMB guidance, several agencies had already designated privacy officials at higher levels without legislative requirements. For example, the Internal Revenue Service had been one of the first, establishing its privacy advocate in 1993. In 2001, the Postal Service established a Chief Privacy Officer.

2. Would there be any benefit in establishing legislatively created privacy officers in other federal agencies?

As discussed above, it may not be necessary to establish legislatively-created privacy officers in agencies such as the Internal Revenue Service and the Postal Service, which have already established senior privacy officials and privacy offices, and other agencies are already under legislative requirements for privacy officers. However, to the extent that the Congress believes that individual agencies need to place additional emphasis on privacy, legislatively establishing such offices may be beneficial to heighten awareness and attention to these issues.

---

[3] The Paperwork Reduction Act (Pub. L. 96-511), as amended (44 U.S.C. 3506(a)(2) and (3) and 44 U.S.C. 3506(g)).

[4] The Transportation, Treasury, Independent Agencies, and General Government Appropriations Act of 2005, Sec. 552, Division H, Consolidated Appropriations Act of 2005 (Pub. L. 108-447; 118 Stat 3268; 5 U.S.C. 552a note).

[5] OMB, *Designation of Senior Agency Officials for Privacy*, Memorandum M-05-08 (Feb. 11, 2005).

3. Based on your office's previous review of the Department of Homeland Security Privacy Office, how does that component compare with other federal agencies that handle privacy issues?

We have not yet conducted a review of the effectiveness of the DHS Privacy Office, nor have we performed a comparative analysis of the privacy policy and management structures in place at other federal agencies. Nevertheless, as discussed above, the DHS Privacy Office has taken positive steps to raise the visibility of privacy issues within the department. Specifically, these include establishing an external advisory committee, conducting public workshops on topical privacy issues, and issuing guidance on the conduct of privacy impact assessments.

4. What are some ways that federal agencies could ensure that their data mining efforts do not compromise privacy protections?

Federal agencies can mitigate concerns about the potential for data mining programs to compromise personal privacy by complying with the requirements of the Privacy Act and E-Government Act of 2002, including the requirement to conduct a privacy impact assessment (PIA). PIAs are important tools that: (1) require an agency to fully consider the privacy implications of planned systems and data collections before those systems and collections have been fully implemented, when it may be relatively easy to make critical adjustments, and (2) provide the public with more complete information about the privacy impacts of agency activities than would otherwise be available. Keeping the public fully informed of agency activities involving personal information is a key element in protecting individuals' privacy rights.

Our 2005 review of selected data mining efforts at federal agencies[6] determined that PIAs were not always being done in full compliance with OMB guidance. Complete assessments are an important tool for agencies to identify areas of noncompliance with federal privacy laws, evaluate risks arising from electronic collection and maintenance of information about individuals, and evaluate protections or alternative processes needed to mitigate the risks identified. Agencies that do not take all the steps required to protect the privacy of personal information risk the improper exposure or alteration of such information. We recommended that the agencies responsible for the data mining efforts we reviewed complete or revise PIAs as needed and make them available to the public.

In addition, agencies can obtain guidance from a March 2004 report on privacy concerns regarding data mining in the fight against terrorism, issued by an advisory committee chartered by the Department of Defense.[7] The report made numerous recommendations to better ensure that privacy requirements are clear and stressed that proper oversight be in place when agencies engage in data mining that could include personal information. Further, agency privacy offices can provide a degree of

---

[6] GAO, *Data Mining: Agencies Have Taken Key Steps to Protect Privacy in Selected Efforts, but Significant Compliance Issues Remain*, GAO-05-866 (Washington, D.C.: Aug. 15, 2005). See also GAO, *Data Mining: Federal Efforts Cover a Wide Range of Uses*, GAO-04-548 (Washington, D.C.: May 4, 2004).

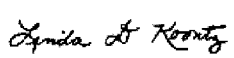
[7] Technology and Privacy Advisory Committee, *Safeguarding Privacy in the Fight Against Terrorism* (Washington, D.C.: Mar. 1, 2004).

internal oversight to help ensure that privacy is fully addressed in agency data mining activities.

In preparing this correspondence, we relied on previously issued GAO products, testimony of the Department of Justice Chief Privacy and Civil Liberties Officer, and a May 22, 2006 Office of Management and Budget memorandum concerning agency responsibilities for safeguarding personally identifiable information.

Should you or your office have any questions on matters discussed in this letter, please contact me at (202) 512-6240, or John de Ferrari, Assistant Director, at (202) 512-6335. We can also be reached by e-mail at koontzl@gao.gov and deferrarij@gao.gov, respectively.

Sincerely yours,



Linda D. Koontz
Director, Information Management Issues