AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. Hrg. 110–1025

# PROTECTING PERSONAL INFORMATION: IS THE FEDERAL GOVERNMENT DOING ENOUGH?

## HEARING

BEFORE THE

## COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED TENTH CONGRESS

SECOND SESSION

JUNE 18, 2008

Available via http://www.gpoaccess.gov/congress/index.html

Printed for the use of the
Committee on Homeland Security and Governmental Affairs

U.S. GOVERNMENT PRINTING OFFICE

44–117 PDF WASHINGTON : 2010

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) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

JOSEPH I. LIEBERMAN, Connecticut, *Chairman*

CARL LEVIN, Michigan
DANIEL K. AKAKA, Hawaii
THOMAS R. CARPER, Delaware
MARK L. PRYOR, Arkansas
MARY L. LANDRIEU, Louisiana
BARACK OBAMA, Illinois
CLAIRE McCASKILL, Missouri
JON TESTER, Montana

SUSAN M. COLLINS, Maine
TED STEVENS, Alaska
GEORGE V. VOINOVICH, Ohio
NORM COLEMAN, Minnesota
TOM COBURN, Oklahoma
PETE V. DOMENICI, New Mexico
JOHN WARNER, Virginia
JOHN E. SUNUNU, New Hampshire

MICHAEL L. ALEXANDER, *Staff Director*
HOLLY A. IDELSON, *Counsel*
ADAM R. SEDGEWICK, *Professional Staff Member*
BRANDON L. MILHORN, *Minority Staff Director and Chief Counsel*
JOHN K. GRANT, *Minority Counsel*
TRINA DRIESSNACK TYRER, *Chief Clerk*
PATRICIA R. HOGAN, *Publications Clerk and GPO Detailee*
LAURA W. KILBRIDE, *Hearing Clerk*

# CONTENTS


| | Page |
|---|---|
| Opening statements: | |
| Senator Lieberman | 1 |
| Senator Collins | 4 |
| Senator Akaka | 7 |
| Senator Carper | 34 |

WITNESSES

WEDNESDAY, JUNE 18, 2008

| | |
|---|---|
| Linda D. Koontz, Director, Information Management Issues, U.S. Government Accountability Office | 9 |
| Hugo Teufel III, Chief Privacy Officer, U.S. Department of Homeland Security | 11 |
| Ari Schwartz, Vice President and Chief Operating Officer, Center for Democracy and Technology | 13 |
| Peter P. Swire, C. William O'Neill Professor of Law, Moritz College of Law, The Ohio State University Senior Fellow, Center for American Progress | 15 |

ALPHABETICAL LIST OF WITNESSES

| | |
|---|---|
| Koontz, Linda D.: | |
| Testimony | 9 |
| Prepared statement | 39 |
| Schwartz, Ari: | |
| Testimony | 13 |
| Prepared statement | 75 |
| Swire, Peter P.: | |
| Testimony | 15 |
| Prepared statement | 87 |
| Teufel, Hugo, III: | |
| Testimony | 11 |
| Prepared statement | 64 |

APPENDIX

| | |
|---|---|
| Susan E. Dudley, Administrator, Office of Information and Regulatory Affairs, and Karen Evans, Administrator, Office of E-Government and Information Technology, Office of Management and Budget, prepared statement | 95 |
| GAO Report to Congressional Requesters, "Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information," GAO–08–526, May 2008 | 98 |

# PROTECTING PERSONAL INFORMATION: IS THE FEDERAL GOVERNMENT DOING ENOUGH?

**WEDNESDAY, JUNE 18, 2008**

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
*Washington, DC.*

The Committee met, pursuant to notice, at 10:04 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Joseph I. Lieberman, Chairman of the Committee, presiding.

Present: Senators Lieberman, Akaka, Carper, and Collins.

## OPENING STATEMENT OF CHAIRMAN LIEBERMAN

Chairman LIEBERMAN. Good morning and welcome to our hearing today on Federal efforts to protect personal privacy. I want to welcome our distinguished panel and also particularly commend the Government Accountability Office (GAO), Ms. Koontz, for your excellent work on the report that is being released today on the Federal Government's privacy efforts.[1] I also want to particularly thank our colleague and dear friend, Senator Akaka, who has taken a particular interest in government privacy issues and has encouraged Senator Collins and me to convene today's hearing.

We live in an age that really is defined by information. The explosion of new technologies to gather, share, and store huge quantities of information has made possible significant advances in every aspect of our lives, including more efficient and effective governmental programs. But these same technologies have also dramatically altered the privacy landscape. It is easier than ever for government and private entities to acquire large amounts of personal information about people—information that can cause harm to those people if improperly disclosed or used.

Loss of privacy, for instance, can lead to crimes such as identify theft or stalking. The dissemination or misuse of certain private data can also result in the loss of employment, discrimination, harassment, or surveillance. So it is essential, obviously, for government to collect and use personal information—for example, to provide security, conduct law enforcement, or administer and extend governmental benefits. But we also have to do everything we possibly can to ensure that in collecting and using personal information, we tread very carefully because when dealing with the personal information of individual Americans, we have got to properly

[1] The GAO Report on Privacy appears in the Appendix on page 98.

balance our policy goals against potential incursions on their privacy.

Congress constructed a foundation for respecting individual privacy within the Federal Government in the landmark Privacy Act of 1974 which seeks to prohibit unauthorized disclosure of personal information, ensure the accuracy and relevance of information collected by the government, and provide individuals with access to their information and a means of redressing errors. Six years ago, the law was strengthened by the Electronic Government Act of 2002, the so-called E–Government Act, which went through this Committee on its way to becoming law. That Act now requires that agencies analyze in advance the potential privacy impacts of new information systems and data collections, and minimize those potential risks. One of the questions I want to ask today is whether governmental agencies are fulfilling their obligations under the E–Government Act.

Obviously, notwithstanding these two pieces of legislation, we know that there is much more to do, and the GAO report makes that clear.

New technologies and data practices have overtaken some of the core definitions of the Privacy Act of 1974. That is, in the world of information collection and dissemination, millennia ago. For instance, in 1974, Congress simply could not foresee the government's use of what are now called "private data brokers"—a totally unimagined line of enterprise in 1974—with access to extensive personal information about individuals. So we now need to ensure that this practice does not become an end run around the protections of the Privacy Act. I know that is not the intention. These private data brokers are of significant assistance both to the government and, of course, the private sector. But, still, we have to be concerned about privacy.

New policy demands, including some of the homeland security efforts that have originated in this Committee, call for sharing information among a wider array of agencies. Security concerns combined with new technologies, such as biometrics, are driving the collection of new types of personal information. The American people may have justifiable concerns about sharing their personal information when the government is collecting and storing their fingerprints, retinal scans, even their DNA, and we have to reassure them. We need to look closely to see how these new programs and practices intersect with existing privacy law and what adjustments may be necessary.

When we created the Department of Homeland Security, however, we did mandate the establishment of a Chief Privacy Officer within the Department to address what we knew would be challenging questions as to how to integrate privacy considerations—including implementation of government privacy law—into the critical mission, the new mission post-September 11, 2001, of homeland security. I am pleased that the second person to hold that position, Mr. Teufel, is one of our witnesses today. Incidentally, Senator Collins and I working closely together with other Members of the Committee, also created an expanded network of privacy officials as part of the two laws that originated in this Committee that enacted recommendations of the 9/11 Commission.

But the question remains whether we have adequate leadership and resources devoted to privacy at the government-wide level. In 2003, in response to another request from this Committee, GAO concluded that the Office of Management and Budget (OMB) needed to assert more leadership on privacy questions to ensure that the agencies of our government were actually carrying out their responsibilities under the Privacy Act and other government privacy law. In fact, today there is no one in OMB, no office in the Federal Government, no high-level official, not even, as far as I can determine, a political appointee or member of the Senior Executive Service (SES), whose job it is to focus full time on government-wide privacy policy. This contrasts, interestingly enough, with many other countries, including those of our friends and allies in Europe, which have elevated privacy policy to the highest levels of their governments. This absence of leadership for privacy in the U.S. Government I know is a message we will hear loud and clear today.

So I look forward to the testimony, and then to working together to ensure our privacy laws continue to provide appropriate and meaningful protections for our citizens. It sure does look to me, based on the GAO report, that it is time for us to do an updating and overall revision of the Privacy Act of 1974.

[The prepared statement of Senator Lieberman follows:]

PREPARED STATEMENT OF SENATOR LIEBERMAN

Good morning and welcome to our hearing today on federal efforts to protect personal privacy. I want to welcome our distinguished panel and also commend the Government Accountability Office for its excellent work on this issue, as reflected in their report being released today on the federal government's privacy efforts. I also want to thank my colleague, Senator Akaka, who has taken a particular interest in government privacy issues and encouraged Senator Collins and me to convene today's hearing.

We live in an "information age," and the explosion of new technologies to gather, share, and store huge quantities of information has made possible huge advances in every aspect of our lives, including more efficient and effective government programs. But these same technologies have also dramatically altered the privacy landscape. It is easier than ever for government and private entities to acquire large amounts of personal information about people—information that can cause harm to those people if it is improperly used or disclosed.

For the individual, loss of privacy can lead to crimes such as identify theft or stalking. The dissemination or misuse of certain private data can also result in other harms such as loss of employment, discrimination, or unwarranted harassment or surveillance. Certainly, it is essential for government to collect and use personal information—for example to provide security, conduct law enforcement, or administer benefits. But we must strive to ensure that we tread carefully when dealing with the personal information of individuals and that we properly balance our many policy goals against potential incursions on privacy.

Congress constructed a foundation for respecting individual privacy within the federal government in the landmark Privacy Act of 1974 which seeks to prohibit unauthorized disclosure of personal information, ensure the accuracy and relevance of information collected by the government, and provide individuals with access to their information and a means of redress for errors. Six years ago, that law was buttressed by the Electronic Government Act of 2002, which I introduced and had the privilege of guiding through this Committee on its way to becoming law. The E-Government Act requires that agencies analyze in advance the potential privacy impacts of new information systems and data collections, and minimize those potential risks. But we know there is more to do.

New technologies and data practices have overtaken some of the core definitions of the Privacy Act. For instance, the Act simply could not foresee the government's use of private data brokers with access to extensive personal information about individuals, and we need to ensure this practice does not become a serious end-run around the protections of the Privacy Act.

New policy demands—including some of the homeland security efforts that are of vital concern to this Committee—call for sharing information among a wider array of agencies. Security concerns combined with new technologies, such as biometrics, are also driving the collection of new types of personal information. Americans may have justifiable concerns about sharing their personal information when the government is collecting and storing their fingerprints, retinal scans, even their DNA. We need to look closely to see how these new programs and practices intersect with existing privacy law, and what adjustments may be necessary.

This Committee has recognized the need for dedicating officials and resources to address privacy concerns within government, particularly as we tackle challenging new missions such as homeland security. When we created the Department of Homeland Security, we mandated the establishment of a Chief Privacy Officer within the department to address what we knew would be challenging questions as to how to integrate privacy considerations—including implementation of government privacy law—into the critical mission of homeland security. I am pleased that the second individual to hold that position, Mr. Teufel, is one of our witnesses today. We also created an expanded network of privacy officials as part of the two laws enacting recommendations of the 9/11 Commission.

But the question remains whether we have adequate leadership and resources devoted to privacy at the government-wide level. In 2003, in response to a request from this committee, GAO concluded that OMB needed to assert more leadership on privacy to ensure that agencies fulfilled the mandates of the Privacy Act and other government privacy law. In fact, there is no one in OMB, no office in the federal government, no high-level official, not even a political appointee or member of the Senior Executive Service, whose job it is to focus full-time on government-wide privacy policy. This stands in stark contrast to many other countries, including those in the European Union, which have elevated privacy policy to the highest levels of government. This absence of leadership is a message we will hear loud and clear today.

I look forward to the testimony and to working together to ensure that our privacy laws continue to provide appropriate and meaningful protections for our citizens. Senator Collins.

Senator LIEBERMAN. Senator Collins.

## OPENING STATEMENT OF SENATOR COLLINS

Senator COLLINS. Thank you. Thank you, Mr. Chairman, for holding this important hearing.

We live in a world of unprecedented access to information. Data are being collected and stored in quantities of almost unimaginable size by a wide range of public and private entities. People freely share personal information about themselves on blogs or social networking Web sites. At the same time, most Americans believe that protecting some degree of personal privacy is a fight worth waging in the Digital Age.

In 1974, Congress passed the Privacy Act to establish rules for government's use of computerized recordkeeping systems. To provide some context, in that same year, President Nixon resigned the presidency in the wake of the Watergate scandal. Gasoline cost 55 cents per gallon. And an exciting new gadget—the pocket calculator—was just beginning to appear on store shelves.

Thirty-four years later, as we hold this hearing, six presidents have occupied the Oval Office, the average cost of gasoline exceeds $4 per gallon, and the BlackBerrys that the Chairman and I depend so heavily on can do more than all but the most sophisticated computers of 1974.

Yet with very few modifications, the 1974 Privacy Act has remained the primary law governing the Federal Government's collection, storage, and use of personal information about its citizens.

Obviously, technology has changed dramatically during the past 34 years. The Federal Government can now gather, store, and

share information much more efficiently than was even contemplated 34 years ago. Yet it is a testament to the original drafters of the Privacy Act that, in spite of these significant advances in technology, many of the law's provisions remain applicable to the technology in use today.

Nevertheless, as the GAO and our other witnesses will testify, current law could be strengthened to improve assurances that personal information is legitimately collected and adequately secured.

We should build on the success of the original law while ensuring that it is adequate to meet the new challenges of the Information Age. We can accomplish this by remaining true to the principles of openness, accuracy, transparency, and accountability that underpin the Fair Information Practices, which were developed by the U.S. Government and endure as guiding principles for protecting the privacy and security of personal data.

This hearing will examine several important questions. First, are the rules governing the collection and use of personal information clear to both the officials who have access to it and the public that provides it? System of Records Notices, descriptions of routine uses of information, and other basic tools of the privacy regime are supposed to describe various information systems so that government officials and the public will know when and how personal information can be collected and shared. In many cases, however, the tools are worded so broadly that they really provide little clarity as to which rules govern any particular information system.

Second, how can we ensure the security of personal information collected and maintained by the U.S. Government? Unfortunately, there are far too many recent examples that demonstrate the need for the Federal Government to better secure the sensitive information that it collects and maintains.

For example, in 2006, the Veterans Affairs Department reported that the personal information of approximately 26.5 million veterans was compromised when a laptop containing departmental records was stolen. A 2007 study by the Inspector General for Tax Administration found that at least 490 laptops containing sensitive taxpayer data had been lost or stolen between 2003 and 2007. But lost or stolen laptops are not the only security concern, as is evidenced by a 2006 data compromise of employee information at the Department of Agriculture that was caused by unauthorized access to the agency's systems.

Beyond the physical and cyber security of sensitive data, we must also ask what is the best way to deal with innovative technologies—such as data mining—that seek to use information in entirely new ways. Technology develops so rapidly in this day and age that we will need to be more vigilant in ensuring that the wheels of progress are not inadvertently running over our basic privacy rights.

And, finally, how can we continue to encourage the legitimate sharing of accurate information among government agencies for legitimate purposes while maintaining adequate controls to hold accountable those who might compromise an individual's privacy by misusing their personal information? The recent inappropriate searches by State Department contractors of the passport files of Senators McCain, Obama, and Clinton highlight the need for im-

provements in this area. Prohibitions against unauthorized use of the passport system did not prevent these improper inquiries, although audit mechanisms did facilitate prompt administrative action against the contractors responsible. As the government searches for ways to improve the sharing and the analysis of the information it collects, we must develop effective security measures and consider whether our laws properly sanction those who use sensitive information for inappropriate purposes.

This hearing is yet another step in a robust dialogue now occurring about privacy in our country. A strong privacy regime, built on the principles of transparency, accountability, and security, should inspire the confidence of the American people that the Federal Government is not compromising personal privacy but, rather, preserving and protecting it. Doing so, however, in the Digital Age is a new challenge.

Thank you, Mr. Chairman.

[The prepared statement of Senator Collins follows:]

PREPARED STATEMENT OF SENATOR COLLINS

We live in a world of unprecedented access to information. Data are being collected and stored in quantities of almost unimaginable size by a wide range of public and private entities. People freely share personal information about themselves on blogs or social networking Web sites. At the same time, most Americans believe that protecting some degree of personal privacy is a fight worth waging in the digital age.

In 1974, Congress passed the Privacy Act to establish rules for government's use of computerized record-keeping systems. In that same year, President Nixon resigned the presidency in the wake of the Watergate scandal. Gasoline cost 55 cents per gallon. And an exciting new gadget—the pocket calculator—was just beginning to appear on store shelves.

Thirty-four years later, six presidents have occupied the Oval Office, the average cost of gasoline exceeds $4 per gallon, and the Blackberrys that the Chairman and I depend on can do more than all but the most sophisticated computers of 1974. Yet with very few modifications, the 1974 Privacy Act has remained the primary law governing the federal government's collection, storage, and use of personal information about its citizens.

Obviously, technology has changed dramatically since the Privacy Act was written. The federal government can now gather, store, and share information more efficiently than was even imagined possible 34 years ago. Yet it is a testament to the original drafters of the Privacy Act that in spite of these significant advances in technology, many of its provisions remain applicable to the technology in use today.

Nonetheless, as the GAO and our other witnesses will testify, current law could be strengthened to improve assurances that personal information is legitimately collected and adequately secured. We should build on the success of the original laws while ensuring that they are adequate to meet the new challenges of the Digital Age. We can accomplish this by remaining true to the principles of openness, accuracy, transparency, and accountability that underpin the Fair Information Practices, which were developed by the U.S. government and endure as guiding principles for protecting the privacy and security of personal information.

This hearing will examine several important questions. First, are the rules governing the collection and use of personal information clear to both the officials who have access to it and the public that provides it? System of Records Notices, descriptions of routine uses of information, and other basic tools of the privacy regime are supposed to describe various information systems so that government officials and the public will know when and how personal information can be collected and shared by the government. In many cases, however, these tools are worded so broadly that they provide little clarity as to what rules govern any particular information system.

Second, how can we ensure the security of personal information collected and maintained by the U.S. government? Unfortunately, there are far too many recent examples that demonstrate the need for the federal government to better secure the sensitive information that it collects and maintains.

In 2006, the Department of Veterans Affairs reported that the personal information of approximately 26.5 million veterans was compromised when a laptop containing Department records was stolen. A 2007 study by the Inspector General for Tax Administration found that at least 490 laptops containing sensitive taxpayer data had been lost or stolen between 2003 and 2007. But lost or stolen laptops are not the only security concerns, as in a 2006 data compromise of employee information at the Department of Agriculture that was caused by unauthorized access to the agency's systems.

Beyond the physical- and cyber-security of sensitive data, we must also ask what is the best way to deal with innovative technologies—such as data mining—that seek to use information in entirely new ways. Technology develops so rapidly in this day and age that we will need to be vigilant to ensure that the wheels of progress are not inadvertently running over our basic privacy rights.

And, finally, how can we continue to encourage the sharing of information among government agencies for legitimate purposes while maintaining adequate controls to hold accountable those who might compromise an individual's privacy by misusing their personal information? The recent inappropriate searches by State Department contractors of the passport files of Senators McCain, Obama, and Clinton highlight the need for improvements in this area. Prohibitions against unauthorized use of the passport system did not prevent these improper inquiries—though audit mechanisms did facilitate prompt administrative action against the contractors responsible. As the government searches for ways to improve the sharing and analysis of the information it collects, we must develop effective security measures and consider whether our laws properly sanction those who use sensitive information for inappropriate purposes.

This hearing is yet another step in a robust dialog now occurring about privacy in this country. A strong privacy regime, built on principles of transparency and accountability, should inspire the confidence of the American people that the federal government is not compromising personal privacy but rather preserving and protecting it.

Chairman LIEBERMAN. Thank you, Senator Collins, for that excellent opening statement.

Let me say again how much I appreciate the leadership role that Senator Akaka has played on these matters, and I would like now to ask him if he would like to make an opening statement.

## OPENING STATEMENT OF SENATOR AKAKA

Senator AKAKA. Thank you very much, Mr. Chairman. I also want to welcome the panel and thank you and Ranking Member Collins for having this hearing today.

Two years ago, following our joint hearing on the Department of Veterans Affairs (VA) data breach, I requested that this Committee take a closer look at the Privacy Act to see if it continued to protect Americans' personal information in this increasingly electronic age. Systems and procedures to prevent loss or unauthorized disclosure are not enough. Data security also relies on a robust privacy framework that minimizes the collection, use, and sharing of personal information and provides individuals the opportunity to access their data and correct any mistakes.

For the past few years, I have been looking into Federal data collection and privacy issues and asked GAO for several reports. And today GAO is releasing two reports which I and others requested: One on the need for updating the Privacy Act and another on the need to consolidate privacy functions with a Senior Privacy Officer. And I agree with the GAO's findings, and I am glad to see that the Chairman also believes that the Privacy Act needs to be updated.

Without strong privacy oversight, I fear that key privacy safeguards will fall through the cracks and Americans' personal information will remain at risk. Furthermore, I believe that the framework for protecting privacy in the Federal Government needs to be

updated and loopholes closed. Failure to do so risks inaccurate information guiding our national security decisions as well as Americans' access to government services and benefits.

I look forward to working with the Chairman and Ranking Member on legislation to address these issues, and, Mr. Chairman, I would like to ask that my full statement be made part of the record.

Chairman LIEBERMAN. Without objection, so ordered, and thank you very much, Senator Akaka, for those words.

[The prepared statement of Senator Akaka follows:]

PREPARED STATEMENT OF SENATOR AKAKA

Thank you Chairman Lieberman and Ranking Member Collins for holding today's hearing on the Privacy Act.

Two years ago, following our joint hearing with the Veterans' Affairs Committee on the data breach at the Department of Veterans Affairs—which risked the personal information of 26.5 million veterans and active duty military—I requested that this Committee take a closer look at the Privacy Act to see if it continued to protect American's personal information in this increasingly electronic age. While our hearing at that time was focused on information security practices, I knew that we also needed to look at the safeguards for the collection, use, and sharing of personal information.

Data security does not just rely on systems and procedures to prevent loss or unauthorized disclosure. It also relies on a robust privacy framework that minimizes the amount and use of personal information and provides individuals the opportunity to access their data and correct any mistakes.

For the past few years I have been looking into federal data collection and privacy issues. At my request, the Government Accountability Office (GAO) conducted several investigations on federal data mining activities and found that federal agencies are not following all key privacy and information security practices. In its May 2004 report, GAO found 122 data mining activities in the federal government that use personal data. Thirty-six of these activities mined personal information from the private sector and 46 activities mined it from other agencies. This included student loan application data, bank account numbers, credit card information, and taxpayer identification numbers. The use of private sector data and the failure of agencies to follow key privacy requirements limit the ability of the public to control their personal information and risks the denial of government services or benefits.

I believed then, as I do now, that a strong privacy official at each federal agency would help ensure compliance with federal privacy and information security laws. Unfortunately, according to a report being released today by GAO, despite the fact that federal agencies are required to designate a senior official for privacy, some of these officials still do not have full responsibility for all of the major privacy functions. Without such oversight—from ensuring compliance with privacy laws to providing redress procedures and privacy training—I fear that key privacy safeguards will fall through the cracks and Americans' public information will remain at risk.

Today, however, our focus is on how the law is working. According to GAO and many privacy experts, the framework for protecting privacy in the federal government needs to be updated and loopholes closed. Whether it is the ineffective definition of System of Records or the ever expanding list of routine uses, we need to reexamine the Privacy Act and related privacy laws to ensure that they work in the 21st century. Failure to do so risks inaccurate information guiding our national security decisions as well as Americans' access to government services and benefits.

I believe that legislative changes are needed to the federal privacy framework and look forward to working with the Chairman and Ranking Member to address these issues. Thank you again for holding this hearing.

Chairman LIEBERMAN. Let's go right to the panel. Again, I would like to welcome you all. Our first witness is Linda Koontz, who is the Director for Information Management Issues at the Government Accountability Office, with responsibility for issues concerning the collection, use, and dissemination of government information. Ms. Koontz has recently directed studies on privacy,

records management, data mining, information access and dissemination, and E–Government.

It is a pleasure to have you. Please proceed with your testimony.

**STATEMENT OF LINDA D. KOONTZ,[1] DIRECTOR, INFORMATION MANAGEMENT ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE**

Ms. KOONTZ. Thank you, Mr. Chairman and Members of the Committee. I appreciate the opportunity to participate in today's hearing on government protection of personally identifiable information. As you know, collecting such information is vital for the Federal Government to provide services and benefits, as well as to respond to threats such as terrorism. At the same time, government use of personal information raises privacy concerns, such as whether the legal mechanisms governing such use remains sufficient for protecting personal privacy in the context of modern information technology.

In my remarks, I will present key results from a report that we are releasing today on this issue. For our review, we assessed the sufficiency of current laws and guidance for protecting personally identifiable information and identified alternatives for addressing issues raised by our assessment.

The primary relevant statute is the Privacy Act of 1974, which is the major mechanism for controlling Federal collection, use, and disclosure of personally identifiable information. The Act's provisions are largely based on a set of key privacy principles know as the Fair Information Practices, which call for such things as limiting the collection of personal information, ensuring that information is accurate when it is collected, and keeping the public informed of any such collections. These widely accepted principles, first proposed in 1973 by a U.S. Government Advisory Committee, are not legal requirements. However, they do provide a useful framework for balancing the need for privacy with other public policy interests, and they are used by numerous countries and organizations as the basis for privacy laws and policies.

Besides the Privacy Act, another relevant statute is the E–Government Act of 2002, which requires agencies to conduct Privacy Impact Assessments (PIAs)—that is, analyses of how personal information is protected when it is collected, stored, shared, and managed in a government information system.

The two statutes and related guidance from the Office of Management and Budget set minimum requirements for agencies. But our review showed that they may not consistently protect personally identifiable information and may not fully adhere to key privacy principles. Based on our analysis, extensive discussions with agency officials and the perspectives of privacy experts obtained through a panel convened for us by the National Academy of Sciences, we identified issues in three major areas: First, applying privacy protections consistently to all Federal collection and use of personal information; second, ensuring the use of personally identifiable information is limited to a stated purpose; and third, estab-

[1] The prepared statement of Ms. Koontz appears in the Appendix on page 39.

lishing effective mechanisms for informing the public about privacy protections.

In the first area, applying protections consistently, issues arise primarily from the scope of the Privacy Act, which is limited to what are called "System of Records." These are defined as any grouping of records containing personal information that is retrieved by an individual identifier. Thus, the Act covers personal information in a given information system if an agency uses an individual identifier for retrieval, but not if some other method is used, such as searching for all individuals with a certain medical condition or who apply for a certain benefit.

The resulting inconsistency has led experts to agree that the definition of a System of Records is too narrow. The Congress could address this issue by revising the definition to cover all personally identifiable information collected, used, and maintained systematically by the Federal Government.

The second area, ensuring that use of personally identifiable information is limited to a stated purpose, is based on the principles that collecting personal information should be disclosed beforehand, and use of this information should be limited to a specified purpose. When the government must define a specific purpose and use for personal information, individuals gain assurance that their privacy will be protected and the information will not be used in ways that could unfairly affect them. However, current laws and guidance impose only modest requirements for defining the purposes and use of personal information. Agencies may define purposes very generally which allows for unnecessarily broad ranges of uses without meaningful limitations. These issues could be addressed by requiring that specific limits be set on the use of information both within and among agencies.

The third area, establishing effective mechanisms for informing the public, is related to both openness and accountability. These principles call for informing the public about privacy policies and practices and for holding agencies accountable for protecting privacy in their use of personal information. Currently, these principles are enforced through a System of Records Notices that agencies are required to publish in the *Federal Register*. However, it is questionable that such a publication effectively informs the public at large. First, the notices can be difficult to understand, as they are generally written in legalistic terms. Second, they do not always contain complete and useful information. And, finally, finding relevant notices and determining which ones are in force may be challenging. Options to address these issues include providing easy-to-understand, brief notices along with comprehensive versions, setting requirements to improve the content of privacy notices, and revising the Privacy Act to require that all notices be published on a central Web site.

The challenge of how best to balance the Federal Government's need to collect and use information with individuals' privacy rights in the current environment merits a national debate on all relevant issues. In assessing such a balance, Congress should consider amending applicable laws according to the alternatives we have identified in our report.

Mr. Chairman, that concludes my statement. I would be happy to answer questions at the appropriate time.

Chairman LIEBERMAN. Thanks, Ms. Koontz. That is a good beginning.

Our next witness is Hugo Teufel III, Chief Privacy Officer of the Department of Homeland Security, a position he has occupied since July 2006. Mr. Teufel has primary responsibility in his position for privacy policy at the Department, including compliance with the 1974 Privacy Act and the privacy provisions of the E–Government Act. He previously served in the General Counsel's office at the Department and, before that, was the Associate Solicitor for General Law at the Department of the Interior.

Thanks for being here, Mr. Teufel.

**STATEMENT OF HUGO TEUFEL III,[1] CHIEF PRIVACY OFFICER, U.S. DEPARTMENT OF HOMELAND SECURITY**

Mr. TEUFEL. Thank you very much, Chairman Lieberman, Ranking Member Collins, Senator Akaka, and Members of the Committee. It is an honor to testify before you here today, and I must confess that I am humbled in the presence of my co-panelists here. Linda Koontz and I have worked together for the last 2 years, and we take very seriously the recommendations in her reports. And we usually get it right, but sometimes there is room for improvement, and she lets us know, and we carry out her recommendations, by and large. Ari Schwartz is someone who we regularly reach out to, along with other members of the privacy advocacy community, and I often seek Mr. Schwartz's advice and counsel on issues. And, of course, Peter Swire is someone from whom, since the very first week or two of my tenure in the Privacy Office, I have sought advice and counsel, and it is always great to see him and talk to him and be here.

I read with interest the formal letter inviting me to come and testify, and I noted that this hearing was to consider the adequacy of laws and structures with respect to privacy. And, of course, this is a Congressional Committee, a Senate Committee, and so there will be a lot of talk on the law. I would like to spend just a little bit of time on structure before I conclude my opening remarks.

In the 23 months that I have been in the office, I have thought a lot about the office and the position of Privacy Officer and what it is and what it should be and what it has been at other agencies. And so in my opinion, and what I have tried to do at the Department of Homeland Security, I have grouped our responsibilities into five functional categories: Policy, process, incidents and breaches, education, and outreach.

The significance there is that if you look at other Privacy Officers—and I will put aside Census Bureau, Internal Revenue Service, and Postal Service—most other Privacy Officers and Privacy Offices within government often focus on the technical aspects and do not necessarily get involved with policy and with outreach. Policy is critical as part of Section 222 of the Homeland Security Act, and we are the primary privacy policy office—that is difficult to say fast early in the morning—at the Department of Homeland Secu-

[1] The prepared statement of Mr. Teufel appears in the Appendix on page 64.

rity. But outreach is also essential because there are a lot of external stakeholders who are concerned about what it is that government is doing with personally identifiable information.

So policy, advice—it can be advice and counsel orally given or it can be written policy, as we have done with respect to Social Security numbers and mixed-use systems, administratively extending Privacy Act protections to non-U.S. citizens.

Process, what we think about when we talk about Privacy Impact Assessments and System of Records Notices.

Incidents and breaches—just as it sounds.

Education, really undervalued but terribly important, because whenever humans are involved, people make mistakes. And you cannot get rid of mistakes, but you can minimize them, and the way to do that is education, education, education.

And then the last is outreach—part of what we are doing today and what we regularly do in and around the D.C. area, and sometimes even internationally.

So having said that, as I was preparing today, I was reminded of something that I had heard a couple of weeks ago. As you may know, I am going to be graduating this week from the Naval War College with a master's in national security and strategic studies. The University of Connecticut had not started their master's program in homeland security 4½ years ago, or I would have probably entered that program. And 2 weeks ago, I was at the University of Virginia Law School for their National Security Law Institute. And, in fact, we were at the Pentagon, and we were listening to Judge Jamie Baker, who is the former legal adviser to the National Security Council and now is an associate judge on the Court of Appeals for the Armed Forces, and he was talking about his office and the importance of the legal adviser to the National Security Council. And he noted in his remarks that the law and structure are important, but they are not conclusive. Senior officials have to call on you, and they have to have trust and confidence in you as an adviser in order for you to be able to do your job effectively.

And with that, I will stop, and thank you very much.

Chairman LIEBERMAN. Very interesting. Thank you. The record will note that had you had the opportunity, you would have become a UConn Huskie. [Laughter.]

Ari Schwartz is next, familiar with this Committee, but you have already received a good introduction from Mr. Teufel: Vice President and Chief Operating Officer at the Center for Democracy and Technology (CDT). Mr. Schwartz also serves as a member of the National Institute of Standards and Technology Information Security and Privacy Advisory Board and the State of Ohio Chief Privacy Officer Advisory Committee.

At this time I will ask you to talk about the fact that you lead the Anti-Spyware Coalition. We welcome you today and look forward to your testimony, Mr. Schwartz.

**STATEMENT OF ARI SCHWARTZ,[1] VICE PRESIDENT AND CHIEF OPERATING OFFICER, CENTER FOR DEMOCRACY AND TECHNOLOGY**

Mr. SCHWARTZ. Thank you very much, Mr. Chairman, Ranking Member Collins, and Senator Akaka, for holding this hearing today.

Thirty-four years ago, the U.S. Congress took the revolutionary step toward ensuring that U.S. citizens' information in the hands of the Federal Government would be treated fairly and with respect. The Privacy Act of 1974 sets forth privacy protections that have been an example for governments at different levels around the world. While the Act reached for the goal of privacy, it was by no means perfect. And, in fact, Congress recognized its imperfections even at the time of passage, creating a study commission to report back on how, among other things, the Privacy Act could be improved.

The GAO studies released today suggest that the major concerns of the Personal Privacy Study Commission of 1977 have not only never been addressed fully, but have even worsened with time. While the structure of the Act is still solid, technological advances have outdated many of the key definitions. The Privacy Act guidance from OMB has served to confuse as much as it clarified, and the Department of Justice has not released its Privacy Act Overview for agencies for 4 years. This important document had been issued at least every 2 years since the mid-1980s.

While the Privacy Act implementation has been allowed to decay, Congress has created other protections to help ensure greater transparency over collections of personal information. The E–Government Act recognized that making more information available online was certain to raise new privacy concerns, and in order to address this problem, Congress took the step of requiring a Privacy Impact Assessment for all new and changed collections and new databases. The Privacy Impact Assessments were designed to provide greater transparency to how the government collects and uses personal information.

Over the past 6 years, Privacy Impact Assessments have become an essential tool to help protect privacy. Unfortunately, as with other privacy laws, the Federal Government has unevenly implemented even the most basic transparency requirements of the PIAs across agencies. Like other directives issued by the Administration on privacy, the guidance was vague and has simply not provided agencies with the tools they need to successfully implement the Privacy Impact Assessment requirement unless they already had privacy experts on staff.

Too few agencies have the kind of privacy expertise and leadership necessary to develop internal rules and best practices or even to comply with existing law. The Department of Homeland Security is one agency that has had that kind of leadership through its inception through Nuala Kelly, who started the privacy program, and now through Hugo Teufel, who has already shown us why he is a leader that can bring together this kind of program at the agency.

[1] The prepared statement of Mr. Schwartz appears in the Appendix on page 75.

While privacy experts often focus on these major problems as if the only thing harmed is the privacy of Americans, it is important to note that they have an even greater impact on the effectiveness of the Federal Government. For example, one agency that CDT spoke to told us that the privacy audit revealed that they had lost track of half of their System of Records and, therefore, millions of the personal records held by the agency. At the time of the audit, they just did not know where this information was.

As one retiring security official from the Department of Interior explained publicly earlier this month while discussing that agency's constant failures in privacy and security reporting, he said, "We are promiscuous with our data. We don't know where our data is."

You can call this a privacy concern, you can call this a security concern, or you can call this a data management concern. But to the American taxpayer, the loss of their personal information is certainly called a failure.

To solve these problems, CDT suggests that Congress work with the Executive Branch on the five following areas:

One, expanding Privacy Act coverage. CDT agrees with the GAO's basic assertion that the Privacy Act key definition of System of Records is out of date. We believe that this issue must be addressed in legislation and urge the Committee to introduce such legislation in this Congress. We suggest a new definition that would ensure coverage of all information that reasonably can be expected to identify an individual.

Two, closing Privacy Act loopholes. CDT also urges the Committee to consider legislation that would limit the "routine use" exemptions. As GAO found, there are simply no current standards across the government for this exemption, and agencies have filled the void with an array of confusing and overbroad loopholes.

In addition, we urge the closing of another common loophole. Congress should make it clear that the Act's core principles apply to commercial data used by government.

Three, improving Privacy Impact Assessments. As we testified before this Committee last year, CDT supports the creation of best practices for Privacy Impact Assessments as called for in the E–Government Act Reauthorization Act, recently passed by this Committee. CDT urges the Committee to require PIAs for any program that uses commercial data, whether the personal information will be stored in the agency or kept outside of the agency. CDT also supports requiring PIAs for systems of government employee information.

Four, improving privacy leadership. When Peter Swire was chief privacy counselor, privacy had a higher profile within the Federal Government than at any other time. While Professor Swire is a unique leader in this space, CDT believes that a similar permanent Chief Privacy Officer within OMB written into law would help ensure that agencies understand the importance of this issue to Congress, to the next Administration, and to the Americans that you represent.

CDT also urges the creation of an independent Chief Privacy Officer (CPO) Council with a similar structure to the Chief Information Officers (CIO) Council and to the Chief Financial Officers (CFO) Council as well.

And five, increasing and improving privacy reporting and audits. OMB requirements for privacy reporting are a major leap forward in focusing attention on privacy issues, but getting the right implementation and accountability processes in place is an essential goal. Most importantly, OMB should be required to create standardized measurements for privacy-protecting processes. CDT also believes that the Committee should require that the systems of greatest privacy risk undergo regular audits by Inspectors General and/or, when the IGs are overwhelmed or not experts in privacy, by third-party audit firms.

In conclusion, I would like to urge this Committee to act this year. In the past, CDT has called for the creation of a new 1-year commission to study the Privacy Act and privacy policy in the government and offer solutions. But with the release of these GAO reports and numerous hearings on this and related issues in this Congress, we believe that the basic work that would have been done by such a commission has already been completed. There is now consensus around a set of recommendations for action by Congress and the Executive Branch to fill gaps and loopholes in privacy law and policy. CDT urges this Committee to draft a bill with the recommendations outlined above and quickly bring it to the Senate floor so that the next President can have the right tools in place upon taking office and can get started immediately on strengthening privacy in the Federal Government.

We look forward to working with you, and we thank you for your leadership on this important issue.

Chairman LIEBERMAN. Thanks very much, Mr. Schwartz. Thanks for your specific proposals, too, which are very helpful to the Committee.

The final witness this morning is Peter Swire, the C. William O'Neill Professor of Law at the Moritz College of Law of the Ohio State University. I want to express relief that I have been able to announce that when Senator Carper is not here because as a very zealous Ohio State graduate, he probably would have created a disruption of some kind. [Laughter.]

Mr. SWIRE. There was some discussion of whether to make it——

Chairman LIEBERMAN. Yes, the Big O, right. Also, Professor Swire is a Senior Fellow at the Center for American Progress specializing in privacy issues. From 1999 to early 2001, during the Clinton Administration, he served as the Chief Counselor for Privacy in the U.S. Office of Management and Budget.

Thanks very much for being here, and we welcome your testimony now.

**STATEMENT OF PETER P. SWIRE,[1] C. WILLIAM O'NEILL PROFESSOR OF LAW, MORITZ COLLEGE OF LAW, THE OHIO STATE UNIVERSITY**

Mr. SWIRE. Thank you, Chairman Lieberman, Ranking Member Collins, and Senator Akaka, for your attention to these issues today. And thanks to your Committee and the E–Government Act of 2002 for really making Privacy Impact Assessments a major tool across the Federal Government. This Committee has been vital in

[1] The prepared statement of Mr. Swire appears in the Appendix on page 87.

protecting and addressing these issues. And it is a pleasure, as we have heard across the panel today, being on this panel, that GAO has been really a major source of expertise in government-wide attention to privacy for a number of years.

At Homeland Security, Hugo Teufel and his predecessor have really built what has become the leading office in any Federal agency on privacy issues, and Federal Computer Week, for instance, earlier this year recognized Becky Richards of the office for her outstanding achievements for compliance in privacy. And so it is good to see that kind of recognition from the outside world.

And Ari Schwartz has been obviously a leader on these issues for quite a few years now, and we appreciate that.

In my statement today, I am going to talk about two issues and then briefly mention a third. I am going to try to give some of my experiences at OMB and some lessons for what that means going forward. The main technical substantive issue today is on biometrics. I am going to talk about an emerging issues, fingerprints and things like that, where I think the Committee really should consider action.

And then in my written testimony, we talk about a third issue that I could get to in questions, but I am not going to address it in detail. The Center for American Progress released a report earlier this month called "The ID Divide: Addressing the Challenges of Identification and Authentication in American Society." We put together a working group over a period of a year to address a wide range of issues—homeland security, immigration, voting, privacy, and security. And so we have a series of recommendations about how a process to look at identification systems would be a good thing to bring into the Federal Government as they address this generally going forward.

So turning to OMB and my 2 busy years there, I have five points to sort of bring up from that experience. And the overarching theme is that in an information-sharing world, we have tried to break down the data silos. We have tried to make sure that information gets shared across agencies. But, unfortunately, we have put the silos back in when it comes to privacy protection. So we have an agency over here and an agency over there with separate Privacy Officers, but no overarching structure for handling privacy across agencies. And I think that has really been a lack for the last number of years.

So to get to my list of five things, during the time that I was at OMB as a political appointee, a policy official, the first thing we did was coordinate across agencies. For instance, Ari Schwartz of CDT released a study just a couple of months into my time showing we had forgotten to put privacy policies up on Federal agencies. And that was deeply embarrassing, but it was also deeply helpful because within 4 months we got all the major Federal agencies to have privacy policies up. We saw a problem and could fix it.

During that time, at the CIO Council we created a Privacy Committee, which was active during that time, which made Privacy Impact Assessments a best practice at that time. And so the E–Government Act was able to build on some things that happened in the agencies when the time came. So the first point is to coordinate across agencies.

The second point is to act as a source of expertise. We answered Privacy Act questions from around the government. When the Health Insurance Portability and Accountability Act (HIPAA), the medical privacy rule, was happening, I served as White House coordinator for that, and the interagency issues were informed by somebody who does privacy across agencies. Similarly, when the Gramm-Leach-Bliley Act was being put into effect, there were many different agencies involved, and we served as a background source of expertise on privacy issues.

A third point, which people in Congress and the government would appreciate, is our role in clearance. You know that in the Federal Government, the moment they decide to testify, it all goes through OMB. And I was in OMB, and when there was a privacy issue, it got routed to my office, and we were able to comment with a consistent, informed view on how to handle privacy issues.

The way it works in Homeland Security is Mr. Teufel would get to see things as they are happening at DHS. But when it goes to OMB, that is somebody else's job at that point. It is the next step in the process. So having somebody at the central White House level really makes that job work better.

A fourth point is that I was available for special projects. In 2000, the Chief of Staff, John Podesta, asked me to chair a White House task force on a tricky set of issues. How do you update our wiretap laws for the Internet age? We had telephone wiretap laws. How does it work for the Internet? And I chaired a 14-agency task force with all the intelligence agencies, but it meant there was some privacy expertise in the room to work together with the agencies who most were focused on gathering information. And we came up with recommendations that year.

And then the fifth point about this OMB position was I could serve as a single point of contact. People knew who to yell at. The press knew who to call. The public could come to us. For the privacy groups, industry groups, and government agencies, there was one place to go for a forum and a way to talk about these issues going forward.

So I think those five points suggest some real usefulness to having a policy official in the White House structure that focuses on privacy going forward.

There is one lesson, I think, that I learned from that time—that it helps to have it be a statutory position. The position of the Administration when I was there was, because I was not statutory, I was not appropriate to testify in front of Congress. So I had to brief other people every time we had a privacy-related hearing. And I think that having a statutory position would help make sure that Congress would be well informed on these issues going forward.

I am now going to shift to talking for the remainder of my time on biometric issues, which I think is a major emerging issue. It is vaguely covered by the Privacy Act but has not gotten the attention. We have new videos up today at the Center for American Progress Web site on this. But I highlight this in part because President Bush signed Homeland Security Presidential Directive 24 (HSPD–24), his guidance on biometrics, on June 9, 2008, using words like "expanding" and "maximizing" the use of biometrics.

The guidance mentions privacy, but does not provide any implementation of what that is going to mean going forward. And here is the sort of background for concern.

Computer scientist Terry Boult has raised an issue called the "biometric dilemma." The more you use biometrics, the less secure they become. And the reason is the more you use secrets, the less secret they become. And so, in particular, when you think about fingerprints—Secretary Chertoff said not too long ago in a press availability that it is very difficult to fake a fingerprint. But that is not true. You can do a highly advanced research task. Go to Google or your favorite search engine and put in "fake fingerprint." And on the first page, you will see multiple articles about how to do that for under $10. Unfortunate, but true. Go do it. You can do it on your BlackBerry probably while we are having the hearing.

And how effective are these fake fingerprints? Well, Bruce Schneier, a famous security expert, tested one of the techniques, and he reported, "against 11 commercially available fingerprint biometric systems, it was able reliably to fool all of them."

And so we have a situation where fingerprints become the new data breach problem. If we have great big Federal databases full of fingerprints, those are data breaches waiting to happen. If you lose your Social Security number or your credit card number, you can, you hope, get a new one. You lose your fingerprint, it is very hard to get a new finger. And so we have this systematic security problem, data breach problem going forward if we have these huge government databases maximizing and expanding, as the recent directive said.

There are things to do about this, but they have not been done yet. And so in my testimony, I suggest a couple of actions this Committee could consider immediately to start to do the work on biometrics that I think would be helpful.

The first idea—and this is part of data breach laws generally—is to encourage encrypting transmission of things like this, biometrics, and encourage encryption when you store them. And so I suggest the E–Government Act of 2002 can be amended to provide a default for storing and transmitting biometrics in encrypted form. An exception to this "always encrypt" policy should be permitted only if it is justified in a Privacy Impact Assessment, only if it is really a good idea, and if it has received specific authorization from the Chief Privacy Officer for the agency. So I would like Mr. Teufel to have to sign off on it if we are going to have unencrypted uses of biometrics around the agency. And it may have to be considered whether in the private sector this should apply as well because if the private sector compromises these biometrics, then the government cannot use them either.

A second point going forward is that access to biometric databases should be very well audited. We saw with the passport records of the Senators how audit can be helpful in sending a message and training people that they should not be messing around in people's files. Biometrics going forward can be compromised, and we should audit the possibility.

And then in the written testimony, I also talk about some promising new biometric technologies that are more privacy protective. One is called biometric encryption. And I suggest reports are ap-

propriate. You could ask Homeland Security and the Justice Department Privacy Office to do reports on these technologies so that they have to say what works, what does not, whether pilot programs are appropriate to fix this.

In conclusion, when it comes to biometrics, I will go back to an analogy I used when the Homeland Security Department was being created 6 years ago and I testified in Congress. Too often, we see this as if it is a truck where we only have an accelerator for some of these uses, but no brakes. And the concern with new technologies, if we simply expand biometrics without the brakes, is that we could compromise our fingerprints and our biometrics for a generation and we cannot get them back, so we should build them right in the first place. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks, Mr. Swire. Very interesting and obviously informed and helpful testimony. We will do 6-minute rounds of questions and keep going until we are finished with our questions.

Ms. Koontz, let me begin with you. The GAO report highlights a longstanding concern, which is that agencies are sharing and using personal data for purposes beyond the original stated purpose. I wanted to ask you to give us a few examples that you found in your work of that and indicate to us how widespread you think the practice is.

Ms. KOONTZ. I think that what we were covering in our report is that there are only really very modest limitations in the law on sharing. Within an agency, the information may be shared as long as it is necessary for an employee to do their job. Outside of an agency, it can be shared pursuant to a routine use, but I think that all the panelists have commented that routine uses over time have become very numerous, very broad, and do not serve as a very useful way to limit the sharing of information.

Chairman LIEBERMAN. And, again, this is sharing between agencies of the Federal Government.

Ms. KOONTZ. Yes. I think we also make the point, though, that as we move toward an information-sharing environment, in the wake of September 11, 2001, we realize we need to share information better than we have in the past. In some cases, information also needs to be shared with State and local governments, and it needs sometimes to be shared with the private sector.

One of the concerns that we raise in our report is that the Privacy Act does not ensure in all cases that the privacy protections travel with the data; that is, there are not onward transfer provisions that make sure that the protections travel with the data when they go outside the hands of the original collector and maintainer of the information. So I think that is a definite concern going forward that we need stronger protections because we foresee that there is going to be more sharing. We need stronger protections to ensure that the information is protected consistently as it travels.

Chairman LIEBERMAN. You are quite right that a real focus for us on information sharing, again, started in this Committee with the legislation based on the 9/11 Commission Report, which found that, to use the familiar metaphor, there was no place where the dots were located together so that they could be connected to try to prevent September 11, 2001, from happening. So there is no

question that what we are trying to do is really encourage—and, insofar as possible, mandate—the sharing of information for national security or homeland security purposes.

But is that the major area in which you are concerned? My own concern was that other agencies, unrelated to security work, are collecting information on American citizens and, beyond the stated purpose, sharing that information with other agencies for matters unrelated to security.

Ms. KOONTZ. I am not sure that I can give you any examples where people actually exceeded the purposes for which it was originally collected. I think our concern is that it can be shared pursuant to all kinds of routine uses, and they are so numerous and broad that there are not really meaningful bounds on the sharing of information.

Chairman LIEBERMAN. OK. What are possible solutions to this problem?

Ms. KOONTZ. In terms of sharing?

Chairman LIEBERMAN. Yes, sharing among agencies that goes beyond the original purpose for which the information was collected.

Ms. KOONTZ. Right. It is a very important part of privacy that the information be only used in the way that is consistent with the purpose for which it was collected. So when the government told the person when they collected the information in the first place that this was the purpose, we need to handle that consistently over time.

There are a couple things. First of all, in the System of Records Notices, in the public notices under the Privacy Act, there is not a requirement to state an overall purpose. Agencies are supposed to state purposes for each of the routine uses, but not an overall purpose. We think that requiring agencies to state the overall purpose of the collection is important. It is also important that they be very specific about that purpose so that it serves as a useful constraint.

We also think that there should be mechanisms so that when information is shared outside an agency, that there are agreements with outside entities that will constrain the use of that information and provide protections to it.

Chairman LIEBERMAN. That makes sense. Mr. Teufel, just to state again the obvious, in the case of a lot of information that the Department of Homeland Security and, obviously, the National Counterterrorism Center have, the original purpose, if you will, that Congress has mandated is that you share the information for the collective good. Why don't you talk a little bit about how you react to this question about the original purpose being exceeded?

Mr. TEUFEL. Sure. Well, first of all, I do not think I have an answer. Second, what I am going to tell you may run over my time, so with the Committee's indulgence, I will do the best I can to answer the question.

Chairman LIEBERMAN. Go ahead.

Mr. TEUFEL. We think a lot about routine uses. You may be aware, and Ms. Koontz, in a report that she did on my office last year, mentions that we have 208 legacy agency System of Records Notices. So these are System of Records Notices that could be from Department of Energy, Department of Transportation, or Depart-

ment of Justice, and every agency approaches System of Records Notices differently.

Chairman LIEBERMAN. Just for the record give us a brief definition of what that means, what a System of Records Notices is.

Mr. TEUFEL. A System of Records Notice is a document that is required to be published under the Privacy Act of 1974 when an agency has a System of Records. A System of Records is a collection of information about U.S. citizens or legal permanent residents that is accessible by some unique identifier. So there are a lot of databases out there, and this is one of the things that others will talk about, that you can have a database that has personally identifiable information in it, but it will not be, under the definition in the Privacy Act, considered a System of Records. And, accordingly, there is not a System of Records Notice published in the Federal Register. We put them up on our Web site.

So we have 208 legacy agency System of Records Notices (SORNs), and we are determined by the end of the year to update as many of those as possible. So the first thing that we did was we revised our guidance that is up on our Web site on how to conduct and prepare a System of Records Notice, and we looked at routine uses. And often there are routine uses that agencies will have, and they will just publish lists of routine uses that apply to every System of Records Notice at the agency. We do not do that. We do have a template where we list standard routine uses that one might see. Some may be for State and local information sharing. It might be for health purposes, law enforcement purposes, those sorts of things. But we do not have blanket routine uses that we have published. We look at each and every System of Records Notice when we decide which routine uses go into that particular document.

So we have these 208 System of Records Notices out there, and over the last few months, my office and a contractor have gone through all of those to look at the different approaches and to see where we can harmonize and reduce. And this is something that Ms. Koontz had recommended in a report last year. There is a requirement under the Privacy Act, and I think it is OMB Circular A–130, that we, every 2 years, go through and look at System of Records Notices to make sure that we actually need the information and what are we doing with it.

So we have made tremendous progress, and we have draft System of Records Notices for all 208. Many we will consolidate and go under government-wide, Executive Branch-wide System of Records Notices. Others will be DHS-wide, and for the remaining, they will be component-specific SORNs. So that is part of the answer.

The other part of the answer is information sharing, and it is something that my office really has been grappling with, and in the remaining time in my office, it is one of two fairly major priorities, the other being cyber security. How do we do this? How do we do information sharing as Congress has mandated we do, but we do it in a way that is privacy sensitive? And I do not have an answer for you. We are working on this issue and working very closely with our colleagues at the Department of Justice and the Office of

the Director of National Intelligence, as well as the program manager for the information-sharing environment.

Chairman LIEBERMAN. That is a good answer. Thank you. Senator Collins.

Senator COLLINS. Thank you.

Professor Swire, I want to follow up on some of your comments on biometrics. Biometrics have really been sold to Congress, and I think to the public and by the Department of Homeland Security, as the answer. I, therefore, was very interested in your comments about the ability to fake fingerprints, for example, because I believe as your testimony said and as I recall, Secretary Chertoff has been quoted as saying, that it is very difficult to fake a fingerprint. And I think you are telling us today that it is not.

The U.S. Visa Waiver Program is based on having biometrics included in the exit program so that we can track who is here and who is leaving our country. So I am particularly interested in your analysis of the rush to embrace biometrics and whether they really will result in a better, more secure system, and also your red flags about the need for encryption.

Do you know whether or not the Transportation Security Administration (TSA), for example, which is using biometrics for the new Clear system at airports to speed on the way travelers who have given the Department biometric information, do you know if that system is using encrypted data when it is being used at the test airports around the country?

Mr. SWIRE. Thank you, Senator. I have not reviewed the Clear system in particular, so I do not have an answer on that.

I think that when it comes to biometrics, there are vendors who are trying to sell systems, and they want to have people believe it is a good answer. And I also think that there is enormous pressure to sort of do something, to come up with secure ways to do things. And if our current things do not work very well, we want to move to the next generation, and biometrics has seemed tempting.

The fact that fingerprints are easy to fake, the basic way you do it and the simplest method is if I have a picture of your finger, I just—nowadays, pictures come in my cell phone, for instance. I just blow it up, put it on my computer, and photo-shop it a little bit, and then I am able to print it out on a laser printer—this is pretty standard—and I can then get Gummy Bears or similar gel from the CVS and put it over my finger. And that is basically what it takes.

You could have fancy machines, which is not what we mostly have, that could make sure the pulse is pulsing and things like that. But the basic idea that I just put your fingerprint on top of my finger is very easy to do.

So that is known, and biometrics researchers, the sort of academic ones who are not trying to sell their products, have long lists of articles explaining these vulnerabilities. And that is why I think reports from the agencies, maybe including the Privacy Office, to really look at these might be one very specific step so that the eagerness to do things can be tempered by making sure we get the technical part right.

Senator COLLINS. Well, it is particularly interesting to hear you say that, because several years ago, when I was the Chairman of the Permanent Subcommittee on Investigations, we did an inves-

tigation on how easy it was to counterfeit identification using readily available software on the Internet. And, indeed, my staff counterfeited, I think, a dozen different IDs for me, licenses in five different States, a college ID—probably that one would not have been——

Mr. SWIRE. You should be careful doing those. There are some laws about that.

Senator COLLINS. Exactly. [Laughter.]

Well, I can tell you that the law is a lot stronger after we did that investigation. But there were real loopholes in the law as far as making that illegal if it is done through the Internet. So we are constantly trying to catch up with our laws and our policies to the technology that is out there. And your comments on biometrics are an excellent caution to us because it has been sold as the way to have secure IDs. And now I am hearing from you that just as my staff was able to easily locate the technology on the Internet to counterfeit identifications, now you are telling me that we could do that with fingerprints as well.

So it seems to me there are two issues here. One is: Is this technology really increasing security? The second is: How do we protect individual fingerprints from being counterfeited and used by those who would do us harm.

Mr. SWIRE. If we do it badly, our fingerprints will get out there. They will be breached, and they will be out there. And we cannot get them back, right? So that means for our generation that fingerprint will be an insecure identifier. And that is a reason to be a step or two more cautious because if you screw it up, you have done it for a generation of people.

Senator COLLINS. Well, that is why I want to follow up with TSA on the Clear system and what the protections are, and I am going to turn to Mr. Teufel to see if he knows the answer to that.

When the fingerprint and other information that is given to airports that are being used, it it encrypted? Is it retained at the airport and, thus, subject to misuse?

Mr. TEUFEL. Sadly, the BlackBerry is a wonderful thing, but it does not always give me an answer as fast as I might need it.

I do not know the answer, but I can tell you that on our Web site, dhs.gov/privacy, we have privacy documentation posted, and I believe the answer may be in there. And I will be talking with TSA's Privacy Officer, Peter Pietra, on this when I get back. So I am just hesitant to give an answer without being informed.

Senator COLLINS. If you would get back to us on that issue, that would be helpful.[1]

Just quickly, because my time is expiring, Mr. Teufel, what do you think of the idea that Mr. Schwartz and Mr. Swire have raised about having a Privacy Officer at OMB designated in law so that it does not depend on the interests of a particular Administration to help provide government-wide guidance on privacy issues? Would that be helpful to you? Or would it be just another layer of bureaucracy?

[1] Response from Peter Pietra to Senator Collins appears in Mr. Teufel's response on page 36.

Mr. TEUFEL. Well, I do not think it would be another layer of bureaucracy, and certainly as a Privacy Officer, I like Privacy Officers.

Senator COLLINS. Some of your best friends. [Laughter.]

Mr. TEUFEL. Some of my best friends are Privacy Officers. But my one concern would be I am just a Privacy Officer for DHS, and I am hesitant to speak beyond my role at DHS. And also I am mindful of the head of OMB's ability to manage his or her office.

Senator COLLINS. But just your personal opinion—I realize you are not speaking for the Department or the Administration. But you are on the front lines day in and day out in the Department, that, other than the VA and the Department of Health and Human Services (HHS), has the most information about Americans, and the Internal Revenue Service (IRS), I suppose.

Mr. TEUFEL. Yes, ma'am. I work very closely with Karen Evans at OMB, and I think very highly of her. She co-chairs the Privacy Committee within the CIO Council, and she has designated me to be the Chair of the Cyber Security Subcommittee of the Privacy Committee. I think it is a good approach, and I like working with her. I think she has provided some excellent leadership in the role as the person I interact with on a regular basis at OMB for privacy issues.

Senator COLLINS. Thank you.

Chairman LIEBERMAN. Thanks, Senator Collins. I just want to point out that Ms. Evans is the E–Government person at OMB.

Mr. TEUFEL. Yes, sir.

Chairman LIEBERMAN. So she is not, as you know, a full-time government-wide privacy person.

I just want to make sure I understand what you said, Mr. Swire because it is important to the Committee. What you are saying is obviously you have to get somebody else's fingerprint to be able to compromise the biometric system.

Mr. SWIRE. Yes.

Chairman LIEBERMAN. So your concern is about the security, quite consistent with what we are focused on today, of fingerprints that the government has in its possession.

Mr. SWIRE. And, in particular, if there are databases that the government holds where they just have lots and lots of fingerprints in there, if you have a breach of those databases, then all those people's fingerprints become compromised.

Chairman LIEBERMAN. Right, with very significant consequences.

Mr. SWIRE. Even if it is encrypted at Clear or out at the edges, if the database is lying around subject to breach, that is a risk.

Chairman LIEBERMAN. Right. That is a good point. Senator Akaka.

Senator AKAKA. Thank you very much, Mr. Chairman.

GAO's report lays out some solid suggestions about ways to strengthen our privacy laws. However, one of the major issues not discussed in the report is the list of exemptions to the Privacy Act for law enforcement and intelligence activities. I believe that this issue merits some discussion since the major privacy arguments over the past few years have been with the treatment of personal information in the national security and homeland security context.

Can each of you discuss these exemptions and whether you have recommendations for changing these sections of the Privacy Act?

Ms. KOONTZ. I will start us off. The exemptions are definitely an issue. They did not come up specifically in the work that we did, but we think that, going forward, any reconsideration of the provisions of the Privacy Act will have to include debate about the law enforcement exemptions and the general and specific exemptions in the Privacy Act.

Mr. SWIRE. This is related, in my mind, to the information-sharing environment set of issues because that is where it comes up a lot of the time. I wrote an article called "Privacy and Information Sharing in the War Against Terrorism." It came out about 2 years ago. And it was an attempt to—this was after I had worked on the Markle Task Force, which did a lot of information-sharing work.

I think it is somewhat difficult to address it within the Privacy Act itself, but what the article called for was an expanded process, a sort of due diligence process or an expanded Privacy Impact Assessment process, at the time that you create new information-sharing programs. I think when you are building each one of those programs, an expanded list of questions about how to look at it, what should be shared, what should not, how do you minimize, and the rest, that might be the best way day in and day out to try to address that.

Mr. SCHWARTZ. I will say, Senator, it is a good question. I am hesitant to touch the more general exemptions, especially the law enforcement exemption. I think that exemption actually is, compared to other law enforcement exemptions, pretty tailored for the Privacy Act and fits into the Privacy Act pretty well. The problem that we have had is more of these routine use exemptions where we see lists of 30 or 40 exemptions that the agency is just making up at that particular time. So if you have a set of 40 exemptions for a particular program that, as Ms. Koontz said, does not have a main purpose listed in the first place so you cannot compare the main purpose to these exemptions and try and figure out how they should be used, it is basically giving a complete loophole for sharing of the information for many purposes, and maybe for any purpose, if these exemptions are written widely enough. And I have even spoken with agencies, and with the Postal Service, for example, where there was a System of Records Notice that they put out a number of years ago, where I questioned the existence of some of the routine uses. And they said, "Well, those are just our blanket routine uses; we always put them in there. We agree with you they do not make sense for this particular program, but those are the ones we always use."

So then they went back and they changed their blanket exemptions because of our concerns based on that. But most agencies have not done that. As I mentioned in my testimony, the Department of Defense has 16 routine uses that they use for every collection of information. Obviously, not every collection is used in exactly the same way 16 times. It makes sense to look at how that particular program is being used and say this is how we plan on sharing it. If we want to do something different, we have to put out another System of Records Notice. We have to make a commitment to the American people that we are going to let them know what

this system does and how we are going to use that; and if we change that, we have to let them know how we are changing it.

Mr. TEUFEL. So what I would reiterate is that we do not at the Department of Homeland Security have blanket routine uses. For every System of Records Notice, we think about each and every routine use individually. Do we need this routine use in this particular System of Records Notice? So we are very thoughtful or we seek to be very thoughtful in terms of what we include in a System of Records Notice.

With respect to law enforcement and intelligence exemptions, I can think of a number of occasions when I have had a number of senior staff in my office, and we have gotten out our Department of Justice Privacy Act guide and gone through and looked at the case law and discussed what the meaning is of the particular exemptions and how they apply and whether they apply in a given System of Records Notice. And so I can tell you with respect to my agency—I cannot speak to others—that we seek to be very thoughtful in the use of those exemptions and to make sure that they are appropriate for a particular system.

Senator AKAKA. Thank you. I have been concerned about the impact of data mining on the protection of personal information in the Federal Government for a number of years. This includes the use of commercial data for data mining. Could each of you discuss how the Privacy Act could be amended to cover data mining and the use of commercial data? Ms. Koontz.

Ms. KOONTZ. I think one thing that could be done is to expand the protections of the Privacy Act to all personally identifiable information regardless of whether it is retrieved by a personal identifier or maintained in some other kind of way. We actually have done a number of studies about data mining and seen how much it has increased in recent years, as well as other analytical initiatives. And it is true that the Privacy Act does not currently always cover data-mining kinds of initiatives, but this is one way that it could.

As far as information resellers, one of the reasons that it is not always covered by the Privacy Act is that the Act says that the government has to maintain the information. So it means if someone merely pings a database or looks at a database but does not retrieve the information and maintain it, the protections of the Privacy Act will not apply in that case.

Some language along the lines of "systematic use," focusing on use rather than maintenance of the information, might be an appropriate way to treat that reseller information.

Mr. SCHWARTZ. First, I would like to strongly agree with everything that Ms. Koontz just said, and those are two excellent points. The first one that she made on the information and identifiability of information I think is a key one. The way that the Privacy Act was written, the question was whether information is actually being retrieved by name, by Social Security number, by a specific identifier. In data mining, you are not doing that. You could have a database that has 200 times more personal information, than what is considered a System of Records today, where you are searching on someone's actual Social Security number, and use this new database for data mining where you are searching not on the

person's name, not on the person's Social Security number, but for attributes about them. Then that pulls out names and information, and that would not be considered a Privacy Act System of Records today or covered under the Privacy Act.

It gets very confusing, but the basic problem is that we set up this system, this law, with the idea of what a database in the 1970s looked like, where you would search for a particular identifier or a particular person's name. We do not do that today, and data mining is one key example where you do not do that at all today, and the privacy sensitivity may actually even be greater than in the kind of database that the Privacy Act was written for, although clearly the goals of the Privacy Act cover this. And I think some of the agencies have taken that idea and said, we have to write Privacy Impact Assessments for this kind of data; we should take a step further and make sure that this is protected. But it is not clear that is being done across the government, and we need to make sure that is protected.

Mr. SWIRE. Can I just respond? This is the single place where technology has changed the most since the 1970s. I think this is echoing what we just heard. In the 1970s, you had things in files retrieved by name. Today we have things called "Search," and we can go through huge databases. And so changing that is the core of how technology has been changed. There are some ideas in the GAO report about ways to possibly do it, but it is worth recognizing this is the one place where the technology has really shifted and the law has not caught up.

Senator AKAKA. Mr. Teufel.

Mr. TEUFEL. A couple of very quick things here. First, I note that my office is holding a workshop on data mining. I do not know if we have the *Federal Register* notice out yet, but I think we have scheduled it for July 24 and July 25, and we will be looking at coming up with best practices.

Second, the Homeland Security Act talks about data mining and, if I am not mistaken, talks about the Department looking at data mining and doing data mining.

The third thing is what is the definition of "data mining," and my office has issued a series of reports over the years—I think in 2006, 2007, and 2008—and every year we have a different definition to look at. So without getting into what those definitions are, it is important to note that when we talk about it, we need to have some common frame of reference.

And then, finally, with respect to information resellers, our Data Privacy and Integrity Advisory Committee has issued some reports on that. One of the things that has come out of those reports has been that in our PIA guidance, we have made some changes so that we ask the question, and then we publish in our Privacy Impact Assessments whether information is being used that comes from information resellers.

Senator AKAKA. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks, Senator Akaka. We will go now to a second round of 6 minutes for Members who have questions.

One of the Fair Information Practices underlying the Privacy Act is so-called "data integrity," the importance of ensuring that personal information the government collects is accurate. When this is

not the case, it obviously increases the risk that individuals will be subject to unfair treatment, in this case not only based on violation of privacy but on the inaccuracy of the personal data.

I know that people who spend a lot of time in this field have said that inaccurate and incomplete information, so-called "dirty data," is a large problem in some government programs. And, Ms. Koontz, I wanted to ask you first about that. Is it a large problem? And is the government investing in technologies to monitor and improve data quality? For instance, one of the places we have heard it is on the so-called no-fly list, that there is a lot of names there that may not be quite right.

Ms. KOONTZ. Obviously, data integrity, a big issue across government and in the privacy area. The principle really talks about the fact that the data has to be accurate enough for the purpose for which it is used. So, again, it has to be tied to that purpose. Accuracy for one purpose may not be enough for another purpose. The no-fly list may need a higher level of accuracy than other ones.

We did not do a compliance audit across government in order to determine to what extent agencies were complying with these various principles. I will say that when we did our report on Privacy Act compliance a number of years ago at your request, we did point out that while there was sort of mixed compliance across the Federal Government, one area was data integrity that needed improvement across 25 agencies that we looked at at that point.

Chairman LIEBERMAN. Mr. Teufel, what is your experience with this in the Department of Homeland Security? Do we have a dirty data problem in accurate information being collected?

Mr. TEUFEL. Well, I think government always can work on improving the accuracy, relevance, timeliness, and completeness of data that it has. So I do not think I can answer any way other than we can always do a better job, and part of our effort in looking at all of these legacy SORNs and revising them is considering this very issue.

I also note that, as we discussed earlier with respect to law enforcement and intelligence exemptions, there is an exemption with respect to accuracy, relevance, timeliness, and completeness when it comes to law enforcement and intelligence information. And so while I am a Privacy Officer and not an intel guy or not a law enforcement guy, I have to at least on behalf of the agency mention this, that in those contexts you cannot have necessarily accurate, timely, complete information because you have sources and methods, some of whom or which you cannot attest to the veracity of. You get information that comes in, and you will have to assess it and determine its credibility, but it may not be accurate, timely, or complete.

Chairman LIEBERMAN. OK. Mr. Schwartz, and Mr. Swire, let me get you both into this question of so-called dirty data. Is it a significant problem, inaccurate information, personal information being held by government agencies? And if it is, are there any mechanisms that we should be putting into place to try to clean up the data?

Mr. SWIRE. Yes, in our ID Divide report, we have about four pages on dirty data problems, and the place that really hits home is on matching programs. So, for instance, under the Help America

Vote Act, there is matching where you delete voter rolls if you think there is not the right person signed up. Under E–Verify for new hires, you can say somebody is not eligible to work. And there has been very high levels of error reported and we have detailed footnotes because of this dirty data problem.

What you see is numbers like 3 percent, 5 percent, or 10 percent of all records have inaccuracies in them, depending on which thing you look at. And if you then say you are not eligible to vote, you are not eligible to get a job, you are not eligible to get a driver's license at that 3- or 5-percent level, that is a lot of people's lives that are getting hit.

And so dirty data directly affects people's lives if they get turned down at the Department of Motor Vehicles (DMV) and have to try to figure out how to get a driver's license. And so that is where you really see it, and those are big numbers, millions of people.

Chairman LIEBERMAN. Those are big numbers. So how do we deal with that? I mean, just at the beginning somebody input the data inaccurately or did not have accurate information?

Mr. SWIRE. It is a long list of things that happen. You type it in wrong, or somebody read the reader wrong. But also you have nicknames—there are lists of ways. I think that you need to have redress procedures. You need to have second ways for people——

Chairman LIEBERMAN. Give me a little more definition of what a redress procedure is.

Mr. SWIRE. OK. Let's say I go to the DMV and they say you cannot get a driver's license because your match is not right with Social Security or something. There has to be some way for me as a normal person, not having to hire a lawyer, to be able to say, look, there is a mistake here, work with me on this. I am an American citizen. I am supposed to be able to get a driver's license. Social Security says I do not have a match.

And how those day-in, day-out procedures work when you get the bureaucratic "no" is something I think we have not spent enough time talking about. If we are going to be matching databases and we know there are going to be errors, we have to have ordinary ways for ordinary people to get it fixed.

Chairman LIEBERMAN. I agree. Mr. Schwartz.

Mr. SCHWARTZ. I agree that it is not going to be perfect, and I think Mr. Teufel's points are well taken. However, I do think that it is a widely acknowledged problem in the Federal Government. I think pretty much any agency you speak to directly, speak to their Chief Information Officers, and they will say, yes, that this is a problem not just with my agency but with every agency across government. And it is something that we need to address.

The important piece here is, to get to the point that Professor Swire was speaking about, that we do not think of privacy as the barrier to getting to better data. There are a lot of times where people talk about privacy as a bureaucracy that is in place on top of putting these kinds of systems in place. In this case, I think that privacy actually is helping greater efficiency by making sure that you have the correct data. By including people in the redress process and by coming up with a redress process that works efficiently and effectively, that is not adding bureaucracy to the system. That is making sure that the information you have is correct and works

efficiently. So if we can get that kind of process in place where we are correcting data, where we involve the data subject, where possible, into that process, I think we are going to end up with more efficiency down the road, although it is going to take longer to clean up the data in the short term.

Chairman LIEBERMAN. Mr. Teufel, do you want to add something quickly?

Mr. TEUFEL. Please, if I may. Redress is an important issue, the ability to find out what information government has and then correct that information. And I note that at the Department of Homeland Security there is DHS TRIP, Traveler Redress Inquiry Program, which is a one-stop shop for people affected by things that happen at DHS to write in and seek redress. And it applies not just to U.S. citizens and legal permanent residents, which is one of the restrictions of the Privacy Act, but also applies to non-U.S. citizens.

Chairman LIEBERMAN. This is all done on the Internet?

Mr. TEUFEL. Yes, it is.

Chairman LIEBERMAN. And do you have any sense of how it is going?

Mr. TEUFEL. It has been awhile since I have looked at the figures, but from what I recall, it is very good.

Chairman LIEBERMAN. Good. Thank you. Senator Collins.

Senator COLLINS. Thank you.

We have talked a lot this morning about potential changes in the Privacy Act, the E–Government Act, and other laws. But the Fair Information Practices, the principles in that, which were developed in 1972, have proven very resilient because they are not technology dependent. They are principles like openness, transparency, and accountability.

I would like to ask all of you whether we should be considering, in addition to changes in the Privacy Act, any changes in the Fair Information Practices. And I will start with Ms. Koontz.

Ms. KOONTZ. I think you said it already. The Fair Information Practices have stood the test of time. The Privacy Act is based on the Fair Information Practices. The laws in many countries are based on Fair Information Practices, and over time, we have used them frequently in our work as a framework to look through to look at privacy protections. So I would not suggest anything specific.

Senator COLLINS. Mr. Teufel.

Mr. TEUFEL. As Privacy Officers, we live and die by the Fair Information Practices. So it is not making changes to them. I think it is adhering rigorously to them.

Senator COLLINS. Mr. Schwartz.

Mr. SCHWARTZ. I agree with that, but I think it is important to note that the Fair Information Practices have evolved over time. In the 1972 set, we had four listed, and now I think when you talk to most people, it is between eight and ten, depending on if you merged two together here or there. So they have changed over time. Ideas like data minimization, which was not in the original set, but is embedded in the Privacy Act, is now a term that we use pretty regularly today where you are getting rid of data. You are not collecting data you do not need, and you are getting rid of it

when you do not need it anymore. That is one example where we have had a shift over time.

But I think the basic Fair Information Practices still exist today, and they were written into the Privacy Act, and I think that is the structure of the Privacy Act that we need to keep and make sure that we do not tinker with the Act so much that we lose that structure.

Senator COLLINS. Professor Swire.

Mr. SWIRE. I agree with what was said, but there is one of them that is under huge pressure—the idea of no secondary use, that you just use the data for the reason you started with it, and then you do not use it for 100 other purposes. That is where the pressure is.

So within each agency, including the huge Homeland Security Department, it can go around for other purposes, not just the original purpose, and then these routine uses means it can go out of the agency to other agencies, and it can sort of be in a free zone.

And so I think that is the hardest thing, is which uses are OK and which ones are not. And it has been hard to figure out how to build that into law.

Senator COLLINS. Thank you.

Mr. Teufel, Mr. Schwartz noted in his testimony that there are times when the Privacy Impact Assessment is actually completed after the project has been developed and approved rather than being anticipated beforehand. Is this a problem at DHS?

Mr. TEUFEL. To the extent it is, it is less and less of a problem, and the reason for that is because of a couple of things. One is the increase in component Privacy Officers. Last year, I made a recommendation to Secretary Chertoff and he agreed that we ought to have more component Privacy Officers, and so in some of the operational components and department-level components that did not have Privacy Officers, there are now Privacy Officers. Immigration and Customs Enforcement (ICE) and Citizenship and Immigration Services (CIS) come to mind. TSA had a component Privacy Officer; still does. U.S. Visitor and Immigrant Status Indicator Technology (US–VISIT) has one as well.

So having folks on the ground out in the components makes a difference because they can work these issues and are much closer to the people at the programmatic level who are doing things.

The other thing is that we have been able to—and I hate to use the word—operationalize—just because I am not sure that is a real word. But we have operationalized privacy throughout the Department, so we have really infused ourselves into the bureaucratic process. And I do not use that in a pejorative way, but government is bureaucracy, and if you can get into the bureaucracy, you can make it work for you from a privacy perspective. And so we are doing better and better.

Now, there are always programs that pop up, and we hear about them. One popped up earlier this week, and I was after hours on the phone with senior officials from a component and the General Counsel's Office—Where are we? What is going on? And we will be able to get our work done before this program goes live. But sometimes we have to be very quick on our feet that we make sure that we do a thorough job but a timely job, even though the component

or the program folks have not told us early enough on what they are up to.

Senator COLLINS. Thank you.

Chairman LIEBERMAN. Thanks, Senator Collins.

Senator Akaka, next. And then we will conclude with Senator Carper.

Senator AKAKA. Thank you very much, Mr. Chairman.

Mr. Teufel, today GAO is releasing a report I requested that reviews the responsibilities of senior agency Privacy Officers across the government. According to the report, some agencies like DHS have placed all of the responsibility under one official while others have shared responsibility.

As the DHS Chief Privacy Officer, what do you believe are the benefits of having one individual responsible for privacy at an agency?

Mr. TEUFEL. Well, I think the benefits that Mr. Swire mentioned earlier, that single point of contact, the person who is responsible for privacy so that if there is a question or a problem, the public, Congress, and people within the agency know to whom to go for an answer, to get the situation resolved, I think it is important, but I recognize that every agency is different, and so some agencies may have less involvement with personally identifiable information. For others like DHS, a big part of the Department's success is reliant on personally identifiable information. So you have to have someone who is senior enough and who has access to the right people to go in and say, hey, I think there is an issue here, we need to talk about it.

And as I mentioned earlier in my opening remarks, at a lot of agencies it makes sense to have someone who is more of a technician than a policy person because the privacy issues may not be that great at other agencies, and DHS is among them. You have to have somebody who is involved with policy and somebody who can go into the front office and component leadership offices and talk about the issues and work out solutions.

Senator AKAKA. You mentioned having a person at a senior level. Where do you think this office should be set? At what level of an agency?

Mr. TEUFEL. I think it could be any number of places, and I think, whether it is an SES-level position or an executive schedule-level position, whether it is a direct report to the Secretary or perhaps somebody senior within the management or the Administration bureau or directorate, as I mentioned before, listening to Judge Baker, the important thing is that you have that access and that people will listen to you, that they have trust in confidence in you and that they will seek out your advice and counsel.

Having said that, there is value to reporting directly to the Secretary and Deputy Secretary.

Senator AKAKA. Yes. The reason I asked that is several years back, we wanted to bring about changes in accounting in Defense, and we set up an office for that. Two years later, the person that we were able to put there came to me and said, "I am resigning." And I asked, "Why?" He said, "Because I cannot make the changes that need to be made." He said, "It should be on a higher level."

This tells me that a privacy officer needs to be at a higher level to make a difference.

Mr. TEUFEL. I agree with you, Senator, and certainly when I have talked to some of my colleagues at other departments, senior career employees who are at the GS–15 level, I am not sure that at every one of those departments they are able to effectuate the policy changes that need to be made at those agencies.

Senator AKAKA. Thank you.

Ms. Koontz, I believe that it is extremely important for the public to be aware of how the Federal agencies are using their personal information. The GAO report suggests a layered notice with a summary of the most important facts up front, followed by a more detailed description. However, Privacy Impact Assessments, if done correctly, can provide more meaningful notice.

Could you elaborate how under your proposal Privacy Act notices could be more easily understood by the public and how they would interact with PIAs?

Ms. KOONTZ. Generally speaking, the problem with the public notices right now is that they are difficult to understand, they are treated as a legal compliance factor, and it may be hard for the public to identify which ones are in force. Publishing them in the *Federal Register* may not be the best way to communicate with the public. I mean, it serves a purpose, but I think in addition to publishing in the *Federal Register*, we think that publishing them on the Internet and some kind of centralized Web site, privacy.gov or something of the like, would be a good step to help the public be able to identify them. And then, second, I think the idea of layered notices really lends itself to a Web-type of presentation because you can provide an overall statement and then you can provide details if people want to go deeper into the statement and understand more about how the government is using information.

I agree that the Privacy Impact Assessments can be a useful way of communicating with the public. If the agency has done a good job talking about why they are collecting the information and talking about the trade-offs, that can be an additional way of communicating this to the public. My feeling is that privacy is a lot about transparency, and having both means of communications would still make sense.

Senator AKAKA. Mr. Chairman, may I ask——

Chairman LIEBERMAN. Please, go right ahead.

Senator AKAKA. Mr. Swire, you mentioned in your testimony a report you recently co-authored on identification in America. I believe this report is timely considering the fact that DHS is working to implement the REAL ID Act. As you may know, Senator Sununu and I introduced S. 717 to repeal provisions of the REAL ID Act and replace it with a negotiated rulemaking process that incorporates States' views and provides privacy safeguards. And you also know that some States have rejected the REAL ID Act for these same reasons.

What are your views on S. 717, and the REAL ID Act, in general?

Mr. SWIRE. Thank you, Senator. I support S. 717. I think it is useful, just for a few sentences, to explain why. REAL ID, as a process, never was debated in the Senate, never came through the

Committee process, etc. And I think as a statute, there were things that would have been fixed, more stakeholders could have been involved and all the rest, if it had a more thorough process.

Going to the negotiated rulemaking means that the different expert people, including the States, would be more deeply involved, and I think that would create a framework for a better long-term outcome.

Senator AKAKA. Thank you. Mr. Chairman, if I may, a short one.

Chairman LIEBERMAN. Sure.

Senator AKAKA. Mr. Schwartz, I understand that you are also a member of the Information Security and Privacy Advisory Board, which is working with the DHS Data Privacy and Integrity Advisory Committee to develop recommendations for revisions to the Privacy Act. And that is what we are trying to get at here.

Can you tell me the status of this joint effort and whether other changes to the Privacy Act are being considered outside of those listed in your testimony?

Mr. SCHWARTZ. Thank you, Senator Akaka. I actually just joined the Board at the last meeting, which was the beginning of this month, but there was a status update on that, and there was a discussion. It is a joint group that is working with the DHS Advisory Committee as well, and my understanding is that it is in its final phases now, and they are expecting to publish something sometime this year if they can work out some of the details together.

I think that many of the changes discussed are similar to the things in the GAO report from what I was told. I have not seen the latest draft, though, so I cannot fully comment on if there is anything broader than that. Because I just came to the Board, I am not on that Subcommittee at this point. So I will try to get a report back to you from the chairman of the committee sometime in the next couple of days.

Senator AKAKA. Thank you very much, Mr. Chairman.

Chairman LIEBERMAN. Thanks, Senator Akaka. Senator Carper, I do want to put you on notice that in introducing Professor Swire and mentioning his university affiliation——

Senator CARPER. What affiliation is that? [Laughter.]

Senator COLLINS. You are just proving what the Chairman said would happen. [Laughter.]

Chairman LIEBERMAN. It is all yours.

Senator CARPER. Ohio State University.

Chairman LIEBERMAN. That is it.

**OPENING STATEMENT OF SENATOR CARPER**

Senator CARPER. I apologize to our panelists, but I was just over on the Senate floor with another graduate of Ohio State, a law school graduate, Senator Voinovich. And I shepherded with the support of, among others, Senator Lieberman and Senator Collins legislation to help reduce the emission of particulates from diesel engines. There are about 11 million of them on the roads. Bad stuff. They create a lot of bad health for us. And we appreciate the support of our colleagues in getting the legislation done, and on to the President to sign into law.

Professor Swire, he told me that you were here, and he said, "In the French Quarter of Columbus, we pronounce his name 'Swi-

ray.'" And so I said, "Well, you call him what you want. We will call him Swire at the hearing." [Laughter.]

But we are glad that you are here, and thank you all for coming.

I have a statement I would like to share and then maybe a question or two, if I could. When I come in late at a hearing like this and I have missed your testimony, what I am going to ask you to do is just share with me and with my colleagues the common ground that you see here, sort of the takeaways, evolving from the discussion and from the questioning that occurred. So just be thinking about that, if you will.

Mr. Chairman, thanks very much for holding this hearing. And I want to say to Senator Akaka, thank you very much for your leadership in bringing us here as well. And sometimes it seems that almost every week another agency is compromised by suspected hackers or a laptop is lost or stolen by current or former employees. And all too often, these events put at risk millions of Americans' sensitive information, names, birth dates, Social Security numbers, and health information included.

In fact, my staff tells me that there are criminal elements in this world that have massive inventories of bank numbers, Social Security numbers, and other personally identifiable information that are sold to the highest bidder. Some of these criminals have been caught—not enough—but largely these criminal groups remain immune to our laws here in the United States. And a lot of them operate outside of the United States, as you know.

That is why agencies need to ensure that sensitive information is protected during its collection, during its transmission, and throughout its storage. Placed in the wrong hands, this information can leave an individual vulnerable to identity theft, which we suffered in our own family, or to worse.

That is one of the reasons I chaired a hearing of the Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security on March 12, 2008. And we looked into the Federal Information Security Management Act. What I found there surprised me. Many times agencies do not even know what information they hold. They do not know where the information is stored. They do not know who has the access and whether that information has been compromised.

Our Federal Government stores some of our Nation's most sensitive economic, corporate, and military secrets. It is imperative that agencies find a better way to protect not just an individual's identity but as much of that sensitive information as we possibly can.

However, I feel the American public is slowly but surely losing faith in our government's ability to protect its sensitive information. That is why I have asked my staff to work hard with some of our colleagues on this Committee on reforming this critical information security law. And I look forward to working with our Chairman and with my other colleagues on this Committee on this legislation to protect our Nation's most sensitive information.

With that having been said, and earlier having telegraphed my pitch, we will just ask maybe Professor Swire to lead off. Please summarize what you see as common ground and lessons for us to take away from this hearing. Thank you. Again, welcome.

Mr. SWIRE. Oh, thank you very kindly. Go Buckeyes.

I think in terms of common ground, one thing I heard is that the definition of "Systems of Records," the definition in the Privacy Act of what is covered, leaves out a lot of data mining. That is a technological change from the 1970s. And how to create a legal structure around that, I do not think we have any answer to necessarily. There is going to be a workshop coming up on that. But the idea that we do not retrieve records one at a time now the way we did 35 years ago and we need to come up with a new set of ways to deal with that, I think that is a strong theme I heard today from pretty much everyone.

Senator CARPER. Thank you, sir. Mr. Schwartz.

Mr. SCHWARTZ. Well, I will pick one item out from, I think, a number of things that the four of us probably agreed on. But I think that there was a discussion about changes to encourage leadership in privacy across agencies, and there are a number of ways to do that, particularly through making sure that we have high-level appointees within the agencies and probably within OMB as well. But I think that certainly there was agreement that it has to be a high-level staff on privacy that can take accountability.

Senator CARPER. Thanks very much.

Mr. TEUFEL. So my answer to you, sir, would be transparency. It is key to the privacy framework in the public sector in the United States, and Chairman Lieberman had mentioned the European approach. And there are many things the Europeans do well, but transparency is not something, I think, the Europeans do as well as we can and often do in the United States. The goal is for the public to have trust and confidence in what its government is doing.

The other thing that one gets through transparency is that it allows the public to make informed decisions that they then can let you, the elected representatives of the country, know about those views. And so I would stop with that.

Senator Collins, I did want to mention, thanks to the magic of the BlackBerry, Peter Pietra, the component Privacy Officer, tells me that Clear is one of the many providers under the Registered Traveler Program, and there is a PIA out on the Registered Traveler Program, and the data is encrypted.

Senator COLLINS. Thank you.

Senator CARPER. We could not have done that 34 years ago, could we? [Laughter.]

Pretty amazing. Thank you. Actually, information like that sort of makes my colleagues and I joyful, which rhymes with your name "Teuful." [Laughter.]

Mr. TEUFEL. Thank you, Senator. I have never heard that before. Thank you.

Chairman LIEBERMAN. That was the proper response to a Senator. Very well done. [Laughter.]

Senator CARPER. Ms. Koontz.

Ms. KOONTZ. I think we agree that the System of Records concept in the Privacy Act is outmoded. It is not consistent with current uses of information or the technology that we are employing. We would like to see the protections of the Privacy Act expanded

to all personally identifiable information, regardless of how it is held.

I think another point is that we would like to see personally identifiable information, its use and collection, limited to a specified purpose.

And, finally, I agree with the point on transparency. We need to promote transparency, and we need to improve the public notices in a number of ways that serve as a vehicle for us to inform the public about what the Federal Government is doing with personally identifiable information.

Senator CARPER. I thank you all. We thank you for being here. We thank you for your testimony. And thank you for allowing me to look for some common ground and some takeaways that should serve us well in the future.

Mr. Chairman, much obliged.

Chairman LIEBERMAN. Thank you very much, Senator Carper. Actually, your question was a great one to conclude the hearing on, and it illuminates what struck me. Senator Collins and I were talking about it. As I listened to the testimony, you have all been very helpful, and what is also true and significant, and not always the case when we bring together a group of people from different perspectives on a common issue, is that there is quite a consensus among you about what needs to be done.

So you have helped us enormously this morning, and I think now we want to consider what we can do and perhaps in a short time frame—which, unfortunately, is the case with this session of Congress—whether there is some common ground proposal that we can come forward with that will not stir up the kind of controversy that will block it from being passed or whether we want to wait until the next session and do something more comprehensive.

But there is no question, in my mind, anyway, as I listen to the testimony or read the GAO reports, that the Privacy Act of 1974 is just not up to the realities of 2008 in the age of information.

Senator Collins, did you want to add anything in conclusion?

Senator COLLINS. Thank you. I just want to thank our witnesses. This was an excellent panel, and I very much appreciate your leadership, Mr. Chairman. Thank you.

Chairman LIEBERMAN. Thanks, Senator Collins.

We will keep the record of the hearing open for 15 days in case any of you want to add to your testimony, any answers you may not have received already over your BlackBerrys and shared with the Committee, or in case Members of the Committee who have not been here, or even those who have, have additional questions for you.

But, with that, I thank you very much. The hearing is adjourned.

[Whereupon, at 11:57 a.m., the Committee was adjourned.]

# APPENDIX

United States Government Accountability Office

GAO

Testimony
Before the Committee on Homeland Security and Governmental Affairs, U.S. Senate

For Release on Delivery
Expected at 10 a.m. EDT
Wednesday, June 18, 2008

## PRIVACY

## Congress Should Consider Alternatives for Strengthening Protection of Personally Identifiable Information

Statement of Linda Koontz
Director, Information Management Issues

GAO-08-795T

June 18, 2008

Highlights of GAO-08-795T, a testimony before the Committee on Homeland Security and Governmental Affairs, U.S. Senate

# PRIVACY

## Congress Should Consider Alternatives for Strengthening Protection of Personally Identifiable Information

### Why GAO Did This Study

Concerns have been raised about the privacy and security of personal information in light of advances in information technology and the increasingly sophisticated ways in which the government obtains and uses information. Federal agencies' use of personal information is governed by the Privacy Act of 1974 and the E-Government Act of 2002, while the Office of Management and Budget (OMB) provides implementation guidance and oversight. These laws and guidance are based on the Fair Information Practices , a set of widely accepted principles for protecting privacy.

GAO was asked to testify on its report, being released today, concerning the sufficiency of privacy protections afforded by existing laws and guidance. To do this, GAO analyzed privacy laws and guidance, compared them with the Fair Information Practices, and obtained perspectives from federal agencies as well as an expert forum.

### What GAO Recommends

In its report GAO identified alternatives that the Congress should consider, including revising the scope of privacy laws to cover all personal information, requiring that the use of such information be limited to a specific purpose, and revising the structure and publication of privacy notices.

OMB commented that the Congress should consider these alternatives in the broader context of existing privacy and related statutes.

To view the full product, including the scope and methodology, click on GAO-08-795T. For more information, contact Linda Koontz at (202) 512-6240 or koontzl@gao.gov.

### What GAO Found

Although privacy laws and guidance set minimum requirements for agencies, they may not consistently protect personally identifiable information in all circumstances of its collection and use throughout the federal government and may not fully adhere to key privacy principles. Based on discussions with privacy experts and agency officials, as well as analysis of laws and related guidance, GAO identified issues in three major areas:

***Applying privacy protections consistently to all federal collection and use of personal information.*** The Privacy Act's definition of a "system of records," which sets the scope of the act's protections, does not always apply whenever personal information is obtained and processed by federal agencies. For example, if agencies do not retrieve personal information by identifier, the act's protections do not apply. This has led experts to agree that the Privacy Act's system-of-records construct is too narrowly defined. An alternative for addressing these issues could include revising the system-of-records definition to cover all personally identifiable information collected, used, and maintained systematically by the federal government.

***Ensuring that use of personally identifiable information is limited to a stated purpose.*** According to the Fair Information Practices, the use of personal information should be limited to a specified purpose. Yet current laws and guidance impose only modest requirements for describing the purposes for personal information and limiting how it is used. For example, agencies are not required to be specific in formulating purpose descriptions in their public notices. Overly broad specifications of purpose could allow for unnecessarily broad ranges of uses, thus calling into question whether meaningful limitations had been imposed. Alternatives for addressing these issues include setting specific limits on use of information within agencies and requiring agencies to establish formal agreements with external governmental entities before sharing personally identifiable information with them.

***Establishing effective mechanisms for informing the public about privacy protections.*** Public notices are a primary means of establishing accountability for privacy protections and giving individuals a measure of control over the use of their personal information. Although the *Federal Register* is the government's official vehicle for issuing public notices, critics have questioned whether system-of-records notices published in the *Federal Register* effectively inform the public about government uses of personal information. Options for addressing concerns about public notices include requiring that purpose, collection limitations, and use limitations are better addressed in the content of privacy notices, and revising the Privacy Act to require that all notices be published on a standard Web site, with an address such as www.privacy.gov.

June 18, 2008

Mr. Chairman and Members of the Committee:

I appreciate the opportunity to discuss today the critical protections afforded to individual privacy by laws and guidance governing the federal government's use of personally identifiable information.[1] The increasingly sophisticated ways in which personal information is obtained and used by the federal government has the potential to assist in performing critical functions, such as preventing terrorism, but also can pose challenges in ensuring the protection of citizens' privacy. In this regard, concerns have been raised that the framework of legal mechanisms for protecting personal privacy that has been developed over the years may no longer be sufficient, given current practices.

Federal agency use of personal information is governed primarily by the Privacy Act of 1974 and the E-Government Act of 2002.[2] The Privacy Act of 1974 serves as the major mechanism for controlling the collection, use, and disclosure of personally identifiable information within the federal government. The E-Government Act of 2002 strives to enhance the protection of personal information in government information systems by requiring that agencies conduct privacy impact assessments.[3] The Office of Management and Budget (OMB) is charged with ensuring implementation of the privacy

[1]For purposes of this testimony, the terms *personal information* and *personally identifiable information* are used interchangeably to refer to any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

[2]In addition, the Paperwork Reduction Act, enacted in 1980 and significantly revised in 1995, also has provisions affecting privacy protection in that it sets requirements for limiting the collection of information from individuals, including personal information. While the act's requirements are aimed at reducing the paperwork burden on individuals rather than specifically protecting personally identifiable information, the act nevertheless serves an important role in protecting privacy by setting these controls.

[3]A privacy impact assessment is an analysis of how personal information is collected, stored, shared, and managed in an information system.

impact assessment requirement and the Privacy Act by federal agencies and is also responsible for providing guidance to agencies.

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, with some variation, are used by organizations to address privacy considerations in their business practices and are also the basis of privacy laws and related policies in many countries, including the United States, Germany, Sweden, Australia, and New Zealand, as well as the European Union.

My testimony today will highlight key findings from a report that we are releasing today.[5] In the report, we assess the sufficiency of laws and guidance covering the federal government's collection and use of personal information. We also identify alternatives for addressing issues raised by our review. In conducting our work, we analyzed the Privacy Act of 1974, section 208 of the E-Government Act, and related guidance to identify any inconsistencies or gaps in the coverage of these laws as they apply to uses of personal information by federal agencies. We also compared these laws and related guidance with the Fair Information Practices to identify any significant gaps, including assessing the role of the Paperwork Reduction Act (PRA) in protecting privacy by limiting collection of information. We obtained an operational perspective on the sufficiency of these laws from six federal departments and agencies with large inventories of information collections, prominent privacy issues, and varied missions. We also obtained expert perspective through the use of an expert panel convened for us by the National Academy of Sciences. We conducted our work for this performance audit in accordance with generally accepted government auditing

[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).

[5]GAO, *Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information*, GAO-08-536 (Washington, D.C.: May 19, 2008).

standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Today, after a brief summary of the laws and guidance currently in place, my remarks will focus on key results of our review of their sufficiency in governing the government's collection and use of personal information.

## Results in Brief

Although the Privacy Act, the E-Government Act, and related OMB guidance set minimum requirements for agencies, they may not consistently protect personally identifiable information in all circumstances of its collection and use throughout the federal government and may not fully adhere to key privacy principles. Based on discussions with privacy experts and agency officials, as well as analysis of laws and related guidance, we identified issues in three major areas:

***Applying privacy protections consistently to all federal collection and use of personal information.*** The Privacy Act's definition of a "system of records" (any grouping of records containing personal information retrieved by individual identifier), which sets the scope of the act's protections, does not always apply whenever personal information is obtained and processed by federal agencies. For example, if agencies do not retrieve personal information by identifier, the act's protections do not apply. Our 2003 report concerning compliance with the Privacy Act found that among the agencies surveyed, the most frequently cited reason for systems not being considered Privacy Act systems of records was that the agency did not use a personal identifier to retrieve the information.[6] Factors such as these have led experts to agree that

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

the Privacy Act's system-of-records construct is too narrowly defined. An alternative for addressing these issues could include revising the system-of-records definition to cover all personally identifiable information collected, used, and maintained systematically by the federal government.

***Ensuring that use of personally identifiable information is limited to a stated purpose.*** According to the purpose specification and use limitation principles, the use of personal information should be limited to a specified purpose. Yet current laws and guidance impose only modest requirements for describing the purposes for personal information and limiting how it is used. For example, agencies are not required to be specific in formulating purpose descriptions in their public notices. While purpose statements for certain law enforcement and antiterrorism systems might need to be phrased broadly enough so as not to reveal investigative techniques or the details of ongoing cases, very broadly defined purposes could allow for unnecessarily broad ranges of uses, thus calling into question whether meaningful limitations had been imposed. Examples of alternatives for addressing these issues include setting specific limits on the use of information within agencies and requiring agencies to establish formal agreements with external governmental entities before sharing personally identifiable information with them.

***Establishing effective mechanisms for informing the public about privacy protections.*** According to the openness principle, the public should be informed about privacy policies and practices, and the accountability principle calls for those who control the collection or use of personal information to be held accountable for taking steps to ensure privacy protection. Public notices are a primary means of establishing accountability for privacy protections and giving individuals a measure of control over the use of their personal information. Yet concerns have been raised that Privacy Act notices may not serve this function well. Although the *Federal Register* is the government's official vehicle for issuing public notices, critics have questioned whether system-of-records notices published in the *Federal Register* effectively inform the public about government uses of personal information. Among others, options for addressing concerns about public notices could include setting

requirements to ensure that purpose, collection limitations, and use limitations are better addressed in the content of privacy notices, and revising the Privacy Act to require that all notices be published on a standard Web site, with an address such as www.privacy.gov.

Some of these issues—particularly those dealing with limitations on use and mechanisms for informing the public—could be addressed by OMB through revisions or supplements to guidance. However, unilateral actions by OMB would not have the benefit of public deliberations regarding how best to achieve an appropriate balance between the government's need to collect, process, and share personally identifiable information and the rights of individuals to know about such collections and be assured that they are only for limited purposes and uses. In assessing such a balance, we suggested that Congress consider amending applicable laws, such as the Privacy Act and the E-Government Act, according to the alternatives outlined in the report, including

- revising the scope of the laws to cover all personally identifiable information collected, used, and maintained by the federal government;
- setting requirements to ensure that the collection and use of personally identifiable information is limited to a stated purpose; and
- establishing additional mechanisms for informing the public about privacy protections by revising requirements for the structure and publication of public notices.

In commenting on a draft of our report OMB officials noted that they shared our concerns about privacy and listed guidance that the agency has issued in the areas of privacy and information security. The officials stated that they believe it would be important for Congress to consider potential amendments to the Privacy Act and the E-Government Act in the broader context of the several privacy statutes that Congress has enacted.

Though we did not make specific recommendations to OMB, the agency provided comments on the alternatives identified in conjunction with our matter for congressional consideration. Regarding alternatives for revising the scope of laws to cover all personally identifiable information collected, used, and maintained

by the federal government, OMB stated that it would be important for Congress to evaluate fully the potential implications of revisions such as amending the Privacy Act's system-of-records definition. We believe that, given that the Privacy Act's controls on the collection, use, and disclosure of personally identifiable information do not consistently protect such information in all circumstances of its collection and use throughout the federal government, amending the act's definition of a system of records is an important alternative for Congress to consider. However, we agree with OMB that such consideration should be thorough and include further public debate on all relevant issues.

## Background

In response to growing concern about the harmful consequences that computerized data systems could have on the privacy of personal information, in 1972 the Secretary of Health, Education, and Welfare commissioned an advisory committee to examine to what extent limitations should be placed on the application of computer technology to record keeping about people. The committee's final report proposed a set of principles for protecting the privacy and security of personal information, known as the Fair Information Practices.[7] These practices were intended to address what the committee termed a poor level of protection afforded to privacy under then-existing law, and they underlie the major provisions of the Privacy Act, which was enacted the following year. A revised version of the Fair Information Practices was developed in 1980 by the Organization for Economic Cooperation and Development (OECD) and has been widely adopted.[8] This version of

[7]Department of Health, Education & Welfare, *Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (Washington, D.C.: 1973).

[8]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.

the principles was reaffirmed by OECD ministers in a 1998 declaration and further endorsed in a 2006 OECD report.[9] The OECD version of the principles is shown in table 1.

**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. |
| 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.

The Fair Information Practices are, with some variation, the basis of privacy laws and related policies in many countries, including the United States, Germany, Sweden, Australia, and New Zealand, as well as the European Union.[10] They are also reflected in a variety of

[9]OECD, *Making Privacy Notices Simple: An OECD Report and Recommendations* (July 24, 2006).

[10]European Union Data Protection Directive ("Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data") (1995).

federal agency policy statements, beginning with an endorsement of the OECD principles by the Department of Commerce in 1981.[11]

The Fair Information Practices are not legal requirements but 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. Striking that balance varies among countries and among types of information.

## Federal Laws and Guidance Govern Use of Personal Information in Federal Agencies

There is no single federal law that governs all use or disclosure of personal information. Instead, U.S. law includes a number of separate statutes that provide privacy protections for information used for specific purposes or maintained by specific entities. The major requirements for the protection of personal information by federal agencies come from two laws: the Privacy Act of 1974 and the privacy provisions of the E-Government Act of 2002.

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 a "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 through a system-of-records notice in the *Federal Register* that identifies, among other things, the categories of data collected, the categories of individuals about whom information is collected, the intended "routine" uses of data,

[11]"Report on OECD Guidelines Program," Memorandum from Bernard Wunder, Jr., Assistant Secretary for Communications and Information, Department of Commerce (Oct. 30, 1981).

and procedures that individuals can use to review and correct personally identifiable information.[12]

Several provisions of the act require agencies to define and limit collection and use to 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 that individual's rights or benefits under a federal program. The act also requires that an agency inform individuals whom it asks to supply information of (1) the authority for soliciting the information and whether disclosure of such information is mandatory or voluntary; (2) the principal purposes for which the information is intended to be used; (3) the routine uses that may be made of the information; and (4) the effects on the individual, if any, of not providing the information. According to OMB, this requirement is based on the assumption that individuals should be provided with sufficient information about the request to make a decision about whether to respond.

In handling collected information, agencies are generally required by the Privacy Act to, among other things, allow individuals to (1) review their records (meaning any information pertaining to them that is contained in the system of records), (2) request a copy of their record or information from the system of records, and (3) request corrections to their information.

Agencies are allowed to claim exemptions from some of the provisions of the Privacy Act if the records are used for certain purposes. For example, records compiled by law enforcement agencies for criminal law enforcement purposes can be exempt from a number of provisions, including (1) the requirement to notify individuals of the purposes and uses of the information at the time of collection and (2) the requirement to ensure the accuracy, relevance, timeliness, and completeness of records. A broader category of investigative records compiled for criminal or civil law

[12]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).

enforcement purposes can also be exempted from a somewhat smaller number of Privacy Act provisions, including the requirement to provide individuals with access to their records and to inform the public of the categories of sources of records. In general, the exemptions for law enforcement purposes are intended to prevent the disclosure of information collected as part of an ongoing investigation that could impair the investigation or allow those under investigation to change their behavior or take other actions to escape prosecution.

In 2002, Congress enacted the E-Government Act to, among other things, enhance protection for personal information in government information systems or information collections by requiring that agencies conduct privacy impact assessments, which are analyses of how personal information is collected, stored, shared, and managed in a federal system.

In addition, the Paperwork Reduction Act applies to federal information collections and was designed to help ensure that when the government asks the public for information, the burden of providing this information is as small as possible and the information itself is used effectively.[15] Among the act's provisions is the requirement that agencies not establish information collections without having them approved by OMB, and that before submitting them for approval, agencies' chief information officers certify that the collections meet 10 specified standards. The law also requires agencies both to publish notices in the *Federal Register* and to otherwise consult with the public about their planned collections.

Privacy is also addressed in the legal framework for the emerging information sharing environment. As directed by the Intelligence Reform and Terrorism Prevention Act of 2004, the administration has taken steps, beginning in 2005, to establish an information sharing environment to facilitate the sharing of terrorism-related

[15]The Paperwork Reduction Act was originally enacted into law in 1980 (Pub. L. No. 96-511, Dec. 11, 1980). It was reauthorized with minor amendments in 1986 (Pub. L. No. 99-591, Oct. 30, 1986) and was reauthorized a second time with more significant amendments in 1995 (Pub. L. No. 104-13, May 22, 1995).

information.[14] The move was driven by the recognition that before the attacks of September 11, 2001, federal agencies had been unable to effectively share information about suspected terrorists and their activities. In addressing this problem, the National Commission on Terrorist Attacks Upon the United States (9/11 Commission) recommended that the sharing and uses of information be guided by a set of practical policy guidelines that would simultaneously empower and constrain officials, closely circumscribing what types of information they would be permitted to share as well as the types of information they would need to protect. Exchanging terrorism-related information continues to be a significant challenge for federal, state, and local governments—one that we recognize is not easily addressed. Accordingly, since January 2005, we have designated information sharing for homeland security a high-risk area.[15]

Other federal laws address privacy protection for personal information with respect to information security requirements, as well as for certain types of information, such as when taxpayer, statistical, or health information is involved. This includes the Federal Information Security Management Act (FISMA), which addresses the protection of personal information by defining federal requirements for securing information and information systems that support federal agency operations and assets; the Health Insurance Portability and Accountability Act of 1996, which addresses the use and disclosure of individual health information; the Confidential Information Protection and Statistical Efficiency Act, which limits the use of information gathered for statistical purposes; and laws governing the disclosure of taxpayer data collected by the Internal Revenue Service.

[14]Pub. L. No. 108-458 (Dec. 17, 2004).

[15]For more information, see GAO, *High-Risk Series: An Update*, GAO-07-310 (Washington, D.C.: January 2007), p. 47, and *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information*, GAO-06-385 (Washington, D.C.: Mar. 17, 2006).

## OMB Has Primary Responsibility for Oversight of the Privacy, E-Government, and Paperwork Reduction Acts

The Privacy Act gives OMB responsibility for developing guidelines and providing "continuing assistance to and oversight of" agencies' implementation of the Privacy Act. The E-Government Act of 2002 also assigns OMB responsibility for developing privacy impact assessment guidance and ensuring agency implementation of the privacy impact assessment requirement. In July 1975, OMB published guidance for implementing the provisions of the Privacy Act. Since then, OMB has periodically issued additional guidance, including guidance to assist agencies in complying with the Computer Matching and Privacy Protection Act[16] and guidance to agencies on conducting privacy impact assessments.

In 1980, the enactment of the Paperwork Reduction Act made virtually all federal agency information collection activities subject to OMB review and established broad objectives for OMB oversight of the management of federal information resources. The act established the Office of Information and Regulatory Affairs within OMB and gave this office a variety of oversight responsibilities over federal information functions, including general information policy, reduction of paperwork burden, and information privacy. To assist agencies in fulfilling their responsibilities under the act, OMB took various steps. It issued a regulation[17] and provided agencies with instructions on filling out a standard form for submissions and providing supporting statements.

OMB has also periodically issued guidance on other privacy-related issues, including

- federal agency Web site privacy policies;
- interagency sharing of personal information;

[16]In 1988, Congress passed the Computer Matching and Privacy Protection Act as an amendment to the Privacy Act, to establish procedural safeguards that affect agencies' use of Privacy Act records from benefit programs in performing certain types of computerized matching programs. For example, the 1988 act requires agencies to create written agreements specifying the terms under which matches are to be done.

[17]5 C.F.R. Part 1320.

- designation of senior staff responsible for privacy; and
- data breach notification.

### Prior GAO Reports Have Identified Privacy Challenges at Federal Agencies

We have previously reported on a number of agency-specific and governmentwide privacy-related issues at federal agencies. For example, in 2003, we reported that agencies generally did well with certain aspects of the Privacy Act's requirements—such as issuing systems-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.[18] 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. We have also reported on key privacy challenges facing federal agencies, federal Web site privacy, notification of individuals in the event of a data breach, and government data-mining initiatives.

## Key Terms in the Privacy Act May Be Defined Too Narrowly

Because the Privacy Act's controls on the collection, use, and disclosure of personally identifiable information only apply when such information is covered by the act's key terms, especially the "system-of-records" construct, they do not consistently protect such information in all circumstances of its collection and use throughout the federal government. There are several different ways in which federal collection and use of personally identifiable information could be outside of such a construct and thus not receive the Privacy Act's protections, as shown by the following examples:

- *Personally identifiable information held by the government is not always retrieved by identifier.* The Privacy Act defines a system of

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

records as "a group of records"[19] that is "under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." If personally identifiable information (records) is not retrieved by identifier but instead accessed through some other method or criteria—for example, by searching for all individuals who have a certain medical condition or who applied for benefits on a certain date—the system would not meet the Privacy Act's system-of-records definition and therefore would not be governed by the act's protections. OMB's 1975 Privacy Act implementation guidance reflects an acknowledgement that agencies could potentially evade the act's requirements by organizing personal information in ways that may not be considered to be retrieved by identifier.

In our 2003 report concerning compliance with the Privacy Act, we found that the increasing use of electronic records by federal agencies resulted in personal information falling outside the scope of Privacy Act protections. A key characteristic of agencies' systems of records at the time was that a large proportion of them were electronic, reflecting the government's significant use of computers and the Internet to collect and share personal information. Based on survey responses from 25 agencies in 2002, we estimated that 70 percent of the agencies' systems of records contained electronic records and that 11 percent of information systems in use at those agencies contained personal information that was outside a Privacy Act system of records. We also reported that among the agencies we surveyed, the most frequently cited reason for systems not being considered Privacy Act systems of records was that the agency did not use a personal identifier to retrieve the personal information.[20]

- *The Privacy Act's protections may not apply to contemporary data processing technologies and applications.* In today's highly

[19]A *record* is defined as "any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph."

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

interconnected environment, information can be gathered from many different sources, analyzed, and redistributed in very dynamic, unstructured ways that may have little to do with the file-oriented concept of a Privacy Act system of records. For example, data mining, a prevalent technique used by federal agencies for extracting useful information from large volumes of data, may escape the purview of the Privacy Act's protections.[21] Specifically, a data-mining system that performs analysis by looking for patterns in personal information located in other systems of records or that performs subject-based queries across multiple data sources may not constitute a system of records under the act.

In recent years, reports required by law on data mining have described activities that had not been identified as systems of records covered by the Privacy Act. In one example, DHS reported that all the data sources for the planned Analysis Dissemination Visualization Insight and Semantic Enhancement (ADVISE) data mining program were covered by existing system-of-records notices; however, the system itself was not covered, and no system of records notice was created specifically to document protections under the Privacy Act governing the specific activities of the system.[22] ADVISE was a data-mining tool intended to allow an analyst to search for patterns in data—such as relationships among people, organizations, and events—and to produce visual representations of those patterns.

As a result, personally identifiable information collected and processed by such systems may be less well protected than if it were more specifically addressed by the Privacy Act.

The issues associated with the coverage of the Privacy Act's protections could be addressed by revising the system-of-records definition to cover all personally identifiable information collected,

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

[22]The DHS Privacy Office determined that because the data mining applications did not involve retrieval by individual identifier, a separate system of records notice describing the data mining application was not required. DHS Privacy Office, *ADVISE Report: DHS Privacy Office Review of the Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement (ADVISE) Program* (Washington, D.C., July 11, 2007).

used, and maintained by the federal government. Experts at our forum were in agreement that the system-of-records definition is outdated and flawed and that the act's protections should be applied whenever agencies obtain, process, store, or share personally identifiable information—not just when records are retrieved by personal identifier. Changing the system-of-records definition is an option that could help ensure that the act's protections are consistently applied to all personally identifiable information.

## The Privacy Act Does Not Ensure that the Use of Personal Information Is Limited to Clearly Stated Purposes

The fair information practices' *purpose specification* principle states that the purpose for the collection of personal information should be disclosed before the collection is made and upon any change to that purpose, while the *use limitation* principle provides that personal information, once collected, should not be disclosed or used for other than its specified purpose without consent of the individual or legal authority. When the government is required to define a specific purpose for the collection of personal information and limit its use to that purpose, individuals gain assurance that their privacy will be protected and their information will not be used in ways that could jeopardize their rights or otherwise unfairly affect them.

The Privacy Act requires agencies to (1) inform individuals from whom information is being collected of the principal purpose or purposes for which the information is intended to be used and (2) publish a system-of-records notice in the *Federal Register* of the existence and character of the system of records, including planned routine uses of the records and the purpose of each of these routine uses. Concerns have been raised, however, that these requirements do not go far enough in ensuring that the government's planned purposes are sufficiently specified and that the use of information is limited to these purposes:

- *Purpose descriptions in public notices are not required to be specific.* While there is no requirement for an overall statement of purpose, Privacy Act notices may contain multiple descriptions of

purposes associated with routine uses, and agencies are not required to be specific in formulating these purposes. OMB guidance on the act gives agencies discretion to determine how to define the range of appropriate uses and associated purposes that it intends for a given system of records. While purpose statements for certain law enforcement and anti-terrorism systems might need to be phrased broadly enough so as not to reveal investigative techniques or the details of ongoing cases, very broadly defined purposes could allow for unnecessarily broad ranges of uses, thus calling into question whether meaningful limitations had been imposed.

- *Unconstrained application of predefined "routine" uses may weaken use limitations.* A number of concerns have been raised about the impact on privacy of potentially unnecessary routine uses for agency systems of records, particularly through the application of "standard" routine uses that are developed for general use on multiple systems of records. This practice is not prohibited by the Privacy Act. All six agencies we reviewed had lists of standard routine uses for application to their systems of records. However, the language of these standard routine uses varies from agency to agency. For example, several agencies have a routine use allowing them to share information about individuals with other governmental entities for purposes of decision-making about hiring or retention of an individual, issuance of a security clearance, license, contract, grant, or other benefit. Experts expressed concern that "standard" routine uses such as these vary to such a great extent from agency to agency, with no specific legal requirement that they be formulated consistently.
- *The Privacy Act sets only modest limits on the use of personal information for multiple purposes within an agency.* The Privacy Act permits disclosures from agency systems of records "to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties." However, without additional limits, internal uses could go beyond uses related to the purpose of the original collection. In our interviews with senior agency privacy officials, we asked what, if any, limits were placed on internal agency uses of information. Several agencies responded that, consistent with the Privacy Act and OMB guidance, internal agency usage of personal information was limited to those personnel with a "need to know." However, because the Privacy Act and related guidance do not require it, none

of these agencies took steps to determine whether internal uses were consistent with the purposes originally stated for the collection of information. The potential that personal information could be used for multiple, unspecified purposes is especially heightened in large agencies with multiple components that may collect personal information in many different ways for disparate purposes.

- *The Privacy Act's provisions may not apply when data are shared for use by another agency.* In addition to concerns about limiting use to a specified purpose within an agency, more extensive issues have been raised when data are shared outside an agency. Although the Privacy Act provides assurance that the information in systems of records cannot be disclosed unless it is pursuant to either a routine use or another statutorily allowed condition, the act does not attach its protections to data after they have been disclosed. As data sharing among agencies becomes central to the sharing of terrorism-related information, measures to ensure that data are being used appropriately will become more important. Despite not being required to do so, agencies we reviewed reported taking measures to ensure the data are used appropriately by recipients. However, in the absence of such measures, data shared outside federal agencies would not always have sufficient protections.

To better confine agencies' use of personal information to its specified purposes, laws or guidance could be revised to (1) require agencies to justify the use of key elements of personal information, (2) set specific limits on routine uses and internal agency uses of personal information, and (3) require agencies to establish formal agreements with external entities before sharing personal information with them.

## The Privacy Act May Not Include Effective Mechanisms for Informing the Public

A primary method for providing transparency about government programs and systems that collect and use personal information is through public written notices. A clear and effective notice can provide individuals with critical information about what personal data are to be collected, how they are to be used, and the circumstances under which they may be shared. An effective notice

can also provide individuals with information they need to determine whether to provide their personal information (if voluntary), or who to contact to correct any errors that could result in an adverse determination about them.

In formal terms, the *openness* principle states that the public should be informed about privacy policies and practices and that individuals should have a ready means of learning about the use of personal information. The openness principle underlies the public notice provisions of the Privacy Act. Specifically, the Privacy Act requires agencies to publish in the *Federal Register*, "upon establishment or revision, a notice of the existence and character of a system of records." This notice is to include, among other things, the categories of records in the system as well as the categories of sources of records. The notice is also required to explain agency procedures whereby an individual can gain access to any record pertaining to him or her contained in the system of records and contest its content. Agencies are further required to publish notice of any new use or intended use of the information in the system and provide an opportunity for interested persons to submit written data, views, or arguments to the agency.[23]

However, experts at our forum as well as agency privacy officials questioned the value of system-of-records notices as vehicles for providing information to the general public for several reasons:

- *System-of-records notices may be difficult to understand.* As with other legally required privacy notices, system-of-records notices have been criticized as hard to read and understand. To the lay reader, the meaning of "routine" uses may be unclear, or a list of exemptions could raise more questions than it answers. Agency privacy officials and privacy experts at our forum both agreed that system-of-records notices have limited value as vehicles for public notification.
- *System-of-records notices do not always contain complete and useful information about privacy protections.* They often describe

[23]The Privacy Act allows agencies to claim exemptions if the records are used for certain purposes, such as criminal law enforcement. See the earlier discussion on pp. 9-10.

purposes and use in such broad terms that it becomes questionable whether those purposes and uses have been significantly limited. Likewise, broad purpose statements may not usefully inform the public of the government's intended purposes, and the citation of multiple routine uses does little to aid individuals' understanding of how the government is using their personal information. The Privacy Act does not require agencies to be specific in describing the purposes associated with routine uses of personal information or to publish all expected internal agency uses of that information.

- *Publication in the Federal Register may reach only a limited audience.* Agency privacy officials questioned whether the required publication of system-of-records notices in the *Federal Register* would be useful to a broader audience than federal agency officials and public interest groups, such as privacy advocacy groups. Notices published in the *Federal Register* may not be very accessible and readable. The *Federal Register* Web site does not provide a ready means of determining what system-of-records notices are current, when they were last updated, or which ones apply to any specific governmental function. Officials agreed that it can be difficult to locate a system-of-records notice on the *Federal Register* Web site, even when the name of the relevant system of records is known in advance. Privacy experts at our forum likewise agreed that the *Federal Register* is probably not effective with the general public and that a more effective technique for reaching a wide audience in today's environment is via consolidated publication on a governmentwide Web site devoted to privacy. Both agency officials and privacy experts also agreed, however, that the *Federal Register* serves a separate but important role as the official public record of federal agencies and as the official basis for soliciting comments from the public on proposed systems of records.

Based on discussions with privacy experts, agency officials, and analysis of laws and related guidance, a number of options exist for improving public notice regarding federal collection and use of personal information:

- *Require layered public notices in conjunction with system-of-records notices.* Layering involves providing only the most important summary facts up front—often in a graphically oriented format—followed by one or more lengthier, more narrative versions.

By offering both types of notices, the benefits of each can be realized: long notices offer completeness, while brief notices offer ease of understanding.

- *Set requirements to ensure that purpose, collection limitations, and use limitations are better addressed in the content of privacy notices.* These could include requirements for a specific description of the planned purpose of a system, what data needs to be collected to serve that purpose, and how its use will be limited to that purpose, including descriptions of primary and secondary uses of information. Setting these requirements could spur agencies to prepare notices that include more meaningful descriptions of the intents and purposes of their systems of records.
- *Make all notices available on a governmentwide privacy Web site.* Relevant privacy notices could be published at a central governmentwide location, with an address such as www.privacy.gov, and at corresponding standard locations on agency Web sites with addresses of the form www.agency.gov/privacy. These sites have the potential to reach a far broader spectrum of users than the *Federal Register*.

## Amending Privacy Laws Could Address Gaps and Shortcomings in Privacy Protections

In summary, current laws and guidance governing the federal government's collection, use, and disclosure of personal information have gaps and other potential shortcomings in three broad categories: (1) the Privacy Act and E-Government Act do not always provide protections for federal uses of personal information, (2) laws and guidance may not effectively limit agency collection and use of personal information to specific purposes, and (3) the Privacy Act may not include effective mechanisms for informing the public.

In assessing the appropriate balance between the needs of the federal government to collect personally identifiable information for programmatic purposes and the assurances that individuals should have that their information is being sufficiently protected and properly used, Congress should consider amending applicable laws,

such as the Privacy Act and the E-Government Act, according to the alternatives outlined in our report, including

- revising the scope of the laws to cover all personally identifiable information collected, used, and maintained by the federal government;
- setting requirements to ensure that the collection and use of personally identifiable information is limited to a stated purpose; and
- establishing additional mechanisms for informing the public about privacy protections by revising requirements for the structure and publication of public notices.

In commenting on a draft of our report, OMB officials noted that they shared our concerns about privacy and stated they believe it would be important for Congress to consider potential amendments to the Privacy Act and the E-Government Act in the broader context of all existing privacy and related laws that Congress has enacted.

Though we did not make specific recommendations to OMB, the agency provided comments on the alternatives identified in conjunction with our matter for Congressional consideration. Regarding alternatives for revising the scope of laws to cover all personally identifiable information collected, used, and maintained by the federal government, OMB stated that it would be important for Congress to evaluate fully the potential implications of revisions such as amending the Privacy Act's system-of-records definition. We believe that, given that the Privacy Act's controls on the collection, use, and disclosure of personally identifiable information do not consistently protect such information in all circumstances of its collection and use throughout the federal government, amending the act's definition of a system of records is an important alternative for Congress to consider.

We agree with OMB, however, that any consideration of amendments to the Privacy Act and E-Government Act should be considered thoroughly and within the context of all existing laws. Further, the challenge of how best to balance the federal government's need to collect and use information with individuals' privacy rights in the current technological and political environment

merits a national public debate on all relevant issues, including the alternatives I have highlighted today.

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

## Contacts and Acknowledgements

If you have any questions concerning this testimony, please contact Linda D. Koontz, Director, Information Management, at (202) 512-6240, or KoontzL@gao.gov. Other individuals who made key contributions include John de Ferrari (Assistant Director), Susan Czachor, Nancy Glover, Lee McCracken, David Plocher, and Jamie Pressman.

# WRITTEN STATEMENT

OF

HUGO TEUFEL III
CHIEF PRIVACY OFFICER
U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

UNITED STATES SENATE
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS

FOR A HEARING ENTITLED,

"PROTECTING PERSONAL INFORMATION:
IS THE FEDERAL GOVERNMENT DOING ENOUGH?"

JUNE 18, 2008

**Introduction**

Chairman Lieberman, Ranking Member Collins, and Members of the Committee, it is an honor to testify before you today on the progress of the Privacy Office at the Department of Homeland Security (DHS) and to review the findings and recommendations of the recent report on the framework of Federal privacy law by the Government Accountability Office (GAO). I am particularly pleased to testify again with Linda Koontz, who has become quite familiar with the DHS Privacy Office and our efforts to protect privacy within Departmental Programs. I take great pride in the fact that in many cases her team has found elements of our work to praise, particularly the increasing number and quality of our Privacy Impact Assessments (PIA), the bedrock of a meaningful privacy compliance program. In the rare instances where she and her team found us wanting, I believe their sound recommendations were extremely useful in support of our never-ending mission to improve.

Because this is my first time appearing before this Committee, and indeed any committee of the Senate, I would like to introduce myself and my office. I was appointed Chief Privacy Officer of the U.S. Department of Homeland Security by Secretary Michael Chertoff on July 23, 2006. In this capacity and pursuant to Section 222 of the *Homeland Security Act of 2002*, 6 U.S.C. § 142, my office has primary responsibility for privacy policy at the Department, to include: assuring that the technologies used by the Department to protect the United States sustain, and do not erode, privacy protections

relating to the use, collection, maintenance, and disclosure of personal information; assuring that the Department complies with fair information practices as set out in the *Privacy Act of 1974*; conducting PIAs of proposed rules at the Department; evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government; coordinating with the Officer for Civil Rights and Civil Liberties to ensure that programs, policies, and procedures involving civil rights, civil liberties, and privacy considerations are addressed in an integrated and comprehensive manner; and preparing an annual report to Congress on the activities of the Department that affect privacy. To these duties, the *Implementing Recommendations of the 9/11 Commission Act of 2007* (Pub. L. No. 110-53) added the specific responsibility to conduct privacy impact assessments which was originally required by the E-Government Act of 2002, as well as to provide privacy training to a number of specific programs, coordinate efforts with the Office of Inspector General to investigate privacy complaints, and to issue additional reports to Congress relating to our efforts generally and to the Department's data mining programs. Additionally, I am responsible for overseeing DHS' implementation of privacy-related regulations and policies.

Finally, I also serve as the Department's Chief Freedom of Information Act (FOIA) Officer. In this role, I assure consistent and appropriate Department-wide statutory compliance and harmonized program and policy implementation.

**The GAO Audit**

Earlier this year, GAO conducted a review of the legislative framework for protecting Personally Identifiable Information (PII) and will be issuing a report entitled, "PRIVACY: Alternatives Exist for Enhancing Protection of Personally Identifiable

Information." My office supported this engagement, participating in interviews with members of Linda Koontz's team and providing insights into our own privacy compliance methods. In its report, GAO recommended that Congress consider amending both the Privacy Act and *E-Government Act of 2002* in order to "revis[e] the scope of laws to cover all PII collected, used, and maintained by the Federal Government; set[] requirements to ensure that the collection and use of PII is limited to a stated purpose; and establish[] additional mechanisms for informing the public about privacy protections by revising requirements for the structure and publication of public notices."

Because there were no recommendations directed to DHS or the DHS Privacy Office, in particular, my office did not submit any formal response. Informally, however, we objected to GAO's use of the word "adequacy" to frame its review, for this reason: Adequacy is a term-of-art used by the European Data Protection Authority. Countries outside of Europe deemed to have "adequate" local data protection regimes operate under one set of rules covering international data flows, all others must follow an increased administrative burden. Europe has never found the U.S. adequate creating complications in our commercial and government-to-government relationship with Europe for many years. While it is both helpful and proper for GAO to review the sufficiency of the U.S. data protection framework—or any other synonym for adequacy—it is decidedly unhelpful for them to use language that may be misunderstood by U.S. allies and further hamper vital relationships.

Privacy Compliance - DHS use of the Fair Information Practice Principles

Of course, I share GAO's goal of enhancing privacy protections surrounding the use of the PII government-wide. At DHS, the Privacy Office helps programs achieve this

by maintaining a robust Privacy compliance program. The Privacy Act articulates concepts of how the Federal Government should treat individuals and their information, and imposes duties upon Federal Agencies regarding the collection, use, dissemination, and maintenance of PII. The Homeland Security Act, Section 222(a)(2) states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act.

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS. These principles first appeared in the HEW Report, which was the basis for the passage of the Privacy Act. The FIPPs account for the nature and purpose of the information being collected, maintained, used, and disseminated in relation to DHS' mission to preserve, protect, and secure. They are: Transparency; Individual Participation; Purpose Specification; Data Minimization; Use Limitation; Data Quality and Integrity; Security; and Accountability and Auditing.

Two of GAO's three matters for Congressional consideration are intended to bolster at least four of the FIPPs. For instance, setting requirements to ensure that the collection and use of PII is limited to a stated purpose may enhance the Principles of Purpose Specification, Data Minimization, and Use Limitation. In addition, establishing additional mechanisms for informing the public about privacy protections are intended to enhance the Transparency and Individual Participation Principles.

In general, I have found that strong implementation of the Transparency Principle tends to enhance implementation of the rest of the FIPPs. PIAs and System of Record

Notices (SORNs) are DHS's principal methods of informing the public about the collection, use, maintenance and dissemination of PII. For this reason, the Privacy Office regularly reviews and improves our PIA and SORN guidance, a commitment noted approvingly by GAO. Our Director of Compliance, Rebecca Richards, makes sure these improvements are widely disseminated and understood by her colleagues in the Department, and indeed, the rest of the Federal Government. On May 28, 2008, Ms. Richards delivered her latest PIA and SORN Workshop to more than 125 interested participants from across the government.

In addition to updating and disseminating our guidance, the Privacy Office also updates the PIAs it has already issued. As programs change over time and decisions are made that impact privacy interests, the Privacy Office reexamines the use of PII and issues a new PIA, enhancing understanding of the current state of the program.

Of course, Transparency is furthered through the Privacy Office's practice of publishing our Department's SORNs and as many of the Department's PIAs as is consistent with National Security on our public website, www.dhs.gov/privacy. I note that the Privacy Office conducts PIAs on even the most highly classified programs of the Department. I and a number of my staff carry sufficient security clearances in order to gain full access to the details of such classified programs. Although the PIAs for these may not be made public for many years, in my opinion they still promote the FIPPs because various oversight organizations—GAO, Congress, and the DHS Office of Inspector General, for instance—can use the document to understand the program and its privacy protections. More importantly, such classified or CUI documents are useful to the program to catalogue and understand their own uses of information, including PII.

Implementing OMB and other Guidance

The DHS Privacy Office also fulfils its privacy responsibilities by faithfully executing OMB and other Administration guidance. *The President's Identity Theft Task Force Report* (I.D. Task Force Report), for instance, recommended that Federal Government reduce the unnecessary use of Social Security Numbers (SSN), recognizing that valid SSNs are valuable pieces of information for identity thieves. Less than two months after this report was published, the Privacy Office issued a memo entitled *Use of Social Security Numbers at the Department of Homeland Security*, DHS Privacy Policy Memorandum 2007-02. This policy sets forth the requirements for existing and new programs wishing to continue or initiate use of SSNs, and limits those uses to those that are required by law or pursuant to a specific authorized purpose. Where such use is permitted, the policy also sets limits and/or standards relating to notice to the public, collection and use, security of systems containing SSNs, and retention. We have already begun the process of cataloging and reducing the use of SSN at the Department, and we anticipate this process will lessen the likelihood that PII collected, used, or held by the Department will ever contribute to identity theft.

The Privacy Office has also implemented OMB guidance that followed on the heels of the I.D. Task Force Report. On May 22, 2007, OMB issued a Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*. This guidance required Federal agencies to develop a breach notification policy while ensuring proper safeguards are in place to protect PII. In September 2007, then, the Department issued its *Privacy Incident Handling Guidance* (PIHG), which

frames the response mechanisms DHS employs to reduce the risk of identity theft following a loss of or unauthorized access to PII.

These are just two examples of the role OMB and the Administration play in establishing privacy policy. There are numerous other examples.

Congress Should Consider the Consequences of any Changes to Federal Privacy Law

During my review of GAO's draft report, I had an opportunity to review also OMB's written response to GAO, which I understand will appear in whole as an attachment to the final report.

Let me echo two themes in OMB's response to the then-draft report. First, OMB and I agree that Congress should consider any changes to Federal privacy law—in particular the Privacy Act and E-Government Act—in the broader context of privacy laws enacted by Congress. To the examples cited by OMB, I would add the Homeland Security Act. The Homeland Security Act, amendments to it, and subsequent legislation integrated privacy into the Department in a way targeted at its unique mission. As OMB noted in its letter, Congress has accomplished this integration at other agencies.

Related to looking at each individual agency and policy area, I would like to note that, regardless of how long the list of requirements is, leadership, good judgment, and the collaboration of program owners is essential for strong privacy at any agency. For example, more than 20 percent of DHS' PIAs were not strictly required by E-Government, and that number has trended higher in recent years. The E-Government Act provided a strong 80 percent baseline, but the 20 percent was a result of keen leadership attention to privacy in every facet of the Department's operations. In the end, it may be the last 20 percent will always be identified and addressed through direct, hands on, work

with the operational components and cannot be written ahead of time through legislative requirements.

Second, I join OMB's request that Congress fully examine potential implications of any change to Federal privacy law. Since there is no specific language to comment on within the GAO draft report, I will point to a relatively minor matter we are dealing with within the DHS Privacy Office following enactment of the 9/11 Commission Act, passed during the last session of Congress. We are, of course, busy implementing the many sections related to the Privacy Office. However, Section 803 requires that Privacy Officers "consider whether... the need [for a particular] power is balanced with the need to protect privacy[.]" This new language endorses a "balance" paradigm that we in the Department have explicitly rejected.[1] Respecting privacy is one of the Department's primary missions, and crafting well considered PIAs and SORNs as part of a robust privacy compliance program will enhance program performance, even in fulfilling its homeland security missions. This is an important message the Privacy Office uses to integrate privacy into programs in the earliest stages of development, or as we sometimes say, to bake privacy in. As programs work with the Privacy Office to complete these documents, they must carefully examine their proposed use of PII, within the context of the FIPPs, including critical threshold questions like "What is our authority to collect this information?"; "What are we going to do with this information."; and "What information do we actually NEED?" We have found that this examination imposes an important discipline on programs that ultimately serves their homeland security missions well.

[1] See, e.g., DHS Leadership Journal: A Question of Balance, Teufel III, Hugo, November 23, 2007 (available online at http://www.dhs.gov/journal/leadership/2007/11/question-of-balance.html); DHS Leadership Journal: Privacy *And* Security, Chertoff, Michael, September 26, 2007 (available online at http://www.dhs.gov/journal/leadership/2007/09/privacy-and-security.html).

In all candor, we are still learning how the new language in Section 803 of the 9/11 Commission Act impacts our efforts to work with programs to improve their performance from the beginning, while at the same time being required to evaluate how the need to preserve privacy must limit their proposed objectives—a perspective we do not adhere to.

I am not here to ask for a reconsideration of this portion of the 9/11 Commission Act. I raise it only because this well-intentioned language may have consequences that were not foreseen, and which may ultimately hamper our efforts. It is not hard to imagine that efforts to amend the Privacy Act or E-Government Act will have far greater impact than the example I cite. I can only urge this Committee to make sure those potential implications are deliberately considered and well understood before they are enacted. Once enacted, laws are difficult to amend. As Congress considers amending the government-wide privacy statutory framework, I ask that Congress also recognize: 1) the value of its oversight as a tool to strengthen protections on personally identifiable information, and 2) the value of privacy legislation precisely targeted at specific issues. The DHS Privacy Office stands ready to work with Congress and the President to evaluate any proposed changes.

**Conclusion**

In the past five years, the DHS Privacy Office has built what I believe is a model privacy compliance program, implementing not only the Privacy Act and E-Government Act, but utilizing our inherent authority to examine the privacy impact of programs, offices, rules, and activities under Section 222 of the Homeland Security Act. Congress, too, has endorsed an increased use of the PIA in particular, by requiring PIAs for specific

programs. These developments did not require amendment of either the Privacy Act or the E-Government Act. Yet if Congress should consider amending these authorities, it should be done with full cognizance of the potentially far-reaching consequences.

I thank the Committee and welcome your questions.

**Statement of Ari Schwartz**
**Vice President**
**Center for Democracy & Technology**
**before the**
**Committee on Homeland Security and Governmental Affairs**
**on "Protecting Personal Information: Is the Federal Government Doing Enough?"**

**June 18, 2008**

Chairman Lieberman, Ranking Member Collins, and members of the Committee, thank you for holding this hearing on the protection of personal information by the federal government. I am Ari Schwartz, Vice President of the Center for Democracy & Technology (CDT).

CDT is a non-profit public interest organization founded in 1994 to promote democratic values and individual liberties for the digital age. CDT works for practical, real-world solutions that enhance free expression, privacy, universal access and democratic participation.

**Summary**

Current federal laws and policies provide to those agency officials who care about privacy valuable tools to protect personal information in the hands of the federal government. Unfortunately, these laws and policies clearly have not been implemented consistently in a way that prevents indifference or wanton neglect of personal information. Moreover, even diligent officials find gaps in existing laws, especially because those laws, especially the Privacy Act of 1974, have failed to keep pace with technological change.

To adequately protect privacy in this digital age, when more information is collected and shared than ever before, both Congress and the Executive Branch will need to work together to close the long-recognized gaps in existing laws and policies. At the same time, both branches must foster the leadership and insist upon the measurement capabilities needed to ensure that existing and new laws and policies are implemented uniformly and diligently.

**Shortcomings of the Privacy Act**

Despite a somewhat complicated structure, the Privacy Act of 1974 has generally been successful in offering a baseline standard for the protection of personal information in the hands of the federal government.[1] However, despite this success, some of the Act's flaws were recognized soon after it was passed. Most notably, the Privacy Protection Study Commission (PPSC), a Commission created by the Privacy Act itself, issued an assessment of the law in July 1977 commenting on problems in the Act that have been echoed ever since.

CDT would like to focus on three main areas of concern that have been raised in many reviews of the Privacy Act from the 1977 PPSC assessment to the GAO's report entitled "Alternatives Exist for Enhancing Protection of Personally Identifiable Information" released at this hearing.

I. Scope of the Act

A major concern with the Privacy Act today centers on its most important term, "system of records," which is ill-suited to the current data environment. The definition of "system of records" excludes from the coverage of the Privacy Act information that is not regularly "retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."[2] Thus, as used in the Act, the "system of records" concept is overly restrictive. As the PPSC suggested 30 years ago, the system of records requirement acts as an "on/off" switch for the Privacy Act's other

[1] See, for example, Daniel Solove, The Digital Person, NYU Press, 2004, p. 222.

[2] 5 U.S.C. § 552a(a)(5).

requirements. Information that falls outside of the definition is not covered, no matter how it is used or misused. A classic example of this, that will be familiar to many on this Committee, is the controversy involving the secret acquisition of airline passenger data by the Department of Homeland Security, in which the Privacy Officer for the Department was compelled to conclude that there had been no violation of the Privacy Act despite the fact that the Transportation Safety Administration (TSA) "participation was essential to encourage the data transfer" and "TSA employees involved acted without appropriate regard for individual privacy interests or the spirit of the Privacy Act" no violation occurred in part because the information was not officially a "system of records" under the law.[3]

The definition has also clearly become narrower over time because of major advancements in database technology. Today, it is rare that a system is created with a specific identifier that will be used for searching as was commonplace in the 1970s. Instead, agency personnel and contractors can search on a range of different types of criteria, thereby skirting the law. For example, because it did not specifically search on an identifier, the DHS "ADVISE" data mining program was not covered by a system of records notice. The systems that it linked were, but the narrowness of the concept of a "system of records" gave an incomplete picture of the privacy risks of the ADVISE system. Because of scrutiny, DHS eventually suspended the system. [4] The Privacy Act was certainly intended to address the full range of issue posed by a data mining program like ADVISE, but changes in technology have blurred the scope of the Act's most basic definition.

Another major flaw in the scope of the Act relates to the increased government use of private sector data. In passing the Privacy Act, Congress made it very clear that an agency could not get around the Act by having a contractor hold the data,[5] yet Congress clearly did not envision that data services companies in the private sector would amass enormous databases that federal government agencies could subscribe to and search

---

[3] Department of Homeland Security Privacy Office, "Report to the Public on Events Surrounding jetBlue Data Transfer: Findings and Recomendations," February 20, 2004, p9. http://www.cdt.org/privacy/20040220dhsreport.pdf.

[4] Ryan Singel, "DHS Data Mining Program Suspended After Evading Privacy Review, Audit Finds," Wired Threat Level Blog, August 20, 2007 http://blog.wired.com/27bstroke6/2007/08/dhs-data-mining.html.

[5] 5 U.S.C. § 552a(m).

without either bringing the information into a government database or falling under the provision of the Act that covers contractors. Nevertheless, data brokers that sell information to the federal government today are not held accountable to the privacy, security or data quality standards of the Privacy Act.

II. Breadth of Routine Use Exemptions

The issue that has caused the most concern over the history of the Privacy Act has been the frequent, seemingly standardless invocation of the "routine use" exemption to override the Act's limits on reuse and sharing of information between agencies. The "routine use" exemption was designed to allow agencies to share information in limited circumstances based on the frequency and administrative burden of the project. As early as 1977, the PPSC raised major concerns about how the "routine use" exemption was already being exploited to justify vague exemptions that went beyond the original intention of the Act. Successive Administrations have become ever more accepting of this exemption. Routine uses are now so widely used and utterly unchecked that almost every Privacy Act Notice required by the law lists numerous routine uses, including vague boilerplate language confusing both citizens who want to understand what is happening to their data and the agency personnel responsible for it care. For example, the Department of Defense regularly lists over 20 routine uses and then includes a Web link to a set of 16 "Blanket Routine Uses" that are included with every Privacy Act Notice it publishes.[6] Clearly, this is not what Congress intended.

III. Enforcement

For years GAO and others have reported that the federal government has not properly implemented or enforced the Privacy Act.

For example, implementation difficulties continue to be found in the following areas:

- Publishing all required system of records notices;[7]

---

[6] The "Blanket Routine Uses" are available at http://www.defenselink.mil/privacy/dod_blanket_uses.html
[7] This problem, identified as early as 1987, "Privacy Act System Notices," November 30 1987, GAO/GGD-88-15BR http://archive.gao.gov/d29t5/134673.pdf, is still a major concern today as evidenced in GAO's report released today. In 1990, a more comprehensive GAO study suggested that only 65% of systems

- Consistency in determining how the "system of records" definition and the disclosure provisions apply;[8]
- Building reliable internal assessment measures to ensure personal data are appropriately collected and safeguarded;[9] and
- Establishing basic rules for federal agencies' use of personal information obtained from data resellers.[10]

The problem of lack of enforcement runs deeper than just privacy concerns. Many agencies have simply lost the personal data of millions of Americans. For example, the Chief Privacy Officer of a large agency privately reported to CDT that, when the agency did an audit of its Privacy Act systems of records, it found that half of the systems (and all the records involved) were lost. Other cabinet level agencies do not even audit the existence, location or condition of their systems. As one retiring security official from the Department of Interior recently explained, Interior has been "promiscuous with our data... we don't know anything about our data... we don't know where our data is."[11]

**Shortcomings of the Privacy Impact Assessment Process**

The Privacy Act is not the only federal law affecting the privacy of personal information. Important steps toward updating government privacy policy were taken with the passage of the E-Government Act and efforts toward its effective implementation. In particular, Section 208 of the Act was designed to "ensure sufficient protections for the privacy of personal information."[12] To improve how the government collects, manages and uses

---

covered by the Privacy Act had proper notice procedures. GAO, "Computers and Privacy: How the Government Obtains, Verifies, Uses and Protects Personal Data," August 1990, GAO/IMTEC-90-70BR. Agency personnel have regularly told CDT that there are thousands of systems of records that do not have systems of records notices, suggesting that a substantial proportion of covered systems have still not been properly noticed.

[8] GAO "OMB Leadership Needed to Improve Agency Compliance," June 30, 2003, GAO-03-304 http://www.gao.gov/new.items/d03304.pdf

[9] GAO, "Privacy Act: Federal Agencies' Implementation Can Be Improved," August 22, 1986, GGD-86-107 http://archive.gao.gov/d4t4/130974.pdf

[10] GAO "Agency and Reseller Adherence to Key Privacy Principles," April 4, 2006, GAO-06-421 http://www.gao.gov/new.items/d06421.pdf.

[11] Comments of Ed Meagher, Deputy Chief Information Officer, Department of Interior, before the National Institute of Standards and Technology Information Security and Privacy Advisory Board, June 5, 2008.
[12] PL 107-347, Section 208.

personal information about individuals, Section 208 requires that agencies post privacy notices on their Web sites and that they conduct privacy impact assessments (PIAs).

Section 208(b) of the E-Government Act requires that agencies perform PIAs before (i) developing or procuring new technology that collects, maintains, or disseminates personal information or (ii) initiating new collections of personally identifiable information. These PIAs are supposed to be public documents and are supposed to contain a description of the project, a risk assessment, a discussion of potential threats to privacy, and ways to mitigate those risks. PIAs are intended to ensure that privacy concerns are considered as part of the design of information systems and that the public has access to this element of the decision making process.

Over the past five years, PIAs have become an essential tool to help protect privacy. They are sometimes called "one of the three pillars" of the US government privacy policy.[13] Unfortunately, as with the other privacy laws, federal agencies unevenly implement even the basic requirement of PIAs.

PIA Reporting

The recent OMB Federal Information Security Management Act (FISMA) report to Congress highlighted the fact that agencies, as rated by their own Inspectors General, range from "excellent" to "failing" in their implementations of the PIA requirement.[14] This wide range of compliance is due to two major factors: 1) guidance issued by OMB with respect to PIAs is vague and has simply not provided agencies with the tools they need to successfully implement the PIA requirement and 2) the reporting standards themselves are not uniform, as each Inspector General is basically developing its own standards for issuing these ratings.

---

[13] DHS Chief Privacy Officer Hugo Teufel, *Presentation before the European Commission's Conference on Public Security, Privacy and Technology,* November 20, 2007 Brussels, Belgium. Mr. Teuffel suggested that the three current pillars are the Privacy Act of 1974, Section 208 of the E-Government Act and the Freedom of Information Act.

[14] MB FY 2007 Report to Congress on Implementation of the Federal Information Security Management Act of 2002. http://www.whitehouse.gov/omb/inforeg/reports/2007_fisma_report.pdf.

While some agencies, like the Department of Homeland Security (DHS),[15] have set a high standard for the quality of their PIAs and have continued to improve them over time, the lack of clear guidance has led other agencies to conduct cursory PIAs or none at all. For example, even though the use of RFID in passports has major privacy implications, the US Department of State gave the issue only cursory consideration in its PIA, a document of only ten sentences.[16] Yet DHS received only a "good" mark and the State Department received a "satisfactory" mark in the FISMA report.

Even more troubling is the finding that some agencies simply do not perform PIAs on as many as half their qualifying technologies.[17] An official at the Department of Defense, which received a failing mark in the FISMA report, suggested to CDT that PIAs are still just not considered a priority there and are not taken seriously as an important tool for identifying and addressing privacy and security issues.

Finally, and perhaps most importantly, even those agencies that prepare in depth PIAs too often complete them after a project has been developed and approved. PIAs are supposed to inform the decision making process, not ratify it. They are supposed to be prepared early in the system design process, so they can be used to identify privacy problems before the system design is finalized. They cannot serve this crucial role is they are done after design is completed.

While OMB has begun to take steps to address the inconsistent implementation of PIAs, it should be of great concern to this Committee that some agencies are still not conducting PIAs in a timely and comprehensive manner. The work of those agencies that have taken seriously the mandate to develop PIAs and used them as a tool for analysis and change should be a starting point for developing best practices for all federal agencies. The E-Government Act Reauthorization Act (S.2321) currently in front

---

[15] The DHS Website on Privacy Impact Assessment offers a range of resources to DHS components and to other agencies. http://www.dhs.gov/xinfoshare/publications/editorial_0511.shtm.

[16] http://foia.state.gov/SPIAS/20061.DOS.PIA.Summary.Passport-cleared.pdf Also see CDT's letter May 2, 2007 letter to Secretary of State Rice on the agencies failure to provide adequate PIAs for this and a related project — http://www.cdt.org/security/identity/20070502rice.pdf .

[17] OMB FY2006 Report to Congress on Implementation of the Federal Information Security Management Act of 2002, at www.whitehouse.gov/omb/inforegreports/2006_fisma_report.pdf.

of the Senate includes a provision that would help address these concerns by specifically requiring OMB to create best practices for PIAs across the government. CDT supports this provision.

Private Sector Data

Another concern with Section 208, similar to concern about the coverage of the Privacy Act, is the failure to specifically require PIAs for government access to private sector data. OMB guidelines allow agencies to exempt the government's use of private sector databases from the requirement to conduct PIAs when the commercial data is not "systematically incorporated" into existing databases. CDT believes that this permissive approach is wrong. Companies that provide private sector data to the government have a range of security and privacy practices. Government agencies should use the PIA process to take those issues into account when making decisions about the use of commercial data. Notably, some agencies are already requiring PIAs for uses of commercial data even when the data is not integrated into existing databases despite OMB's guidance.

GAO's report published today points out that, in 2006, it recommended that OMB revise its guidance to clarify the applicability of requirements for PIAs with respect to agency use of data obtained from commercial re-sellers. The GAO further notes that OMB did not address that recommendation[18] and openly disagreed with it in House Oversight and Government Affairs Committee testimony.[19] Simply put, OMB has ignored the serious concerns raised by the ease with which an agency can avoid the PIA requirement simply by subscribing to an information service rather than creating a database of the same information within the agency.

Government Employee Information

---

[18] GAO-03-304.

[19] Karen Evans before the House Committee on Oversight and Government Affairs Subcommittee on Information Policy, Census, and National Archives on "Privacy: The Use of Commercial Information Resellers by Federal Agencies," March 11, 2008. http://informationpolicy.oversight.house.gov/documents/20080318172705.pdf.

Section 208 does not require Privacy Impact Assessments for collections and systems involving information about federal employees. Recent data breaches at federal agencies suggest that the government is not adequately protecting information about its own personnel. For example, earlier this month there was a major breach of patient information at Walter Reed Hospital, [20] presumably no PIA was required for this important database because the patients were federal government employees. PIAs would be one good mechanism for beginning to improve not only the privacy but also the security of systems containing the sensitive data of federal employees.

**Lack of Privacy Leadership**

Some of the blame for the uneven implementation of the Privacy Act clearly falls on the leadership of those individual federal agencies that have not given adequate attention to information privacy and security; their failure stands out because others have done better. But blame also falls on OMB because it is responsible for interpreting and overseeing the implementation of the Privacy Act and Section 208 of the E-Government Act. In June 2003, GAO issued a report at the request of Chairman Lieberman that is still timely, entitled "Privacy Act: OMB Leadership Needed to Improve Agency Compliance." In that report, the GAO identified deficiencies in compliance and concluded: "If these implementation issues and the overall uneven compliance are not addressed, the government will not be able to provide the public with sufficient assurance that all legislated individual privacy rights are adequately protected."[21] Yet, criticism of OMB for failing to provide adequate oversight and guidance to agencies is not new. In 1983, the House Committee on Government Operations raised concerns that OMB had not updated its guidance in the first nine years of the Act's passage.[22] The Department of Justice, which had published an official case law guide to the Act every two years since the late 1980s, has neglected to do so for the past four years.[23]

---

[20] Jennifer C. Kerr, "Walter Reed: Data Breach at Military Hospitals," Army Times, June 3, 2008. http://www.armytimes.com/news/2008/06/ap_walterreed_data_060208/.

[21] GAO-03-304.

[22] House Report No. 98-455.

[23] Ken Mortenson, Acting Chief Privacy and Civil Liberties Officer at DOJ suggested that the delay in publishing the Privacy Act Overview was due to internal changes at the Department and a new version would be released this summer.

OMB is now just beginning to provide the kind of leadership that is needed to help agencies build programs to protect privacy, as evidenced by the changes in its FISMA report to Congress to require some kind of yearly reporting by agencies and the creation of a privacy working group within the CIO Council, led by E-Government Administrator Karen Evans. While these are important steps in the right direction, they are not long-term leadership solutions. The next Administration should be encouraged, on a bi-partisan basis, to make major improvements in Privacy Act implementation and oversight.

**Recommendations**

**1) Expanding Privacy Act Coverage** — CDT agrees with GAO's basic assertion that the Privacy Act definition of "system of records" is out of date. We believe that this issue must be addressed in legislation, and we urge the Committee to introduce such legislation in this Congress. We suggest a new definition that would ensure coverage of all information that reasonably can be expected to specifically identify an individual.

**2) Closing Privacy Act Loopholes** — CDT also urges the Committee to consider legislation that would limit the "routine use" exemptions. This could be accomplished by limiting the definition to encompass only uses compatible with the purpose for which the information in the record was collected or obtained, and consistent with the conditions or reasonable expectations of use and disclosure under which the information in the record was provided, collected, or obtained. In addition, we urge clarifying the Act to make it clear that its core principles apply to commercial data used by the government.

**3) Improving Privacy Impact Assessments** — As we testified before this Committee last year,[24] CDT supports the creation of best practices for PIAs as called for in the E-Government Act Reauthorization Act (S.2327) as passed by this Committee. CDT also urges the Committee to require PIAs for any program that uses commercial data,

---

[24] Statement of Ari Schwartz, Deputy Director, Center for Democracy & Technology before the Committee on Homeland Security and Governmental Affairs on E-Government, December 11, 2007 http://www.cdt.org/testimony/Schwartz_egov_Testimony_20071211.pdf.

whether the personal information used will be stored at the agency or kept by the commercial entity. CDT supports requiring PIAs government-wide for rulemakings as well as information collections. This is currently the law only for DHS. CDT also supports requiring PIAs for systems of government employee information. Finally, we stress the importance of ensuring that PIAs are begun early in the development of a system or program and that they are completed before the project or procurement begins, so that the findings of the PIA can shape rather than merely ratify the activity's impact on privacy.

**4) Creating a Chief Privacy Officer Position at OMB Who Will Run a Separate CPO Council** — Undoubtedly, at the end of the Clinton Administration, privacy had a higher profile within the federal government than at any other time. The main reason for this level of greater attention was the creation of a Chief Privacy Counselor at OMB staffed by Peter Swire, who is testifying here today. CDT would like to see a similar permanent Chief Privacy Officer (CPO) position at OMB written into law.

At the agency level, the new legislative requirements for appointment of CPOs have clearly been a success, Yet many large agencies that have a lot of personal information still do not have statutory CPO, including cabinet agencies such as the Department of Veterans Affairs, the Department of the Interior and the Department of Housing and Urban Development. Based on this experience, we believe that all large agencies (the so called "CFO agencies" based on the threshold from the CFO Act) should be required to have a CPO. These privacy officials should be placed outside of the structure of the CIO office where resources and attention are almost always rightly focused on systems procurement and maintenance instead of information policy. In addition, department heads should ensure that CPOs are engaged in the early stages of developing policies and planning systems or programs that will have a privacy impact. CDT also urges the creation of a CPO Council with a similar structure to the CIO and CFO Councils. While E-Government Administrator Karen Evans' leadership to build a privacy working group of CPOs at the CIO Council utilizing CIO funds is greatly appreciated and a step forward, in the long-run it is not a sustainable model for intergovernmental privacy efforts.

**5) Increasing and Improving Privacy Reporting and Audits** — OMB requirements for privacy reporting in FISMA are a major leap forward in focusing attention on privacy

issues, but getting the right implementation and accountability processes in place is an essential goal. Most importantly, OMB should be required to create standardized measurements for privacy protecting processes (such as, quality of both the PIA process and the PIAs themselves) and make them public. CDT also believes that the Committee should require that the systems of greatest privacy risk (both in size and in program activity) undergo regular audits by IGs and/or, when IGs are overwhelmed or not experts in privacy, by outside third party audit firms.

**Conclusions**

In the past, CDT has called for creation of a new one-year commission to study the Privacy Act and privacy policy in the government and offer solutions. With the release of the GAO report and the numerous hearings on this and related issues in this Congress, we believe that the basic work that would have been done by such a commission has been completed. In essence there is now consensus around a set of sound recommendations for action by Congress and the Executive Branch to fill gaps and loopholes in privacy law and policy. CDT urges this Committee to draft a bill with the recommendations outlined above and quickly bring it to the Senate floor so that the next President can have the right tools in place upon taking office and can get started immediately on strengthening privacy in the federal government.

Center for American Progress

**STATEMENT OF PROFESSOR PETER P. SWIRE**
**C. WILLIAM O'NEILL PROFESSOR OF LAW**
**MORITZ COLLEGE OF LAW, THE OHIO STATE UNIVERSITY**
**SENIOR FELLOW, CENTER FOR AMERICAN PROGRESS**

**BEFORE**

**THE U.S. SENATE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS**

**ON**

**"PROTECTING PERSONAL INFORMATION: IS THE FEDERAL GOVERNMENT DOING ENOUGH?"**

**JUNE 18, 2008**

Chairman Lieberman, Ranking Member Collins, and members of the Committee:

Thank you for the opportunity to testify today on the topic of "Protecting Personal Information: Is the Federal Government Doing Enough?" Chairman Lieberman, I salute you for your personal leadership on these issues, such as your privacy agenda that stated: "Joe Lieberman believes that a technologically advancing world demands a new compact to keep personal information private and shed light on the workings of government."[1] This committee played a key role on a bipartisan basis in enacting the E-Government Act of 2002, a valuable statute that has placed Privacy Impact Assessments at the center of privacy protection in the federal government. I also commend the Government Accountability Office for its thorough and thoughtful new report on protecting privacy in federal agencies.

My testimony highlights two emerging areas where I believe the Committee can and should take prompt action—biometrics and identification systems. I briefly highlight my recommendations here, and explain the basis for them in the full testimony.

For biometrics, such as fingerprints, I recommend three actions.

First, the E-Government Act of 2002 should be amended to provide that the default for storage and transmission of biometrics should be in encrypted form. An exception to this encryption policy should be permitted only if it is justified in a Privacy Impact Assessment, and has received specific authorization from the Chief Privacy Officer for the agency. It is worth considering whether similar requirements

should be imposed on private-sector users of biometrics, in order to prevent private-sector compromise of biometrics that are used by the government.

Second, access to biometric databases should be subject to effective audit systems.

Third, the Committee should ask for a report from key federal privacy offices, including the Department of Homeland Security and the Department of Justice, on the "biometric encryption" approach that is designed to use fingerprints and other biometrics with greater security and privacy. The report should examine the advantages and disadvantages of this approach compared to current biometrics approaches, and should propose settings for pilot projects of the biometric encryption approach.

For identification systems, the Center for American Progress recently published a report that I co-authored with Cassandra Q. Butts, "The ID Divide: Addressing the Challenges of Identification and Authentication in American Society."[2] The testimony describes key aspects of that report. In terms of action by this Committee, I submit the following recommendation:

To address the full range of privacy and other risks from identification systems, this Committee should thus consider an expansion of the E-Government Act of 2002 to have a more thorough due diligence process of new identification systems. The analysis should include consideration of the following principles: achieve real security or other goals; accuracy; inclusion; fairness and equality; effective redress mechanisms; and equitable financing for systems.

In addition, I have reviewed a near-final draft of the testimony for this hearing of Ari Schwartz, Vice President of the Center for Democracy and Technology. Mr. Schwartz has been a leader for the past decade on how privacy should be protected in the federal government. His testimony does an excellent job of recommending next steps for federal privacy protection. I specifically agree with his five key recommendations:

1. Expanding Privacy Act coverage
2. Limiting Privacy Act loopholes
3. Improving Privacy Impact Assessments
4. Creating a Chief Privacy Officer at OMB who will run a separate CPO Council
5. Increasing and improving privacy reporting and audits

**Background**

I am the C. William O'Neill Professor of Law at the Moritz College of Law of the Ohio State University, and a Senior Fellow at the Center for American Progress. I live in the Washington, D.C. area. I also serve on a pro bono basis as a Policy Fellow with the Center for Democracy and Technology.

From 1999 until early 2001 I served as the Chief Counselor for Privacy in the U.S. Office of Management and Budget. In that role, I was essentially acting as Chief Privacy Officer for the U.S. government. I was responsible for coordinating administration policy on public- and private-sector uses of personal information, and served as point of contact with privacy and data protection officials in other countries. During this time, along with many other activities, we: responded to agency questions about the Privacy Act; created guidance for privacy policies on federal web sites; issued guidance on the use of cookies on federal sites; and instituted Privacy Impact Assessments as a "best practice" for new federal information systems.[3]

Since leaving OMB, I have worked and written on a very wide variety of privacy and computer security issues. For instance, I was the only person to testify to Congress on privacy issues at the time of the creation of the Department of Homeland Security, and have written on government privacy issues arising from information sharing, foreign intelligence surveillance, the Patriot Act, and many other topics. My testimony and other writings appear at www.peterswire.net and www.americanprogress.org.

**New policy needed for biometrics**

Biometrics is the first priority area where I believe that federal privacy policy needs to improve. The term "biometric" means something that measures your biology, such as a fingerprint, iris scan, or DNA sample. The focus of my remarks is on what computer scientist Terrence Boult has called the "biometric dilemma"—the more we use biometrics, the more likely they will be compromised and hence become useless for security. Professor Boult's basic point is that fingerprints and other "secrets" become more widely known once they are used repeatedly, and thus don't remain "secret" after all.

The federal government has been rapidly increasing its reliance on biometrics in recent years, especially fingerprints. Privacy and security protections have not kept pace, however. Recent statements by Homeland Security Secretary Chertoff show the reason for concern. Secretary Chertoff spoke in Canada in April in support of the "Server in the Sky" program to share fingerprints among the U.S., Canada, the U.K., and Australia.[4] In a briefing with the Canadian press, Chertoff made the statement that fingerprints are "not particularly private":

> QUESTION: Some are raising that the privacy aspects of this thing, you know, sharing of that kind of data, very personal data, among four countries is quite a scary thing.
>
> SECRETARY CHERTOFF: Well, first of all, **a fingerprint is hardly personal data because you leave it on glasses and silverware and articles all over the world, they're like footprints. They're not particularly private.**

Fortunately, despite this statement by Secretary Chertoff, the Department of Homeland Security does include fingerprints and other biometrics in its definition of "personally identifiable information," the information that triggers a privacy impact assessment when used by government.

The problem remains, however, that current protections for biometric information are systematically weak. Secretary Chertoff, in the same Canadian visit, said that "It's very difficult to fake a fingerprint." That is not true. A quick web search on "fake fingerprints" turns up cheap and easy methods for do-it-at-home fake fingerprints. As discussed by security expert Bruce Schneier, one technique is available for under $10. It was tried "against eleven commercially available fingerprint biometric systems, and was able to reliably fool all of them."[5] In brief, the digital image of the print is sent to a laser printer. It is then easily transferred to a gel that covers the imposter's finger.

Two policies can help ensure that federal biometric efforts are done well, with benefits for privacy and security. If biometrics are badly deployed, by contrast, we could create a new generation of identity theft problems from fake fingerprints and other biometrics. It is hard enough to get a new Social Security number once you have been the victim of identity theft. Once your fingerprint is known, though, you can't get a new finger.

The first policy is to use effective encryption in connection with current forms of biometrics. DHS and other federal agencies are creating an increasing number of databases containing fingerprints and other biometrics. At the same time, federal agencies have suffered a series of serious data breaches, such as the well-known incident where the Veterans Administration lost the personal information of over 26 million veterans. The combination of biometric databases and data breaches is a scary prospect, indeed—a similar data breach with respect to fingerprints could mean that fingerprints would be permanently insecure for all of the millions of people whose information was in the data breach.

In response, federal policy should be to store and transmit biometrics in encrypted form. The use of strong encryption greatly reduces the risks from data breaches, because identity thieves won't be able to read the fingerprints or other data even if they get access to a federal database or stolen laptop. **The E-Government Act of 2002 should be amended to provide that the default for storage and transmission of biometrics should be in encrypted form. An exception to this encryption policy should be permitted only if it is justified in a Privacy Impact Assessment, and has received specific authorization from the Chief Privacy Officer for the agency. It is worth considering whether similar requirements should be imposed on private-sector users of biometrics, in order to prevent private-sector compromise of biometrics that are used by the government.** These requirements would not apply to publicly viewable biometrics, such as the picture of a face.

This policy—using encryption of the full fingerprint or other biometric in storage and in transit—reduces the risk of important types of data breach. It reduces the problem that an *unauthorized* person will gain access to the fingerprint, because an accidental spill or an intrusion by a hacker will only gain access to encrypted data. It does not help, however, against misuse by those who are authorized to see the biometrics. A major computer security risk is that an insider will break the rules. In most computer security settings, a majority of the harms come from this sort of malicious insider—those who have access but go beyond their authority. One important counter-measure is to perform audits on access to sensitive systems, in order to detect, deter, and help punish such violators. **Access to biometric databases should thus be subject to effective audit systems.** An audit system caught State Department contractors earlier this year who had improperly accessed the passport files of Sen. Obama and other presidential candidates. Effective audits should similarly be in place for access to sensitive databases containing biometrics.

Encryption within the central database, however, does not provide long-term protection for fingerprints and other biometrics. The reason is that the number of *authorized* users generally climbs swiftly in today's information -sharing environment. The "Server in the Sky" program, discussed by Secretary Chertoff, is one example. It proposes to share fingerprint databases among four nations, and other information-sharing programs are in the works for state and local officials and also to more countries over time. The fingerprint requirements that apply to most non-U.S. visitors to the U.S. are encouraging other countries to require U.S. travelers to provide our fingerprints as a condition of entry to a growing list of other countries. We are thus moving toward a new reality where fingerprints for a large and growing portion of our population are insecure—they are being held in many settings where a breach can occur. And, once the breach does occur, then we know we can't give the person a new fingerprint. Unlike a credit card number, which is "revoked" when a problem happens, my fingerprint is no longer a good identifier once others can use it as well.

Fortunately, slightly more sophisticated biometric technology can greatly reduce these identity theft and other privacy risks. Ann Cavoukian, the Privacy Commissioner for Ontario, has been a global leader in promoting what is called "biometric encryption." With biometrics expert Alex Stoianov, she has

published: "Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy."[6] As explained by a prominent biometrics researcher:

> "In Biometric Encryption, you can use the biometric to encrypt a PIN, a password, or an alphanumeric string, for numerous applications—to gain access to computers, bank machines, to enter buildings, etc. The PINs can be 100s of digits in length; the length doesn't matter because you don't need to remember it. And most importantly, all one has to store in a database is the biometrically encrypted PIN or password, not the biometric template."[7]

The privacy and security advantages of this approach are large. The system owner, such as an employer, gains the advantages of traditional biometrics approaches, such as being confident that only the correct person can gain access. For the individual, there is the large privacy advantage that a breach by the system owner will not compromise the fingerprint or other biometric. Only that one PIN is lost, and the individual can generate a new PIN/password using the same fingerprint or other biometric. In the long run, systems owners also benefit, because this approach is much less likely to be based on a compromised fingerprint than under the current, flawed approach.

After careful review of the technical and policy literature, Cavoukian and Stoianov highlighted six advantages of the biometric encryption approach:

1. NO retention of the biometric image or template
2. Multiple/cancellable/revocable identifiers
3. Improved authentication security: stronger binding of user biometric and identifier
4. Improved security of personal data and communications
5. Greater public confidence, acceptance, and use; greater compliance with privacy laws
6. Suitable for large-scale applications

In terms of legislative action, this Committee should support a careful federal examination of this promising approach, which appears likely to be better from both a privacy and a security perspective. As a first step, **the Committee should ask for a report from key federal privacy offices, including the Department of Homeland Security and the Department of Justice, on the biometric encryption approach. The report should examine the advantages and disadvantages of this approach compared to current biometrics approaches, and should propose settings for pilot projects of the biometric encryption approach.** This sort of prompt review of the biometrics encryption approach can form the basis going forward for better security and privacy in the deployment of biometric systems.

**The ID Divide**

The second priority area is to ensure better privacy protections are build into government identification systems. I was recently co-author, with Cassandra Q. Butts, of "The ID Divide: Addressing the Challenges of Identification and Authentication in American Society." This report was based on a working group of experts in a wide range of contexts: national and homeland security; immigration; voting; electronic health records; online authentication; computer security; and privacy and civil liberties. The project, at the Center for American Progress, arose from the recognition that the next administration will face identification and authentication issues that cut across this range of issue areas.

The story from the Indiana primary about the 12 nuns who were turned away from voting because they lacked a government-issued ID, illustrates the sorts of challenges facing Americans who are increasingly being asked to identify themselves. And in 2006 the personal identification data of 26.5 million veterans was lost from a government laptop, one in a series of data breaches that threaten the integrity of everyone's identification.

The 12 nuns are among over 20 million other voting age citizens without drivers' licenses, and they join the 26.5 million veterans and many millions of other Americans who suddenly find themselves on the wrong side of what we call the ID Divide—Americans who lack official identification, suffer from identity theft, are improperly placed on watch lists, or otherwise face burdens when asked for identification. The problems of these uncredentialed people are largely invisible to credentialed Americans, many of whom have a wallet full of proofs of identity. Yet those on the wrong side of the ID Divide are finding themselves squeezed out of many parts of daily life, including finding a job, opening a bank account, flying on an airplane, and even exercising the right to vote.

In considering this ID Divide, the report developed a set of six principles for identification systems:

**1. Achieve real security or other goals**

New identification systems proposed in the name of security should be subject to a due diligence review to ensure that they actually promote security and do so cost-effectively compared to other available options. Similarly, identification systems proposed for other purposes, such as immigration policy, should only be deployed after they are shown to be effectively related to achieving the specified policy goals. This principle comes first for a simple reason—the financial and other costs of a new system are justified only if they actually achieve security or other goals. If they do not, then the analysis should end at this step.

**2. Accuracy**

A system will only work in the long run if it has a high level of accuracy. Any system, such as a watch list, has "false positives" (people treated as terrorist suspects mistakenly) and "false negatives" (people who are dangerous who evade detection by the system). A proposed system should be carefully vetted to ensure that the accuracy produced by the system will result in a manageable number of false positives and negatives.

**3. Inclusion**

As ID checks spread, it becomes increasingly important to ensure that people have a workable way to reduce the effects of the ID Divide. In many instances, there may be opportunities to rely on authentication approaches other than full identification. Where identification is used, however, then a goal of the policy process should be to foster inclusion of eligible persons.

**4. Fairness and equality**

New authentication and identification systems should be designed with consideration of their effects on the less wealthy and others who would suffer disproportionate burdens from any given design. Equality principles are especially important with respect to fundamental rights, such as the right to vote, and for any system where use of the ID is vital to daily tasks, such as opening a bank account or proving

eligibility for a job. Where necessary, in order to enable people to live fully in society, fees should be waived based on financial hardship. Procedures for reasonable exceptions should also be developed, in recognition that any one method of identification will not work for the entire eligible population.

**5. Effective redress mechanisms**

Stricter and more numerous identification systems mean that burdens increase greatly on individuals who are mistakenly put on watch lists or otherwise disadvantaged by the system. An integral part of system design must be to have effective redress mechanisms. Otherwise, individuals will be turned into second-class citizens, deprived of the ability to conduct daily activities of life in a normal way. An effective security system must have not just on-ramps, but off-ramps as well. A properly designed system will allow government to distinguish between those who actually pose a threat and those who do not, and to proactively remove names from the watch list without a formal petition. If the security system remains the one-way street it is now, then it will inevitably collapse from its own weight.

**6. Equitable financing for systems**

A major criticism of the REAL ID Act has been its unfunded mandates. Congress has only provided the states with a small fraction of the expenses of implementing the federal requirements, now estimated at $4 billion over 10 years, but perhaps more. Along with such unfunded expenses to states and localities, REAL ID and other new identification systems impose off-budget costs on individuals who must spend time and money to meet the system's requirements. These include: tracking down birth certificates and other documentation; the time needed to try to resolve problems; and the costs to eligible individuals who get put on watch lists or otherwise cannot meet the system requirements. New identification systems, built for the common good, should thus be funded in a transparent and equitable way.

In order to implement these principles for identification, our report calls for a more thorough "due diligence" process when considering and implementing identification systems. The term "due diligence" is used in mergers and acquisitions and other important corporate transactions to describe the careful vetting before a company makes a major investment. Proponents of a merger (or, in our case, of a new identification program) can err on the side of optimism, concluding too readily that the benefits of a merger (or an ID or other security program) will demonstrably improve the situation. In response, a due diligence process looks for the characteristic ways that things might go wrong.

This insight of a due diligence process exactly corresponds to this Committee's support for a privacy impact assessment under the E-Government Act of 2002. The privacy impact assessment is a crucial step, and the Privacy Office at the Department of Homeland Security has made important strides in doing rigorous privacy impact assessments for some authentication systems, such as the Transportation Workers Identification Card.

When it comes to authentication systems, however, a broader analysis is required than exists currently under privacy impact assessments. **To address the full range of privacy and other risks from identification systems, this Committee should thus consider an expansion of the E-Government Act of 2002 to have a more thorough due diligence process of new identification systems. The analysis should include consideration of the principles of: achieve real security or other goals; accuracy; inclusion; fairness and equality; effective redress mechanisms; and equitable financing for systems.**

Identification systems are being rapidly considered and deployed in the Department of Homeland Security and elsewhere in the federal government. Our report on the ID Divide shows a range of serious questions about the wisdom of many of these identification systems, both as a policy matter and at the technical level. The biometrics discussion in this testimony, and included in the report, shows that badly implemented biometric and other identification approaches can actually increase the problem of identity theft, leading to new rounds of privacy and security problems for millions of Americans. This Committee should provide strong oversight of how new identification systems are actually being implemented, and should consider legislation to do an expanded due diligence review of new identification systems.

**Conclusion**

In conclusion, I thank the Committee for requesting the GAO report and for all of its work on privacy and computer security issues in the federal government. My testimony today has focused on two emerging areas of priority concern—new biometrics and identification systems. Attention to those issues should be given while also carefully considering the numerous other privacy issues raised by the GAO and in other testimony today, including by the Center for Democracy and Technology.

---

[1] "Joe Lieberman's Plan to Protect Personal Privacy and Break the Bush Wall of Secrecy: Safeguarding Personal Information and Making Government Open and Accountable to the Public," Jan. 9, 2004, available at http://www.fas.org/sgp/news/2004/01/lieb010904.html.

[2] http://www.americanprogress.org/issues/2008/06/id_divide.html.

[3] For contemporaneous descriptions of our privacy efforts, see Peter P. Swire, "The Administration Response to the Challenges of Protecting Privacy," (2000), available at http://www.peterswire.net/pspublications.htm; "How Well Did the Clinton Administration Do on Privacy Rights?" Jan. 23, 2001, available at http://seclists.org/politech/2001/Jan/0058.html.

[4] "Chertoff Says Fingerprints Aren't 'Personal Data'", available at http://thinkprogress.org/2008/04/16/chertoff-fingerprints/.

[5] Bruce Schneier, "Fun with Fingerprint Readers," (May 15, 2002), available at http://www.schneier.com/crypto-gram-0205.html#5.

[6] Ann Cavoukian & Alex Stoianov, "Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy," (March 2007), available at http://www.ipc.on.ca/images/Resources/up-1bio_encryp.pdf.

[7] Id. at 16 (quoting Dr. George Tomko).

**Written Statement of**
**Susan E. Dudley, Administrator, Office of Information and Regulatory Affairs**
**and**
**Karen Evans, Administrator, Office of E-Government and Information Technology**
**Office of Management and Budget**

**Committee on Homeland Security and Governmental Affairs**
**"Protecting Personal Information: Is the Federal Government Doing Enough?"**
**June 18, 2008**

Chairman Lieberman and Ranking Member Collins, thank your for the opportunity to provide this statement for the record for your hearing on the privacy safeguards federal agencies place on individuals' information and the adequacy of the current statutory privacy framework.

This Administration shares this Committee's goal of safeguarding the privacy of individuals and has made it a priority. The Administration has made considerable progress implementing the recommendations of the President's Identity Theft Task Force, issued new guidance based on the Task Force findings and the lessons of the past two years, and worked diligently to execute the statutory requirements of the Privacy Act of 1974, the Paperwork Reduction Act of 1981, and E-Government Act of 2002. Safeguarding personally identifiable information in the possession of the government and preventing its breach are essential to ensure the government retains the trust of the American public. This is a responsibility shared by officials accountable for administering operational and privacy and security programs, legal counsel, Agencies' Inspectors General and other law enforcement, and public and legislative affairs.

The U.S. Government Accountability Office's (GAO's) draft report, "Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information" (GAO-08-536), identifies as a matter for congressional consideration revising the Privacy Act and the E-Government Act.

As we stated in our comments to GAO over the past year, we urge Congress to consider any revisions in the broader context of the privacy statutes Congress has already enacted and the privacy protections agencies have implemented within the current statutory framework. The Privacy Act and E-Government Act, along with the Paperwork Reduction Act, provide a government-wide statutory foundation for protecting individuals' privacy. Congress has also enacted legislation tailored to meet individuals' privacy needs in specific policy areas, such as healthcare, statistical research, tax administration, intelligence, law enforcement, and homeland security.

Through OMB's Office of Information and Regulatory Affairs, we ensure agencies are aware of Federal policies governing the information they are collecting, maintaining, and transmitting through regulatory actions. When a significant regulatory action undergoes

interagency review under Executive Order 12866, OMB analysts consider existing privacy and security laws and policies throughout the review process. Specifically, review of proposed regulations can include the following -- appropriate information handling and protection for sensitive information within agencies (including personal information), appropriate mechanisms for contractor oversight and review, and coordinated incident handling and response (as well as corrective actions) when something does go wrong. In addition, OMB analysts work with representatives from other agencies on matters arising from new statutory privacy protections on an as needed basis (e.g., the HHS HIPAA regulations and financial privacy notices,) and in developing Administration policy on current privacy issues such as identity theft, social security number (SSN) protection, and do-not-call efforts.

Through the President=s Management Agenda (PMA) and the electronic government scorecard, OMB quarterly examines agency progress. In order to Amaintain green@ on this scorecard, agencies must complete privacy impact statements (PIA) for 90% of applicable systems. In addition, agencies must ensure 90% of systems with personally identifiable information have systems of records notices (SORN). In addition, OMB policy requires agencies to submit a capital asset plan and business case justification for all major information technology investments. In this justification, agencies must answer a series of privacy management questions and describe how the investment meets the requirements of law and policy. In particular, OMB asks if there is a PIA or a SORN covering each system and if so the agency provides the internet link to it as part of the capital asset plan.

As part of our work on the Identity Theft Task Force, OMB and the Department of Homeland Security developed a paper identifying common risks (or "mistakes") and best practices to help improve agency security and privacy programs. Each risk is associated with selected best practices and important resources to help agencies mitigate and avoid these risks. All of the best practices and important resources are inter-related and complementary, and they can be broadly applied when administering agency information security and privacy programs. A copy of this paper can be found at http://csrc.nist.gov/pcig/document/Common-Risks-Impeding-Adequate-Protection-Govt-Info.pdf.

Through OMB Memorandum M-05-08, agencies identified a senior official with overall agency-wide responsibility for information privacy issues. Consistent with the Paperwork Reduction Act, an agency Chief Information Officer (CIO) can perform this role. Alternatively, if the CIO, for some reason, is not designated, the agency may have designated another senior official (at the Assistant Secretary or equivalent level) with agency-wide responsibility for information privacy issues. In any case, the senior agency official has authority within the agency to consider information privacy policy issues at a national and agency-wide level.

Building on the findings of the Task Force, OMB issued Memorandum M-07-16 of May 22, 2007, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information.* In addition to providing a framework for reducing the risk of PII breaches, M-07-16 required agencies to:

- establish breach notification policies;

- emphasized the importance of establishing rules of conduct for users, developers, or operators of Privacy Act systems of records, which has been a long-standing requirement under the Privacy Act of 1974;
- review and reduce the volume of PII handled "to the minimum necessary for the proper performance of a documented agency function;"
- encrypt all sensitive information on mobile computers/devices carrying agency data, unless the Deputy Secretary makes a written determination stating the data are not sensitive.

In order to support agencies responding to PII breaches, the General Services Administration created a government-wide vehicle for acquisition of independent risk analysis services. It focuses on an agency's need for independent risk analysis documenting the level of risk for potential misuse of sensitive information associated with a particular data breach by offering a variety of services, including metadata analysis, pattern analysis, and reports on the probability compromised data has been used to cause harm.

OMB recently released the FY 2007 Report to Congress on Implementation of the Federal Information Security Management Act of 2002 (FISMA), which reports on key measures of agency privacy programs, including SORNs and PIAs. In OMB Memorandum M-08-09 of January 18, 2008, *New FISMA Privacy Reporting Requirements for FY 2008*, we outlined increased reporting of key privacy measures for next year's FISMA report to provide more information to the public on agency privacy efforts.

OMB is continuously striving to improve government practices regarding personal information. We provide guidance and oversight to the agencies through many channels at both the staff and executive levels. We regularly engage in formal and informal communications, both written and oral, with agency CIOs and Senior Agency Officials for Privacy. We also hold regular staff-level meetings with members of the federal privacy community to facilitate interagency discussion of relevant issues as well as provide an open forum for direct communications with OMB as part of the Privacy Committee co-chaired by OMB and Justice as part of the CIO Council.

As Congress considers fundamental revisions to the privacy laws, we would like to highlight the importance of fully evaluating the full range of potential implications for such changes. This guidance, reporting and other transparency requirements, and the underlying statutory framework has been developed over the past three decades and provides an intricate and operationalized system for federal privacy protection. As OMB noted in its comments on the draft GAO report, "We believe that it would be important for Congress, in considering such a fundamental change to the Privacy Act, to consider the full range of implications flowing from that change. It may be that, based on this consideration, other legislative alternatives might be identified that would be more desirable in terms of strengthening privacy protections in the most effective and efficient manner."

Thank you for the opportunity to provide testimony on these important issues. We look forward to partnering with you as you consider these issues and to working to fully execute current statutory privacy protections. We would be happy to answer questions for the record.

United States Government Accountability Office

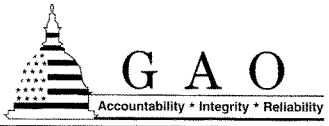
GAO

Report to Congressional Requesters

May 2008

# PRIVACY

# Alternatives Exist for Enhancing Protection of Personally Identifiable Information




GAO-08-536

May 2008

GAO
Accountability·Integrity·Reliability
**Highlights**

Highlights of GAO-08-536, a report to congressional requesters

# PRIVACY

## Alternatives Exist for Enhancing Protection of Personally Identifiable Information

### Why GAO Did This Study

The centerpiece of the federal government's legal framework for privacy protection, the Privacy Act of 1974, provides safeguards for information maintained by federal agencies. In addition, the E-Government Act of 2002 requires federal agencies to conduct privacy impact assessments for systems or collections containing personal information.

GAO was asked to determine whether laws and guidance consistently cover the federal government's collection and use of personal information and incorporate key privacy principles. GAO was also asked, in doing so, to identify options for addressing these issues.

To achieve these objectives, GAO analyzed the laws and related guidance, obtained an operational perspective from federal agencies, and consulted an expert panel convened by the National Academy of Sciences.

### What GAO Recommends

To address the issues identified by GAO, Congress should consider revising privacy laws in accordance with the alternatives outlined in the report. While OMB could address some of these issues in its guidance to federal agencies, Congress is ultimately responsible for balancing the needs of government and individual privacy rights. OMB commented that the Congress should consider these alternatives in the broader context of all privacy and related statutes.

To view the full product, including the scope and methodology, click on GAO-08-536.
For more information, contact Linda Koontz at (202) 512-6240 or koontzl@gao.gov.

### What GAO Found

Increasingly sophisticated ways of obtaining and using personally identifiable information have raised concerns about the adequacy of the legal framework for privacy protection. Although the Privacy Act, the E-Government Act, and related guidance from the Office of Management and Budget set minimum privacy requirements for agencies, they may not consistently protect personally identifiable information in all circumstances of its collection and use throughout the federal government and may not fully adhere to key privacy principles. Based on discussions with privacy experts, agency officials, and analysis of laws and related guidance, GAO identified issues in three major areas:

***Applying privacy protections consistently to all federal collection and use of personal information.*** The Privacy Act's definition of a "system of records" (any grouping of records containing personal information retrieved by individual identifier), which sets the scope of the act's protections, does not always apply whenever personal information is obtained and processed by federal agencies. One alternative to address this concern would be revising the system-of-records definition to cover all personally identifiable information collected, used, and maintained systematically by the federal government.

***Ensuring that collection and use of personally identifiable information is limited to a stated purpose.*** According to generally accepted privacy principles of purpose specification, collection limitation, and use limitation, the collection of personal information should be limited, and its use should be limited to a specified purpose. Yet, current laws and guidance impose only the modest requirements in these areas. While, in the post-9/11 environment, the federal government needs better analysis and sharing of certain personal information, there is general agreement that this need must be balanced with individual privacy rights. Alternatives to address this area of concern include requiring agencies to justify the collection and use of key elements of personally identifiable information and to establish agreements before sharing such information with other agencies.

***Establishing effective mechanisms for informing the public about privacy protections.*** Another key privacy principle, the principle of openness, suggests that the public should be informed about privacy policies and practices. Yet, Privacy Act notices may not effectively inform the public about government uses of personal information. For example, system-of-records notices published in the *Federal Register* (the government's official vehicle for issuing public notices) may be difficult for the general public to fully understand. Layered notices, which provide only the most important summary facts up front, have been used as a solution in the private sector. In addition, publishing such notices at a central location on the Web would help make them more accessible.

# Contents


| | | |
|---|---|---|
| **Letter** | | 1 |
| | Results in Brief | 4 |
| | Background | 8 |
| | The Privacy Act and E-Government Act Do Not Always Provide Protections for Federal Uses of Personal Information | 21 |
| | Laws and Guidance May Not Effectively Limit Agency Collection and Use of Personal Information to Specific Purposes | 30 |
| | The Privacy Act May Not Include Effective Mechanisms for Informing the Public | 43 |
| | Conclusions | 48 |
| | Matter for Congressional Consideration | 48 |
| | Agency Comments and Our Evaluation | 48 |
| **Appendix I** | **Objective, Scope, and Methodology** | 52 |
| **Appendix II** | **National Academy of Sciences Expert Panel Participants** | 54 |
| **Appendix III** | **Privacy Act Exemptions and Exceptions to the Prohibition Against Disclosure without Consent of the Individual** | 56 |
| **Appendix IV** | **OMB Privacy Guidance** | 60 |
| **Appendix V** | **Comments from the Office of Management and Budget** | 63 |
| **Appendix VI** | **GAO Contact and Staff Acknowledgments** | 68 |
| **Related GAO Products** | | 69 |

## Tables

Table 1: The Fair Information Practices 9
Table 2: Major Federal Laws That Address Federal Agency Use of Personal Information 20
Table 3: Recent OMB Guidance on the Protection of Personally Identifiable Information 29
Table 4: Sample Descriptions from Five Agencies of a Standard Routine Use for Hiring or Retention of an Individual or the Issuance of a Security Clearance, Contract, Grant, or Other Benefit 38
Table 5: Privacy Act Provisions Agencies May Claim an Exemption under Subsection (k) 57
Table 6: Privacy Act Provisions from Which Agencies May Not Claim Exemptions 58

**Abbreviations**

| | |
|---|---|
| ADVISE | Analysis Dissemination Visualization Insight and Semantic Enhancement |
| CBP | Customs and Border Protection |
| CIPSEA | Confidential Information Protection and Statistical Efficiency Act |
| DHS | Department of Homeland Security |
| DOJ | Department of Justice |
| DOT | Department of Transportation |
| FBI | Federal Bureau of Investigation |
| FISMA | Federal Information Security Management Act |
| HHS | Department of Health and Human Services |
| HIPAA | Health Insurance Portability and Accountability Act of 1996 |
| IRS | Internal Revenue Service |
| ISPAB | Information Security and Privacy Advisory Board |
| NAS | National Academy of Sciences |
| NIST | National Institute of Standards and Technology |
| NRC | National Research Council |
| OCED | Organization for Economic Cooperation and Development |
| OMB | Office of Management and Budget |
| PIA | privacy impact assessment |
| PPSC | Privacy Protection Study Commission |
| PRA | Paperwork Reduction Act |
| SSA | Social Security Administration |
| TSA | Transportation Security Administration |

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.

**United States Government Accountability Office**
**Washington, DC 20548**

May 19, 2008

Congressional Requesters

The increasingly sophisticated ways in which personally identifiable information[1] is obtained and used by the federal government has the potential to assist in performing critical functions, such as preventing terrorism, but also can pose challenges in ensuring the protection of citizens' privacy. In this regard, concerns have been raised that the framework of legal mechanisms for protecting personal privacy that has been developed over the years may no longer be sufficient, given current practices.

Federal agency use of personal information is governed primarily by the Privacy Act of 1974 and the E-Government Act of 2002.[2] The Privacy Act of 1974 serves as the major mechanism for controlling the collection, use, and disclosure of personally identifiable information within the federal government. The act provides safeguards for information in a system of records (any grouping of records containing personal information retrieved by individual identifier) maintained by a federal agency. The act also allows citizens to learn how their personal information is collected, maintained, used, and disseminated by the federal government. As a result of the act's requirements, the public has benefited from privacy protections applied to countless government systems of records.

The E-Government Act of 2002 strives to enhance protection of personal information in government information systems by requiring that agencies

[1]For purposes of this report, the terms *personal information* and *personally identifiable information* are used interchangeably to refer to any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

[2]In addition, the Paperwork Reduction Act, enacted in 1980 and significantly revised in 1995, also has provisions affecting privacy protection in that it sets requirements for limiting the collection of information from individuals, including personal information. While the act's requirements are aimed at reducing the paperwork burden on individuals rather than specifically protecting personally identifiable information, the act nevertheless serves an important role in protecting privacy by setting these controls.

conduct privacy impact assessments (PIA).[3] This provision has led to the preparation of many PIAs that provide in-depth discussions of protections for personally identifiable information maintained in automated systems.

The Office of Management and Budget (OMB) is charged with ensuring implementation of the PIA requirement and the Privacy Act by federal agencies and is also responsible for providing guidance to agencies. In 1975, OMB issued Privacy Act Implementation Guidelines. Since that time, it has provided periodic supplemental guidance related to privacy on specific subjects.

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, now widely accepted, include:

- collection limitation,
- data quality,
- purpose specification,
- use limitation,
- security safeguards,
- openness,
- individual participation, and
- accountability.[5]

[3]A privacy impact assessment is an analysis of how personal information is collected, stored, shared, and managed in an information system

[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).

[5]These principles are described in table 1.

These principles, with some variation, are used by organizations to address privacy considerations in their business practices and are also the basis of privacy laws and related policies in many countries, including the United States, Germany, Sweden, Australia, and New Zealand, as well as the European Union.

Since enactment of the Privacy Act nearly 35 years ago, both the techniques employed by the federal government to obtain and process personally identifiable information and the technology used to support its collection, maintenance, dissemination, and use have changed dramatically. Advances in information technology have enabled agencies to more easily acquire, analyze, and share personally identifiable information from a variety of sources in increasingly diverse ways and for increasingly sophisticated purposes.

Given the advances in technology used to process, store, share, and manipulate personal information, you asked us to identify major issues regarding whether the Privacy Act of 1974, the E-Government Act of 2002, and related guidance consistently cover the federal government's collection and use of personal information and incorporate key privacy principles. Our objective was not focused on evaluating compliance with these laws; rather, it was to identify major issues concerning their sufficiency in light of current uses of personal information by the federal government. You also asked us to identify options for addressing these issues.

To address our objective, we analyzed the Privacy Act of 1974, section 208 of the E-Government Act, and related guidance to identify any inconsistencies or gaps in the coverage of these laws as they apply to uses of personal information by federal agencies. We also compared these laws and related guidance with the fair information practices to identify any significant gaps, including assessing the role of the Paperwork Reduction Act (PRA) in protecting privacy by limiting collection of information. We obtained an operational perspective on the sufficiency of these laws from six departments and agencies with large inventories of information collections, prominent privacy issues, and varied missions: the Departments of Health and Human Services (HHS), Homeland Security (DHS), Justice (DOJ), and Transportation (DOT); the Internal Revenue Service (IRS); and the Social Security Administration (SSA). We also obtained expert perspective on key issues through use of an expert panel, convened for us by the National Academy of Sciences (NAS). A full description of our objective, scope, and methodology can be found in

appendix I. In addition, the names of privacy experts participating in the NAS expert forum can be found in appendix II.

We conducted this performance audit from March 2007 to May 2008 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

## Results in Brief

Although the Privacy Act, the E-Government Act, and related OMB guidance set minimum requirements for agencies, they may not consistently protect personally identifiable information in all circumstances of its collection and use throughout the federal government and may not fully adhere to key privacy principles. Based on discussions with privacy experts, agency officials, and analysis of laws and related guidance, we identified issues in three major areas:

*Applying privacy protections consistently to all federal collection and use of personal information.* The Privacy Act's definition of a "system of records" (any grouping of records containing personal information retrieved by individual identifier), which sets the scope of the act's protections, does not always apply whenever personal information is obtained and processed by federal agencies. For example, if agencies do not retrieve personal information by identifier, the act's protections do not apply. Our 2003 report concerning compliance with the Privacy Act found that among the agencies surveyed, the most frequently cited reason for systems not being considered Privacy Act systems of records was that the agency did not use a personal identifier to retrieve the information.[6] Further, recent OMB guidance reflects an acknowledgement that, although personally identifiable information does not always reside in Privacy Act systems of records, it should nevertheless be protected. In addition, as we previously reported,[7] federal agencies have not always implemented Privacy Act requirements because they did not clearly apply to their use of

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

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

personal information from information resellers. Factors such as these have led experts to agree that the Privacy Act's system-of-records construct is too narrowly defined. The E-Government Act's privacy provisions, in contrast, apply more broadly; however, the E-Government Act does not include the specific constraints on how information is to be collected, maintained, and shared that are included in the Privacy Act nor does it address federal rulemaking, in which federal agencies can influence how other entities, including state and local government agencies, collect and use personal information. Alternatives for addressing these issues could include revising the system-of-records definition to cover all personally identifiable information collected, used, and maintained systematically by the federal government, and revising the E-Government Act's scope to cover federal rulemaking.

*Ensuring that collection and use of personally identifiable information is limited to a stated purpose.* According to the purpose specification, collection limitation, and use limitation principles, the collection of personal information should be limited, and its use should be limited to a specified purpose. Yet, current laws and guidance impose only modest requirements for describing the purposes for collecting and using personal information and limiting how that information is collected and used. For example, agencies are not required to be specific in formulating purpose descriptions in their public notices. While purpose statements for certain law enforcement and anti-terrorism systems might need to be phrased broadly enough so as not to reveal investigative techniques or the details of ongoing cases, overly broadly defined purposes could allow for unnecessarily broad collections of information and ranges of subsequent uses, thus calling into question whether meaningful limitations had been imposed.

Laws and guidance also may not effectively limit the collection of personal information. For example, the Privacy Act's requirement that information be "relevant and necessary" gives broad latitude to agencies in determining the amount of information to collect. Under these criteria, agency officials do not have specific requirements for justifying how much information to collect. Without establishing more specific requirements for justifying information collections, it may difficult to ensure that agencies limit collection of personal information to what is relevant and necessary.

In addition, mechanisms to limit use to a specified purpose may be weak. For example, the Privacy Act does not limit agency internal use of information, as long as it is needed for an official purpose. Recognizing that information sharing is critically important to certain government

functions such as homeland security and anti-terrorism, it has also been established that protecting privacy in these functions is an equally important goal. However, the Privacy Act does not include provisions addressing external sharing with other entities to ensure that the information's new custodians preserve the act's protections.

Examples of alternatives for addressing these issues include setting specific limits on routine uses and use of information within agencies to include more specific limits, requiring agencies to limit collection of personally identifiable information and to explain how such collection has been limited in privacy notices, and requiring agencies to establish formal agreements with external governmental entities before sharing personally identifiable information with them.

*Establishing effective mechanisms for informing the public about privacy protections.* According to the openness principle, the public should be informed about privacy polices and practices, and the accountability principle calls for those who control the collection or use of personal information to be held accountable for taking steps to ensure privacy protection. Public notices are a primary means of establishing accountability for privacy protections and giving individuals a measure of control over the use of their personal information. Yet concerns have been raised that Privacy Act notices may not serve this function well. Although the *Federal Register* is the government's official vehicle for issuing public notices, critics have questioned whether system-of-records notices published in the *Federal Register* effectively inform the public about government uses of personal information. Among others, options for addressing concerns about public notice could include setting requirements to ensure that purpose, collection limitations, and use limitations are better addressed in the content of privacy notices, and revising the Privacy Act to require that all notices be published on a standard Web site, such as www.privacy.gov.

Some of these issues—particularly those dealing with limitations on collection and use as well as mechanisms for informing the public—could be addressed by OMB through revisions or supplements to guidance. However, unilateral actions by OMB would not have the benefit of public deliberations regarding how best to achieve an appropriate balance between the government's need to collect, process, and share personally identifiable information and the rights of individuals to know about such collections and be assured that they are only for limited purposes and uses. In assessing such a balance, Congress should consider amending

applicable laws, such as the Privacy Act and the E-Government Act, according to the alternatives outlined in this report, including

- revising the scope of the laws to cover all personally identifiable information collected, used, and maintained by the federal government;
- setting requirements to ensure that the collection and use of personally identifiable information is limited to a stated purpose; and
- establishing additional mechanisms for informing the public about privacy protections by revising requirements for the structure and publication of public notices.

We received written comments on a draft of this report from the Deputy Administrator of the Office of E-Government and Information Technology and the Deputy Administrator of the Office of Information and Regulatory Affairs of OMB. The letter is reprinted in appendix V. In their comments, the officials noted that they shared our concerns about privacy and stated they believe it would be important for Congress to consider potential amendments to the Privacy Act and the E-Government Act in the broader context of the several privacy statutes that Congress has enacted.

Though we did not make specific recommendations to OMB, the agency provided comments on the alternatives identified in conjunction with our matter for congressional consideration. Regarding alternatives for revising the scope of laws to cover all personally identifiable information collected, used, and maintained by the federal government, OMB stated that it would be important for Congress to evaluate fully the potential implications of revisions such as amending the Privacy Act's system-of-records definition. We agree with OMB that such consideration should be thorough and include further public debate.

Regarding alternatives for setting requirements to ensure that the collection and use of personally identifiable information is limited to a stated purpose, OMB stated that agencies are working to implement a requirement in a recent OMB memorandum to review and reduce the volume of personally identifiable information they handle "to the minimum necessary." The draft report notes that this requirement is in place; however, because significant concerns have been raised in this area by our previous work and by experts at our forum, we believe Congress should consider additional alternatives for ensuring that the collection and use of personally identifiable information is limited to a stated purpose.

Finally, regarding effective mechanisms for informing the public, OMB stated that it supports ensuring that the public is appropriately informed of how agencies are using their information. OMB stated that they will review agency practices in informing the public and review the alternatives outlined in our report.

OMB provided additional technical comments, which are addressed in appendix V. We also received technical comments from DHS, DOJ, DOT, and IRS. We have addressed these comments in the final report as appropriate.

## Background

In response to growing concern about the harmful consequences that computerized data systems could have on the privacy of personal information, the Secretary of Health, Education, and Welfare commissioned an advisory committee in 1972 to examine to what extent limitations should be placed on the application of computer technology to record keeping about people. The committee's final report[8] proposed a set of principles for protecting the privacy and security of personal information, known as the Fair Information Practices. These practices were intended to address what the committee termed a poor level of protection afforded to privacy under existing law, and they underlie the major provisions of the Privacy Act, which was enacted the following year. A revised version of the Fair Information Practices, developed by the Organization for Economic Cooperation and Development (OECD) in 1980, has been widely adopted.[9] This version of the principles was reaffirmed by OECD ministers in a 1998 declaration and further endorsed in a 2006 OECD report.[10] The OECD version of the principles is shown table 1.

[8]Department of Health, Education & Welfare, *Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (Washington, D.C.: 1973).

[9]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.

[10]OECD, *Making Privacy Notices Simple: An OECD Report and Recommendations* (July 24, 2006).

**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. |
| 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.

The Fair Information Practices are, with some variation, the basis of privacy laws and related policies in many countries, including the United States, Germany, Sweden, Australia, and New Zealand, as well as the European Union.[11] They are also reflected in a variety of federal agency policy statements, beginning with an endorsement of the OECD principles by the Department of Commerce in 1981,[12] and including policy statements

[11]European Union Data Protection Directive ("Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data") (1995).

[12a]Report on OECD Guidelines Program, Memorandum from Bernard Wunder, Jr., Assistant Secretary for Communications and Information, Department of Commerce (Oct. 30, 1981).

from DHS, DOJ, and the Department of Housing and Urban Development.[13] In 2004, the Chief Information Officers Council issued a coordinating draft of its Security and Privacy Profile for the Federal Enterprise Architecture[14] that links privacy protection with a set of acceptable privacy principles corresponding to the OECD's version of the Fair Information Practices.

In addition, in a 2007 report on "Engaging Privacy and Information Technology in a Digital Age," the National Research Council found that the principles of fair information practice for the protection of personal information are as relevant today as they were in 1973.[15] Accordingly, the committee recommended that the fair information practices should be extended as far as reasonably feasible to apply to private-sector organizations that collect and use personal information.

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. Striking that balance varies among countries and among types of information (e.g., medical, employment information).

[13]Privacy Office Mission Statement, U.S. Department of Homeland Security, "Privacy Policy Development Guide," Global Information Sharing Initiative, U.S. Department of Justice, www.it.ojp.gov/global (September 2005); "Homeless Management Information Systems, U.S. Department of Housing and Urban Development (69 *Federal Register* 45888, July 30, 2004). See also "Options for Promoting Privacy on the National Information Infrastructure," Information Policy Committee of the National Information Infrastructure Task Force, Office of Information and Regulatory Affairs, Office of Management and Budget (April 1997).

[14]The Federal Enterprise Architecture is intended to provide a common frame of reference or taxonomy for agencies' individual enterprise architecture efforts and their planned and ongoing information technology investment activities. An enterprise architecture is a blueprint, defined largely by interrelated models, that describes (in both business and technology terms) an entity's "as is" or current environment, its "to be" or future environment, and its investment plan for transitioning from the current to the future environment.

[15]National Research Council of the National Academies, *Engaging Privacy and Information Technology in a Digital Age* (Washington, D.C.: 2007).

## Federal Laws and Guidance Govern Use of Personal Information in Federal Agencies

There is no single federal law that governs all use or disclosure of personal information. Instead, U.S. law includes a number of separate statutes that provide privacy protections for information used for specific purposes or maintained by specific entities. The major requirements for the protection of personal privacy by federal agencies come from two laws, the Privacy Act of 1974 and the privacy provisions of the E-Government Act of 2002.

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 through a system-of-records notice in the *Federal Register* that identifies, among other things, the categories of data collected, the categories of individuals about whom information is collected, the intended "routine" uses of data, and procedures that individuals can use to review and correct personally identifiable information.[16]

The act's requirements also apply to government contractors when agencies contract for the operation of a system of records to accomplish an agency function. According to OMB guidance, in these situations the contractual instrument between the agency and the contractor must specify that such records are to be maintained in accordance with the act. As explained by OMB, this requirement was not intended to cover private-sector record-keeping systems, but only those systems actually taking the place of a federal system that, but for the contract, would have been performed by an agency and covered by the Privacy Act.

Several provisions of the act require agencies to define and limit collection and use to 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 act also requires that an

[16]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).

agency inform individuals whom it asks to supply information of (1) the authority for soliciting the information and whether disclosure of such information is mandatory or voluntary; (2) the principal purposes for which the information is intended to be used; (3) the routine uses that may be made of the information; and (4) the effects on the individual, if any, of not providing the information. According to OMB, this requirement is based on the assumption that individuals should be provided with sufficient information about the request to make a decision about whether to respond.

In handling collected information, agencies are generally required by the Privacy Act to, among other things, allow individuals to (1) review their records (meaning any information pertaining to them that is contained in the system of records), (2) request a copy of their record or information from the system of records, and (3) request corrections to their information.

Agencies are allowed to claim exemptions from some of the provisions of the Privacy Act if the records are used for certain purposes. For example, records compiled by criminal law enforcement agencies for criminal law enforcement purposes can be exempt from a number of provisions, including (1) the requirement to notify individuals of the purposes and uses of the information at the time of collection and (2) the requirement to ensure the accuracy, relevance, timeliness, and completeness of records. A broader category of investigative records compiled for criminal or civil law enforcement purposes can also be exempted from a somewhat smaller number of Privacy Act provisions, including the requirement to provide individuals with access to their records and to inform the public of the categories of sources of records. In general, the exemptions for law enforcement purposes are intended to prevent the disclosure of information collected as part of an ongoing investigation that could impair the investigation or allow those under investigation to change their behavior or take other actions to escape prosecution. Statutory exemptions under the Privacy Act are summarized in appendix III.

In 1988, Congress passed the Computer Matching and Privacy Protection Act as an amendment to the Privacy Act, to establish procedural safeguards that affect agencies' use of Privacy Act records from benefit programs in performing certain types of computerized matching programs. For example, the 1988 act requires agencies to create written agreements specifying the terms under which matches are to be done.

More recently, in 2002, Congress enacted the E-Government Act to, among other things, enhance protection for personal information in government information systems or information collections by requiring that agencies conduct PIAs. A PIA is an analysis of how personal information is collected, stored, shared, and managed in a federal system. More specifically, according to OMB guidance,[17] a PIA is an analysis of how

> ...information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to 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 identifiable form or (2) before initiating any new data collections of information in an identifiable form that will be collected, maintained, or disseminated using information technology if the same questions are asked of 10 or more people. OMB guidance also requires agencies to conduct PIAs when a system change creates new privacy risks, for example, changing the way in which personal information is being used. According to OMB, no assessment is required when the information relates to internal government operations, the information has been previously assessed under an evaluation similar to a PIA, or when privacy issues are unchanged.

The PRA applies to federal information collections and was designed to help ensure that when the government asks the public for information, the burden of providing this information is as small as possible and the information itself is used effectively.[18] Such collections may have a range of purposes, which may or may not involve the collection of personal information, including applications for government benefits, program evaluation, general purpose statistics, research and regulation or compliance; all of these information collections may occur in a variety of forms, including questionnaires and telephone surveys. To achieve the

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

[18]The Paperwork Reduction Act was originally enacted into law in 1980 (Pub. L. No. 96-511, Dec. 11, 1980). It was reauthorized with minor amendments in 1986 (Pub. L. No. 99-591, Oct. 30, 1986) and was reauthorized a second time with more significant amendments in 1995 (Pub. L. No. 104-13, May 22, 1995).

goal of minimizing paperwork burden while maximizing the public benefit and utility of the information collected, the act includes provisions that establish standards and procedures for effective implementation and oversight of information collections. Among these provisions is the requirement that agencies not establish information collections without having them approved by OMB, and that before submitting them for approval, agencies' chief information officers certify that the collections meet 10 specified standards, including that the collection is necessary for the proper performance of agency functions and avoids unnecessary duplication. The law also requires agencies both to publish notices in the *Federal Register* and to otherwise consult with the public about their planned collections.

Privacy is also addressed in the legal framework for the emerging information sharing environment. As directed by the Intelligence Reform and Terrorism Prevention Act of 2004,[19] the administration has taken steps, beginning in 2005, to establish an information sharing environment to facilitate the sharing of terrorism-related information with protections for privacy and civil liberties. The move was driven by the recognition that before the attacks of September 11, 2001, federal agencies had been unable to effectively share information about suspected terrorists and their activities. In addressing this problem, the National Commission on Terrorist Attacks Upon the United States (9/11 Commission) recommended that the sharing and uses of information be guided by a set of practical policy guidelines that would simultaneously empower and constrain officials, closely circumscribing what types of information they would be permitted to share as well as the types of information they would need to protect. Exchanging terrorism-related information continues to be a significant challenge for federal, state, and local governments—one that we recognize is not easily addressed. Accordingly, since January 2005, we have designated information sharing for homeland security a high-risk area.[20]

[19]Pub. L. No. 108-458 (Dec. 17, 2004).

[20]For more information, see *GAO, High-Risk Series: An Update*, GAO-07-310 (Washington, D.C.: January 2007), p.47, and *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information*, GAO-06-385 (Washington, D.C.: Mar. 17, 2006).

## OMB Has Primary Responsibility for Oversight of the Privacy, E-Government, and Paperwork Reduction Acts

The Privacy Act gives OMB responsibility for developing guidelines and providing "continuing assistance to and oversight of" agencies' implementation of the Privacy Act. The E-Government Act of 2002 also assigns OMB responsibility for developing PIA guidance and ensuring agency implementation of the privacy impact assessment requirement. In July 1975, OMB published guidance for implementing the provisions of the Privacy Act. Since then, OMB has periodically issued additional guidance. For example, in 1991, OMB provided guidance to assist agencies in complying with the Computer Matching and Privacy Protection Act. In September 2003, consistent with its responsibility under section 208 of the E-Government Act, OMB issued guidance to agencies on conducting privacy impact assessments.

Enacted in 1980, the PRA made virtually all federal agency information collection activities subject to OMB review and established broad objectives for OMB oversight of the management of federal information resources. The act established the Office of Information and Regulatory Affairs within OMB and gave this office a variety of oversight responsibilities over federal information functions, including general information policy, reduction of paperwork burden, and information privacy. To assist agencies in fulfilling their responsibilities under the act, OMB took various steps. It issued a regulation[21] and provided agencies with instructions on filling out a standard form for submissions and providing supporting statements.

OMB has also periodically issued guidance on other privacy-related issues, including

- federal agency Web site privacy policies;
- interagency sharing of personal information;
- designation of senior staff responsible for privacy; and
- data breach notification.

A list of privacy guidance from OMB can be found in appendix IV.

[21] 5 C.F.R. Part 1320.

## Previous Studies Have Raised Concerns about the Sufficiency of Privacy Laws

Concerns about the Privacy Act have arisen periodically since its passage. The Privacy Act established a temporary national study commission to conduct a comprehensive assessment of privacy policy and to make recommendations for better protecting the privacy of individuals. This commission, called the Privacy Protection Study Commission (PPSC), was to study privacy issues and recommend future legislation.

In its final report,[22] the PPSC concluded that, as transactions involving personal information have proliferated, there has been no compensating tendency to give the individual the kind of control over the collection, use, and disclosure of personal information that natural, or face-to-face, encounters normally entail. The PPSC found that if informational privacy is to be protected, public policy must focus on certain systemic features such as the proliferating use of information for a different purpose than for what it was originally collected, and the greater use of third-party reporting.

The commission concluded that it would be beneficial to create a federal body to oversee, regulate, and enforce compliance with the commission's recommendations. The PPSC formally recommended that the President and Congress create an independent entity to participate in any federal proceeding that would affect personal privacy, including the issuance of rules that must be followed by federal agencies in interpreting the Privacy Act.

As another example, in a 1983 report summarizing 9 years (1975 to1983) of congressional oversight of the Privacy Act, the House Committee on Government Operations concluded that OMB had not pursued its responsibility to revise and update its original guidance from 1975 and had not actively monitored agency compliance with its guidance. It stated "Interest in the Privacy Act at [OMB] has diminished steadily since 1975. Each successive Administration has shown less concern about Privacy Act oversight."[23]

[22]Privacy Protection Study Commission, *Personal Privacy in an Information Society* (Washington, D.C.: July 1977).

[23]U.S. Congress, House of Representatives, *Who Cares About Privacy? Oversight of the Privacy Act of 1974 by the Office of Management and Budget and by the Congress*, House Report No. 98-455 (Washington, D.C.:1983).

More recently, in 2002, the Information Security and Privacy Advisory Board (ISPAB), a federal advisory committee originally established by the Computer Security Act of 1987,[24] issued a report on government privacy policy setting and management. In its report, the ISPAB raised a number of concerns about advances in technology and its impact on privacy. Specifically, ISPAB observed that "with the migration toward e-government services, greater demands will be placed on the government's privacy policies and systems." ISPAB further observed that the public's willingness to use such services will depend "in large measure on their confidence that the information that they disclose will be safeguarded."[25]

The ISPAB report further stated that, "changes in technology, the privacy management challenges stemming from expanded e-government services, the accelerated interaction of networked information systems within and across critical infrastructure boundaries, and the extended, routine exchange of data among Federal and non-Federal government and non-government systems - all mandate immediate and serious attention to Federal government's data privacy policies and operational controls." Among the issues identified was a need for a review of the sufficiency and relevance of the Privacy Act to determine whether modifications were required, given the numerous changes affecting privacy that had occurred since the act was passed.

Following up on its 2002 report, in 2005 ISPAB issued a "Privacy Act White Paper" raising the question of whether the existing legal and policy framework governing the information practices of federal agencies was sufficient to protect the privacy of individuals about whom the federal government maintained or used personal information. The paper postulated that "laws and policies have not kept pace with changes in technology and information and handling processes and suggests the need for an open dialogue on what changes in law and policy are needed and how to best make those changes." Accordingly, in 2006 ISPAB initiated a

[24]The Information Security and Privacy Advisory Board's duties include identifying emerging managerial, technical, administrative, and physical safeguard issues relative to information security and privacy; and advising the National Institute of Standards and Technology (NIST), the Secretary of Commerce, and the Director of the OMB on information security and privacy issues pertaining to federal government information systems. Until December 2002, the ISPAB was named the Computer System Security and Privacy Advisory Board.

[25]Computer System Security and Privacy Advisory Board, *Findings and Recommendations on Government Privacy Policy Setting and Management* (September 2002).

partnership with the DHS Data Privacy and Integrity Advisory Committee[26] to develop recommendations on a 21st century framework for revisions to the Privacy Act and other federal privacy statutes. Work on this initiative was ongoing at the time of our review.

In 2007, the National Research Council[27] issued a report entitled *Engaging Privacy and Information Technology in a Digital Age*.[28] The report identified a number of issues related to the implications of advances in technology on privacy. With regard to government use of personal information, the committee found that the government has important roles to play in protecting the privacy of individuals and groups and in ensuring that decisions concerning privacy are made in an informed fashion. However, the report characterized the U.S. legal and regulatory framework as "a patchwork that lacks consistent principles or unifying themes." The committee concluded that a less decentralized and more integrated approach to privacy policy in the United States could bring a greater degree of coherence to the subject of privacy. The committee recommended that the U.S. government undertake a broad systematic review of national privacy laws and regulations.

Further, with regard specifically to government use of personal information, the committee found that "because the benefits of privacy often are less tangible and immediate than the perceived benefits of other interests, such as public security and economic efficiency, privacy is at an inherent disadvantage when decision makers weigh privacy against these other interests." The committee concluded that, to reduce this inherent disadvantage, governments at federal, state, and local levels should establish mechanisms for the institutional advocacy of privacy within

[26]The DHS Data Privacy and Integrity Advisory Committee is a federal advisory committee that advises the Secretary of DHS and the DHS Chief Privacy Officer on programmatic, policy, operational, administrative, and technological issues within DHS that affect individual privacy, as well as data integrity and data interoperability and other privacy related issues.

[27]The National Research Council (NRC) functions under the auspices of the National Academy of Sciences (NAS), the National Academy of Engineering, and the Institute of Medicine. The mission of the NRC is to improve government decision making and public policy, increase public education and understanding, and promote the acquisition and dissemination of knowledge in matters involving science, engineering, technology, and health.

[28]National Research Council of the National Academies, *Engaging Privacy and Information Technology in a Digital Age* (Washington, D.C.: 2007).

government. Much as the PPSC had recommended in 1977, the NRC recommended that a national privacy commissioner or standing privacy commission be established to provide ongoing and periodic assessments of privacy developments.

We have previously reported on a number of agency-specific and governmentwide privacy-related issues at federal agencies. For example, in 2003,[29] we reported that agencies generally did well with certain aspects of the Privacy Act's requirements—such as issuing systems-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. We have also reported on key privacy challenges facing federal agencies, federal Web site privacy, notification of individuals in the event of a data breach, and government data-mining initiatives. A list of our privacy-related products can be found in appendix V.

## Additional Laws Provide Protections for Federal Agency Use of Personal Information

Other federal laws address privacy protection for personal information with respect to information security requirements as well as for certain types of information, such as when taxpayer, statistical, or health information is involved.

The Federal Information Security Management Act (FISMA) addresses the protection of personal information by defining 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.[30] 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

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

[30]FISMA, Title III, E-Government Act of 2002, Pub. L. No. 107-347 (Dec. 17, 2002).

restrictions on access and disclosure to protect personal privacy, among other things.[31]

Other laws address protection of personal information by federal agencies in specific circumstances and are described in table 2.

**Table 2: Major Federal Laws That Address Federal Agency Use of Personal Information**

| Information covered | Applicable law |
|---|---|
| Patient health information | To the extent a federal agency is a covered entity under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), e.g., a provider of health care programs or services, it may not use or disclose an individual's health information without the individual's authorization, except for certain reasons, and is required to inform individuals of its privacy practices. 42 U.S.C. §§ 1320d – d-7; 45 C.F.R. Part 164. |
| Statistical information | The Confidential Information Protection and Statistical Efficiency Act (CIPSEA) requires that information acquired by an agency under a pledge of confidentiality and for exclusively statistical purposes shall be used by the agency only for such purposes and shall not be disclosed in identifiable form for any other use, except with the informed consent of the respondent. Sec. 512, Title V, Pub. L. No. 107-347, Dec. 17, 2002; 44 U.S.C. § 3501 note. |
| Census data | Except as specifically authorized by law, the Census Bureau may not disclose identifiable census data. Penalties of up to $5,000 and 5 years in prison apply for violating the law. 13 U.S.C. §§ 9 & 214. |
| Taxpayer data | The IRS must keep taxpayer information confidential and may only disclose it under limited circumstances, e.g., for federal or state tax administration, to assist in the enforcement of child support programs, to verify eligibility for public assistance programs, and for use in a criminal investigation. Individuals or agencies receiving taxpayer data must, as a condition of receiving such data, have safeguards for the protection of, and for accounting for, the use of such data. 26 U.S.C. § 6103. |
| Social Security information | Social Security numbers and related records must be treated as confidential and may not be disclosed, except as authorized. 42 U.S.C. §§ 405 & 1306. Such other authorized uses include disclosures for bankruptcy proceedings (11 U.S.C. 342(c)), enforcement of child support programs (42 U.S.C. §§ 653, 653a, & 666(a)(13)), and enforcement of immigration laws (8 U.S.C. §§ 1304 & 1360). |

Source: GAO analysis.

[31] Although we did not assess the effectiveness of information security or compliance with FISMA at any agency as part of this review, we have previously reported on weaknesses in almost all areas of information security controls at 24 major agencies. For additional information see, GAO, *Information Security: Progress Reported, but Weaknesses at Federal Agencies Persist*, GAO-08-571 (Washington, D.C.: Mar. 12, 2008); *Information Security: Despite Reported Progress, Federal Agencies Need to Address Persistent Weaknesses*, GAO-07-837 (Washington, D.C.: July 27, 2007); and *Information Security: Weaknesses Persist at Federal Agencies Despite Progress Made in Implementing Related Statutory Requirements*, GAO-05-552 (Washington, D.C.: July 15, 2005).

## The Privacy Act and E-Government Act Do Not Always Provide Protections for Federal Uses of Personal Information

The Privacy Act's controls on the collection, use, and disclosure of personally identifiable information do not consistently protect such information in all circumstances of its collection and use throughout the federal government. Issues have largely centered on the Privacy Act's definition of a "system of records" (any grouping of records containing personal information retrieved by individual identifier), which triggers the act's protections. Personal information is not always obtained and processed by federal agencies in ways that conform to the definition of a system of records, and in cases where such information falls outside this definition, it may not receive the full privacy protections established by the act. In contrast, the E-Government Act of 2002 sets broader terms for its requirement to conduct PIAs—namely, (1) before an agency develops or procures information technology that collects, maintains, or disseminates information that is in identifiable form, or (2) before an agency collects information in identifiable form using information technology. Although the E-Government Act's broader definition is more inclusive than the system-of-records concept, its requirements are more limited because it imposes no restrictions on agency collection and use of personally identifiable information. Alternatives for addressing these issues could include revising the system-of-records definition to cover all personally identifiable information collected, used, and maintained systematically by the federal government, and revising the E-Government Act's scope to cover federal rulemaking.

### Key Terms in the Privacy Act May Be Defined Too Narrowly

The Privacy Act's controls on the collection, use, and disclosure of personally identifiable information only apply when such information is covered by the act's key terms, especially the "system-of-records" construct. There are several different ways in which federal collection and use of personally identifiable information could be outside of such a construct and thus not receive the Privacy Act's protections:

- *Personally identifiable information held by the government is not always retrieved by identifier.* The Privacy Act defines a system of records as "a group of records[32] under the control of any agency from which information is retrieved by the name of the individual or by some

[32] A *record* is defined as "any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph."

identifying number, symbol, or other identifying particular assigned to the individual." If personally identifiable information (records) is not retrieved by identifier but instead accessed through some other method or criteria—for example, by searching for all individuals who have a certain medical condition or who applied for benefits on a certain date—the system would not meet the Privacy Act's system-of-records definition and therefore would not be governed by the act's protections. OMB's 1975 Privacy Act implementation guidance reflects an acknowledgement that agencies could potentially evade the act's requirements by organizing personal information in ways that may not be considered to be retrieved by identifier.[33]

This scope of the system-of-records definition has been an issue since the Privacy Act became law in 1974. In its 1977 report, the PPSC pointed out that retrieval by name or identifier reflected a manual rather than a computer-based model of information processing and did not take into account emerging computing technology. As the study explained, while manual record-keeping systems are likely to store and retrieve information by reference to a unique identifier, this is unnecessary in computer-based systems that permit attribute searches.[34] The PPSC noted that retrieval of individually identifiable information by scanning (or searching) large volumes of computer records was not only possible but an ever-increasing agency practice.

Our 2003 report concerning compliance with the Privacy Act found that the PPSC's observations had been borne out across federal agencies. A key characteristic of agencies' systems of records at the time was that a large proportion of them were electronic, reflecting the government's significant use of computers and the Internet to collect and share personal information. Based on survey responses from 25 agencies in 2002, we estimated that 70 percent of the agencies' systems of records contained electronic records and that 11 percent of information systems in use at those agencies contained personal information that was outside a Privacy

[33]According to OMB, "systems should not be subdivided or reorganized so that information which would otherwise have been subject to the act is no longer subject to the act. For example, if an agency maintains a series of records not arranged by name or personal identifier but uses a separate index file to retrieve records by name or personal identifier it should not treat these files as separate systems." 40 *Federal Register* 28963 (July 9, 1975).

[34]An attribute search, in contrast to the conventional "name search" or "index search," starts with a collection of data about many individuals and seeks to identify those particular individuals in the system who meet a set of prescribed conditions or who have a set of prescribed attributes or combination of attributes.

Act system of records. We also reported that among the agencies we surveyed, the most frequently cited reason for systems not being considered Privacy Act systems of records was that the agency did not use a personal identifier to retrieve the personal information.[35]

Recent OMB guidance reflects an acknowledgement that, although personally identifiable information does not always reside in Privacy Act systems of records, it should nevertheless be protected. Following a number of highly publicized data breaches at government agencies, OMB issued guidance instructing agencies to take action to safeguard "personally identifiable information." Beginning in May 2006, OMB required senior agency privacy officials to "conduct a review of policies and processes and take corrective action as appropriate to ensure adequate safeguards to prevent the intentional or negligent misuse of, or unauthorized access to personally identifiable information." Most recently, in May 2007, OMB required agencies to review and reduce "all current holding of personally identifiable information." This guidance is not limited to information that is "retrieved by identifier" or contained within systems of records.

- *The Privacy Act's protections may not apply to contemporary data processing technologies and applications.* In today's highly interconnected environment, information can be gathered from many different sources, analyzed, and redistributed in very dynamic, unstructured ways that may have little to do with the file-oriented concept of a Privacy Act system of records. For example, data mining, a prevalent technique used by federal agencies[36] for extracting useful information from large volumes of data, may escape the purview of the Privacy Act's protections. Specifically, a data-mining system that performs analysis by looking for patterns in personal information located in other systems of records or that performs subject-based queries across multiple data sources may not constitute a system of records under the act.

  In recent years, reports required by law on data mining have described activities that had not been identified as systems of records covered by the Privacy Act. In one example, DHS reported that all the data sources for the

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

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

planned Analysis Dissemination Visualization Insight and Semantic Enhancement (ADVISE) data mining program were covered by existing system-of-records notices; however, the system itself was not covered, and no system of records notice was created specifically to document protections under the Privacy Act governing the specific activities of the system.[37] ADVISE was a data-mining tool intended to allow an analyst to search for patterns in data—such as relationships among people, organizations, and events—and to produce visual representations of those patterns.

This was also the case with other data mining programs reported by DHS and DOJ.[38] For example, DHS reported on a data mining system known as Intelligence and Information Fusion—which provides intelligence analysts with an ability to view, query, and analyze multiple data sources from within the government—that is not considered a Privacy Act system of records. While DHS reported that the system was "covered" by the system-of-records notice for the Homeland Security Operations Center Database,[39] that notice does not specifically describe the uses of the Intelligence and Information Fusion system. Thus, while the underlying data sources are subject to the protections of the act, the uses of the Intelligence and Information Fusion system have not been specifically addressed.

Likewise, DOJ reported that its Foreign Terrorist Tracking Task Force[40] was developing a data mining system, known as the System to Assess Risk, to assist analysts in prioritizing persons of possible investigative interest in support of a specified terrorist threat. DOJ reported that the system's data

[37]The DHS Privacy Office determined that because the data mining applications did not involve retrieval by individual identifier, a separate system of records notice describing the data mining application was not required. DHS Privacy Office, *ADVISE Report: DHS Privacy Office Review of the Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement (ADVISE) Program* (Washington, D.C.: July 11, 2007).

[38]DHS Privacy Office, *2007 Report to Congress on the Impact of Data Mining Technologies on Privacy and Civil Liberties* (Washington, D.C.: July 6, 2007); Justice, *Report on "Data-Mining" Activities Pursuant to Section 126 of the USA PATRIOT Improvement and Reauthorization Act of 2005* (Washington, D.C.: July 9, 2007).

[39]Homeland Security Operations Center Database, 70 *Federal Register* 20156 (Apr. 18, 2005).

[40]The task force's mission is to assist federal law enforcement and intelligence agencies in locating foreign terrorists and their supporters who are in or have visited the United States, and to provide information to other law enforcement and intelligence community agencies that can lead to their surveillance, prosecution, or removal.

sources were covered by the system-of-records notice for the Federal Bureau of Investigation's (FBI) Central Records System.[41] However, the Central Records System notice does not specifically describe the uses of the System to Assess Risk and thus provides no evidence that the Privacy Act's protections are being applied to the system. The fact that these notices do not specifically describe data-mining systems that they are said to include reflects the limitations of the system-of-records construct as a way to identify, assess, and report on the protections being applied to these types of analytical uses. As a result, personally identifiable information collected and processed by such systems may be less well protected than if it were more specifically addressed by the Privacy Act.

- *Use of personal information from third party sources is not consistently covered by the Privacy Act.* The Privacy Act requires agencies to collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under federal programs. Yet agencies have increasingly turned to other sources to collect personal information, particularly third-party sources such as information resellers—companies that amass and sell personal information from many sources. Concerns were raised in our expert forum that government agencies may be using such third-party sources as a way to avoid the constraints of the Privacy Act.

  In our 2006 report on federal agency use of personal information from information resellers,[42] we noted that agency officials said they generally did not prepare system-of-records notices for the use of information resellers because they were not required to do so by the Privacy Act. The Privacy Act makes its provisions applicable to third-party systems when "an agency provides by a contract for the operation by or on behalf of the agency a system of records to accomplish an agency function." According to agency officials, information reseller databases were not considered systems of records operated "by or on behalf of a government agency" because resellers develop their databases for multiple customers, not the federal government exclusively. Further, agency officials stated that merely querying information reseller databases did not amount to maintaining the information that was obtained, and thus the provisions of the Privacy Act did not apply. In many cases, agency officials considered

[41] 63 *Federal Register* 8671 (Feb. 20, 1998).

[42] GAO-06-421.

their use of reseller data to be of this type—essentially "ad hoc" querying or "pinging" of databases for personal information about specific individuals, which they were not doing in connection with a designated system of records. Thus, these sources, which agencies use for many purposes, have not been considered subject to the provisions of the Privacy Act. As a result, individuals may be limited in their ability to learn that information is being collected about them, because the information is being obtained from other sources and the activity is not publicly described in a system-of-records notice. Further, the Privacy Act's constraints on collection, use, and disclosure would not apply.

In our 2006 report, we made recommendations to OMB to revise its guidance to clarify the applicability of requirements for public notices and privacy impact assessments with respect to agency use of personal information from resellers. We also recommended that OMB direct agencies to review their uses of such information to ensure it is explicitly referenced in privacy notices and assessments. However, OMB has not addressed our recommendations. OMB stated that following the completion of work on the protection of personal information through the Identity Theft Task Force, it would consider issuing appropriate guidance concerning reseller data. OMB issued guidance based on the work of the Identity Theft Task Force in May 2007; however, it did not include clarifying guidance concerning reseller data. Without clarifying guidance, agencies may continue to consider use of reseller data as not covered by the Privacy Act and thus may not apply the Privacy Act's protections to this use.

## The E-Government Act Applies More Broadly Than the Privacy Act but Lacks Explicit Constraints on Agency Actions

The E-Government Act's requirements for the conduct of PIAs apply to a broader range of government activities than are currently covered by the Privacy Act's definition of a system of records. Specifically, the E-Government Act requires agencies to conduct PIAs before (1) developing or procuring information technology that collects, maintains, or disseminates information that is in individually identifiable form or (2) initiating 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.

The PIA requirement has provided a mechanism for agencies to consider privacy protections during the earliest stages of development of their systems, when it may be relatively easy to make critical adjustments. Senior agency privacy officials at several agencies reported that their PIA processes are incorporated into key stages in systems development. For

example, senior agency privacy officials at the IRS reported that PIAs are required at every stage of the systems development life cycle for new systems or systems undergoing major modifications. In addition, five of the six agencies we interviewed reported that they use a privacy threshold analysis, a brief assessment that requires system owners to answer basic questions on the nature of their systems and whether the systems contain personally identifiable information, to identify systems that require a PIA; this approach enables agencies to ensure that systems undergo the PIA process at the earliest stages of development.

Privacy experts and senior agency privacy officials we interviewed also noted that the E-Government Act provides a mechanism to address certain uses of personal information that might not have been covered by the Privacy Act. According to OMB guidance, PIAs are required to be performed and updated whenever a system change creates new privacy risks. Among the types of changes identified in OMB guidance that might require conducting a PIA are when converting from paper to electronic records, when applying new technologies that significantly change how information in identifiable form is managed in the system, and when merging databases to create one central source of information. Typically, under the Privacy Act changes of this nature could result in limited modifications to a system-of-records notice to reflect additional categories of records and/or routine uses. It would not result in a reassessment of privacy risks, as is required for a PIA.

Because the E-Government Act's PIA requirement applies more broadly than the Privacy Act, it may help in part to address concerns about the narrow definition of terms in the Privacy Act. Specifically, a well-written PIA can inform the public about such things as what information is being collected, why it is being collected, and how it is to be used. However, the E-Government Act does not include the specific constraints on how information is to be collected, maintained, and shared that are included in the Privacy Act—such as restrictions on disclosure of personal information and requirements to allow for access to and correction of records by individuals, among other things. Further, the E-Government Act only applies to information technology systems and therefore does not address personal information contained in paper records.

In addition, the E-Government Act may not be broad enough to cover all cases in which the federal government makes determinations about what personal information is to be collected and how it is to be protected. A major function that is not covered is rulemaking that involves the collection of personally identifiable information. Rulemaking is the

process by which federal agencies establish regulations that can govern individual behavior as well as commercial and other activities. For example, DHS is required by the Homeland Security Act to conduct PIAs for all of its proposed rules,[43] and, as a result, PIAs have been conducted for major initiatives, including the REAL ID Act, which required DHS to establish minimum standards for state-issued drivers' licenses and identification cards that federal agencies would accept for official purposes, and the Western Hemisphere Travel Initiative, aimed at strengthening border security and facilitating entry into the United States for U.S. citizens and certain foreign visitors through a standardized identification card. These PIAs have provided for the evaluation of privacy considerations before final decisions are made concerning specific technologies to be used in drivers' licenses and border-crossing identification cards issued by state governments. However, DHS, DOT, Treasury, and a number of smaller agencies are currently the only agencies required to conduct PIAs on proposed rules. Other agencies may be issuing rules that have privacy implications without conducting privacy assessments of them.

## Alternatives for Broadening the Coverage of Privacy Laws

A number of alternatives exist to address the issues associated with the coverage of existing privacy laws governing federal use of personal information. These alternatives involve revisions to the Privacy Act and E-Government Act, as follows:

- *Revise the system of records definition to cover all personally identifiable information collected, used, and maintained by the federal government.* Like the Privacy Protection Study Commission, which believed in 1977 that the act's definition of a system of records should be revised, experts at our forum were in agreement that the system-of-records definition is outdated and flawed. The experts agreed that the act's protections should be applied whenever agencies obtain, process, store, or share personally identifiable information—not just when records are retrieved by personal identifier. Such an approach could address concerns that certain activities, such as data mining or retrieving information from commercial information resellers could avoid the protections of the act.

[43]Section 222(4) of the Homeland Security Act of 2002 requires the DHS Privacy Officer to conduct "a privacy impact assessment of proposed rules of the Department or that of the Department on the privacy of personal information, including the type of personal information collected and the number of people affected."

As shown in table 3, several recent OMB memoranda providing direction to federal agencies on privacy protection reflects this approach.

**Table 3: Recent OMB Guidance on the Protection of Personally Identifiable Information**

| Memorandum | Major requirement |
|---|---|
| OMB M-06-15:<br>Safeguarding Personally Identifiable Information | Requires the Senior Official for Privacy at each agency to conduct a review of agency policies and processes, and take corrective action as appropriate, to ensure adequate safeguards to prevent the intentional or negligent misuse of, or unauthorized access to, personally identifiable information. |
| OMB M-06-19:<br>Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments | Requires agencies to report all incidents involving personally identifiable information to the federal incident response center at DHS within 1 hour of discovering the incident. The guidance defines personally identifiable information as "any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual." |
| OMB M-07-16:<br>Safeguarding against and Responding to the Breach of Personally Identifiable Information | Requires agencies to develop a policy for handling breaches of personally identifiable information as well as policies concerning the responsibilities of individuals authorized to access such information. Agencies are urged to reduce the volume of collected and retained information to the minimum necessary, limit access to only those individuals who must have such access, and use encryption, strong authentication procedures, and other security controls to make information unusable by unauthorized individuals. |

Source: OMB.

The Privacy Act's narrowly scoped system-of-records definition does not match OMB's broadened approach to protecting personally identifiable information. Changing the system-of-records definition is an option that could help ensure that the act's protections are consistently applied to all personally identifiable information.

- *Revise the E-Government Act's scope to cover federal rulemaking.* The E-Government Act's privacy provisions could be broadened to apply to all federal rulemaking involving the collection of personally identifiable information, as the Homeland Security Act currently requires of DHS and the Transportation, Treasury, Independent Agencies and General Government Appropriations Act of 2005 requires of Transportation, Treasury, and certain other agencies. This change would ensure that privacy concerns are addressed as the federal government proposes and adopts rules that affect how other entities, including state and local government agencies, collect and use personally identifying information.

## Laws and Guidance May Not Effectively Limit Agency Collection and Use of Personal Information to Specific Purposes

Current laws and guidance impose only modest requirements for describing the purposes for collecting and using personal information and limiting how that information is collected and used. For example, agencies are not required to be specific in formulating purpose descriptions in their public notices. Laws and guidance also may not effectively limit the collection of personal information. For example, the Privacy Act's requirement that information be "relevant and necessary" gives broad latitude to agencies in determining the amount of information to collect. In addition, mechanisms to limit use to a specified purpose may be weak. For example, the Privacy Act does not limit agency internal use of information, as long as it is needed for an official purpose or include provisions addressing external sharing with other entities to ensure that the information's new custodians preserve the act's protections. Examples of alternatives for addressing these issues include setting specific limits on routine uses and use of information within agencies to include more specific limits, requiring agencies to justify how collection has been limited in privacy notices, and requiring agencies to establish formal agreements with external governmental entities before sharing personally identifiable information with them.

### Fair Information Practices Call for Purpose Specification and Limitations on Collection and Use of Personal Information

A key area of concern about personal information maintained by government agencies is to ensure that limits are placed on what the government acquires and how it uses the information—thus giving individuals a measure of control over their own personal information. Two of the fair information practices relate specifically to limiting the way the government collects and uses personal information: collection limitation and use limitation. A third principle—purpose specification—is critical to ensuring that the other two are applied effectively.

The purpose specification principle states that the purpose for the collection of personal information should be disclosed before the collection is made and upon any change to that purpose, and its use should be limited to that purpose and compatible purposes. Clearly specifying the purpose of a given activity establishes the measure for determining whether the collection of information has been sufficiently limited to what is relevant for the purpose and whether the ways in which the information is used have also been limited to what is appropriate for the same purpose.

The collection limitation principle states that 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. When the collection limitation principle is applied, individuals can gain assurance that the information about them that is being collected is only what is needed to perform a specific, predisclosed function. In the government arena, this mitigates the risk that an over-collection of personal information could facilitate the improper use of that information to make adverse determinations. For example, the Transportation Security Administration (TSA) received criticism about its now-cancelled Computer-Assisted Passenger Pre-screening System II because it proposed to collect information from third-party sources in addition to airline passengers themselves. Concerns were raised that individuals could be delayed or denied boarding their airline flights based on third-party information that was potentially inaccurate. In developing a successor project, called Secure Flight, TSA responded to privacy concerns by planning to collect far less information and to focus on information collected directly from individuals.[44]

A closely related principle—the use limitation principle—provides that personal information, once collected, should not be disclosed or used for other than a specified purpose without consent of the individual or legal authority. The use limitation principle is arguably of heightened importance in the government arena because the government has many functions that affect numerous aspects of an individual's well-being. Hence, it is important to ensure that information the government collects for one function is not used indiscriminately for other unrelated functions. By requiring the government to define a specific purpose for the collection of personal information and limit its use to that specified purpose, individuals gain assurance that their privacy will be protected and their information will not be used in ways that could jeopardize their rights or otherwise unfairly affect them.

## The Privacy Act Does Not Ensure That Purposes Are Always Stated and Are Specific

The Privacy Act includes requirements that agencies (1) inform individuals from whom information is being collected of the principal purpose or purposes for which the information is intended to be used and (2) publish a system-of-records notice in the *Federal Register* of the existence and character of the system of records, including planned routine uses of the records and the purpose of each of these routine uses. Concerns have been raised that the act's requirements do not go far enough in ensuring that the government's planned purposes are sufficiently specified:

[44]TSA's current plans for Secure Flight do not include the use of reseller information.

- *Statements of overall purpose are not always required.* The Privacy Act requires agencies to inform individuals on forms used to collect information from them of the principal purpose or purposes for which the information is intended to be used. This is an important provision that protects individuals when the government is collecting information directly from them. However, in many cases, agencies obtain information about individuals from other sources, such as commercial entities (including information resellers) and other governmental entities. In those cases, no overall declaration of purpose is required in the system-of-records notice. For each of the stated routine uses a description is required of the potential purposes for which the records may be used; however, there is no requirement for a declaration of the purpose or purposes for the system of records as a whole. Given that individuals may be especially concerned about how their information is collected from different government and commercial entities, not having an overall purpose associated with this information raises concerns.

- *Purpose descriptions in public notices are not required to be specific.* As mentioned above, while there is no requirement for an overall statement of purpose, Privacy Act notices may contain multiple descriptions of purposes associated with routine uses, and agencies are not required to be specific in formulating these purposes. OMB guidance on the act gives agencies discretion to determine how to define the range of appropriate uses and associated purposes that it intends for a given system of records. For example, purpose statements for certain law enforcement and anti-terrorism systems might need to be phrased broadly enough so as not to reveal investigative techniques or the details of ongoing cases. However, overly broadly-defined purposes could allow for unnecessarily broad collections of information and ranges of subsequent uses, thus calling into question whether meaningful limitations had been imposed.
  For example, in previous work on international passenger prescreening by DHS's Customs and Border Protection (CBP),[45] we reported that CBP's public notices and reports regarding its international prescreening process did not fully or accurately describe CBP's use of personal data throughout the passenger prescreening process. In that case, CBP relied on a system-of-records notice for the Treasury Enforcement Communications System—one of several data sources used in the prescreening process—to notify the public about the purpose of the international prescreening program. The notice, however, did not mention CBP's passenger

[45]GAO, *Aviation Security: Efforts to Strengthen International Passenger Prescreening Security Are Under Way, but Planning and Implementation Issues Remain*, GAO-07-346 (Washington, D.C.: May 16, 2007).

prescreening purpose but simply included a broad statement about its law enforcement purpose, namely that "every possible type of information from a variety of Federal, state and local sources, which contributes to effective law enforcement may be maintained in this system of records."[46] Use of such a sweeping purpose statement obscured its use in international passenger prescreening and did not establish a basis for limiting use of the information in the system. Its use shows that the act does not require the government to clearly state its purposes for collecting and using personal information.

Another example can be found in the system-of-records notice for the FBI's Central Records System. The FBI relies on this notice to inform the public about a broad range of files it maintains and uses for a variety of different purposes. According to the notice, the Central Records System contains investigative, personnel, applicant, administrative, and "general" files.[47] In addition to information within 281 different categories of legal violations over which the FBI has investigative jurisdiction, the files also include information pertaining to personnel, applicant, and administrative matters. As a result, it is unclear from the notice how any given record in this system is to be used. While law enforcement agencies are often concerned about revealing their methods to criminals, descriptions of the specific purposes of FBI systems could be crafted to avoid revealing what information had been collected about any specific individual or how it was being used by the agency. DOJ officials acknowledged that there has been frequent criticism of the broad scope of the Central Records System notice but said the notice had been structured that way because all the records covered by the notice are organized according to that same indexing hierarchy. More significantly, the Privacy Act does not require that systems of records be defined and described more specifically. Like the CBP notice, the FBI notice demonstrates that the act does not require the government to clearly state its purposes for collecting and using personal information.

[46]66 *Federal Register* 53029 (Oct. 18, 2001).

[47]63 *Federal Register* 8671 (Feb. 20, 1998).

## Laws and Guidance May Not Effectively Limit Collection of Personal Information

Regarding collection limitation, the Privacy Act states that each agency should maintain only such information about individuals in its systems of records that is "relevant and necessary" to accomplish a purpose the agency is required to accomplish by statute or executive order of the President. The act further states that agencies generally cannot disclose records about an individual without his or her consent, except under a number of specific conditions.[48]

Collection limitation may also be addressed indirectly as part of agency procedures under the E-Government Act for conducting PIAs. Based on OMB guidance, PIAs are required to include explanations regarding what information is being collected, why it is being collected, and what the intended uses are. According to agency privacy officials, they often question agency program officials about whether planned collections are really necessary or could be reduced during the process of reviewing draft PIAs.

The Paperwork Reduction Act also addresses collection limitation when information is to be collected individually from 10 or more people. It requires agency chief information officers to determine whether the information has practical utility and is necessary for the proper performance of agency functions. Once a chief information officer has certified that a planned information collection meets 10 standards set forth in the act, the collection is submitted to OMB for review. The agency may not collect the information without OMB's approval.

Finally, OMB also has issued guidance instructing agencies to limit the collection of personally identifiable information. In early 2007, OMB issued Memorandum M-07-16, which required agencies to review and reduce the volume of their holdings of personally identifiable information to the minimum necessary for the proper performance of documented agency functions. The memorandum noted that "by collecting only the information necessary and managing it properly, agencies can often reduce the volume of information they possess, the risk to the information, and the burden of safeguarding it." The memorandum also required agencies to develop a plan to reduce their use of Social Security numbers and to make public a schedule by which they would periodically update the review of their overall holdings of personally identifiable information.

[48]See appendix III for a list of the specific exceptions where agencies do not need the consent of individuals to share their information.

Nothwithstanding these various provisions in law and guidance, the government's collection of personal information may not be effectively limited:

- *The Privacy Act's "relevant and necessary" provision gives broad latitude to agencies in determining the amount of information to collect.* The Privacy Act states that each agency shall "maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by Executive order of the President." Under these criteria, agency officials do not have specific requirements for justifying how much information to collect; instead, it is a matter of judgment whether any specific piece of information is relevant and necessary. OMB's implementation guidance advises agencies to identify the specific provisions in law that authorize a collection before it is implemented and provides questions that agencies should consider in determining what information to collect but concludes that a final decision on what is relevant and necessary is a matter of judgment. For certain functions, such as homeland security, new and varied collections of personal information may be relevant and necessary. However, several experts at our forum expressed concern about what they view as an increasing trend in the post-9/11 era for federal agencies to collect as much information as possible in the event that such information might be needed at a future date. Without establishing more specific requirements for justifying information collections, it may be difficult to ensure that agencies collect only relevant and necessary personal information.

- *The Paperwork Reduction Act information collection review process has not always been effective at limiting collection.* In addition to provisions in the Privacy Act, the PRA has the potential to serve as a useful control for ensuring that agencies make reasoned judgments about what personal information to collect. However, it has not always achieved this objective. As we reported in 2005, the PRA's constraints on information collection are not always completely followed.[49] For our previous report, we examined a sample of 12 approved information collections to assess the effectiveness of the PRA review process. We found that while chief information officers reviewed information collections regularly, support for a particular collection was often partial. For example, of the 12 approved data collections we reviewed, 6 provided only partial support for

[49]GAO, *Paperwork Reduction Act: New Approach May Be Needed to Reduce Government Burden on Public*, GAO-05-424 (Washington, D.C.: May 20, 2005).

determining whether the collection was necessary for the proper performance of agency functions and 8 had only partial support for determining whether a collection provided the information it was intended to provide. Despite these shortcomings, all 12 data collections were certified by agency chief information officers, and all 12 were also approved by OMB. The fact that agencies are able to have information collections approved despite incomplete justification contributes to concern that the PRA information collection review process may not be effective at limiting collection of personally identifiable information by the government. We recommended that OMB take steps to improve the review process, and OMB responded that it was considering changing its instructions to align them more closely with 10 standards specified in the act. However, OMB has not yet addressed our recommendation.

- OMB guidance does not provide specific measures for limiting information collections. Although agency privacy officials believe the PIA process gives them the opportunity to address collection limitation, the requirements of the E-Government Act do not specifically address collection limitation, and OMB PIA guidance accordingly does not include requirements for limiting information collection, and the process does not include criteria for making determinations as to whether specific planned data elements are necessary. The lack of specific control mechanisms contributes to concerns by privacy experts that collection of personally identifiable information is not being effectively limited. Similarly, OMB's recent guidance to limit collection of personally identifiable information did not include plans to monitor agency actions or take other proactive steps to ensure that agencies are effectively limiting their collections of personally identifiable information. OMB has not reported publicly on agencies' progress in responding to its guidance, and thus it remains unclear what steps agencies have taken. Finally, like previous guidance, M-07-16 did not provide any criteria for making determinations about whether specific data elements are needed. Without a legal requirement to limit collection of personally identifiable information, it is unclear the extent to which agencies will follow OMB's guidance.

## Mechanisms to Limit Use of Personally Identifiable Information to a Specified Purpose May Be Ineffective

The Privacy Act generally prevents agencies from sharing personal information in systems of records, except pursuant to a written request by, or with prior written consent of, the affected individual. There are, however, a number of specific conditions defined by the Privacy Act under which federal agencies may share information from systems of records with other government agencies without the affected individuals' consent.

For example, agencies may share information with another agency for civil or criminal law enforcement activity.[50] Sharing is also allowed if it is for a purpose that is "compatible" with the purpose for which the information was collected, referred to as a "routine use." Agencies are required to enumerate these routine uses in their system-of-records notices[51] and publish the notice in the *Federal Register* for public comment. According to OMB's 1975 implementation guidance, the routine use provisions were intended to "serve as a caution to agencies to think out in advance what uses it will make of information" and was intended "to discourage the unnecessary exchange of information to other persons or to agencies who may not be as sensitive to the collecting agency's reasons for using and interpreting the material." Section 208 of the E-Government Act of 2002 and related OMB guidance also have provisions that implement the use limitation principle, chiefly by requiring that PIAs include the intended uses of the information and with whom the information will be shared.

Although the Privacy Act and E-Government Act have provisions for limiting the use of personally identifiable information to a specified purpose, these mechanisms may not always be effective for the following reasons:

- *Unconstrained application of pre-defined "routine" uses may weaken use limitations.* A number of concerns have been raised about the impact on privacy of potentially unnecessary routine uses for agency systems of records, particularly through the application of "standard" routine uses that are developed for general use on multiple systems of records. This practice is not prohibited by the Privacy Act. All six agencies we reviewed had lists of standard routine uses for application to their systems of records. However, the language of these standard routine uses varies from agency to agency. For example, as shown in table 4, several agencies have a routine use allowing them to share information about individuals with other governmental entities for purposes of decision-making about hiring

[50]5 U.S.C. § 552a(b)(7): "to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought."

[51]In cases where the collection occurs directly from the individual, an agency is required to include the routine uses on the form which it uses to collect the information.

or retention of an individual, issuance of a security clearance, license, contract, grant, or other benefit.

**Table 4: Sample Descriptions from Five Agencies of a Standard Routine Use for Hiring or Retention of an Individual or the Issuance of a Security Clearance, Contract, Grant, or Other Benefit**

| Agency | Standard routine use |
|---|---|
| DHS | To appropriate federal, state, local, tribal, territorial, foreign, or international agency, if the information is relevant and necessary to a requesting agency's decision concerning the hiring or retention of an individual, or issuance of a security clearance, license, contract, grant or other benefit, or if the information is relevant and necessary to a DHS decision concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit and when disclosure is appropriate to the proper performance of the official duties of the person making the request. |
| DOT | A record from this system of records may be disclosed, as a routine use, to a federal agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter. |
| HHS | Disclosure may be made to a federal, state, local, foreign, or tribal or other public authority of the fact that this system of records contains information relevant to the retention of an employee, the retention of a security clearance, the letting of a contract, or the issuance or retention of a license, grant, or other benefit. The other agency or licensing organization may then make a request supported by the written consent of the individual for the entire record if it so chooses. No disclosure will be made unless the information has been determined to be sufficiently reliable to support a referral to another office within the agency or to another federal agency for criminal, civil, administrative personnel, or regulatory action. |
| IRS | Disclose to a federal, state, local, or tribal agency, or other public authority, which has requested information relevant or necessary to hiring or retaining an employee, or issuing or continuing a contract, security clearance, license, grant, or other benefit. This is compatible with the purpose for which the records were collected because the disclosure permits the IRS to assist another agency or authority in ensuring that it only hires or issues benefits to eligible individuals. |
| DOJ | To appropriate officials and employees of a federal agency or entity that requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract; or the issuance of a grant or benefit. |

Source: DHS, DOT, HHS, IRS, and DOJ.

As shown in the table, one agency (HHS) includes a provision that sharing of this information will occur only after the requesting agency has submitted a request supported by written consent of the affected individual. In contrast, similar routine uses at other agencies (DHS, DOJ, IRS, and DOT) have no requirement for the written consent of the individual. Still another agency (SSA) has no comparable standard routine use at all. Experts expressed concern that "standard" routine uses such as these vary so much from agency to agency, with no specific legal requirement that they be formulated consistently.

Further, agencies do not apply these uses consistently. DHS, for example, has a "library" of routine uses that are applied selectively to systems of

records on a case-by-case basis. In contrast, DOT applies its list of general routine uses to all of its systems of records, unless explicitly disavowed in the system's public notice. Similarly, the FBI applies its "blanket" routine uses to "every existing FBI Privacy Act system of records and to all FBI systems of records created or modified in the future." As a result, use may not always be limited as the Privacy Act intended.

- *The Privacy Act sets only modest limits on the use of personal information for multiple purposes within an agency.* Recognizing the need for agency personnel to access records to carry out their duties, the Privacy Act permits disclosures from agency systems of records "to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties." However, without additional limits, internal uses could go beyond uses that are related to the purpose of the original collection. In our interviews with senior agency privacy officials, we asked what, if any, limits were placed on internal agency uses of information. Several agencies responded that, consistent with the Privacy Act and OMB guidance, internal agency usage of personal information was limited to those personnel with a "need to know."[52] Because the Privacy Act and related guidance do not require it, none of these agencies took steps to determine whether internal uses were consistent with the purposes originally stated for the collection of information. Reliance on the "need to know" criteria for sharing information does not require a determination regarding compatibility with the original collection.

  The potential that personal information could be used for multiple, unspecified purposes is especially heightened in large agencies with multiple components that may collect personal information in many different ways for disparate purposes. For example, the establishment of DHS in March 2003 brought 22 agencies with varied missions and 180,000 employees into a single agency. These agencies collect personal information for a range of purposes, including administering citizenship, enforcing immigration laws, protecting land and sea ports of entry, and protecting against threats to aviation security. The Privacy Act does not constrain DHS or other agencies from using information obtained for one of these specific missions for another agency mission. As a result,

[52]OMB's 1975 guidance states that "Minimally, the recipient officer or employee must have an official 'need to know.' [The legislative history] would also seem to imply that the use should be generally related to the purpose for which the record is maintained."

individuals do not have assurance that their information will be used only for the purpose for which it was collected.

- *The Privacy Act's provisions may not apply when data are shared for use by another agency.* In addition to concerns about limiting use to a specified purpose within an agency, more extensive issues have been raised when data are shared outside an agency, even when such sharing is pursuant to a predefined "routine" use. Although the Privacy Act provides assurance that the information in systems of records cannot be disclosed unless it is pursuant to either a routine use or another statutorily allowed condition, the act does not attach its protections to data after they have been disclosed.[53] Despite the lack of requirements, agencies we reviewed reported taking measures to ensure the data are used appropriately by recipients. For example, agencies reported using mechanisms such as computer matching agreements under the matching provisions of the Privacy Act or other types of data-sharing agreements to impose privacy protections on recipients of shared data. However, absent these measures taken by agencies, data shared outside federal agencies would not always have sufficient protections.

Data sharing among agencies is central to the emerging information sharing environment intended to facilitate the sharing of terrorism information. If the information sharing environment is to be effective, it will require policies, procedures, and technologies that link people, systems, and information among all appropriate federal, state, local, and tribal entities and the private sector. In the recent development of guidelines for the information-sharing environment, there has been general agreement that privacy considerations must also be addressed alongside measures for enhancing the exchange of information among agencies. The Intelligence Reform and Terrorism Prevention Act of 2004 called for the issuance of guidelines to protect privacy and civil liberties in the development of the information sharing environment, and the President reiterated that requirement in an October 2005 directive to federal departments and agencies. Based on the President's directive, a committee within the Office of the Director of National Intelligence was established

[53]If personal data are disclosed to another federal agency, the recipient agency may maintain this data in a system of records, and thus protections for this data would be defined by the recipient agency's system-of-records notice. However, these protections may not be consistent with statements originally made in the contributing agency's system-of records notice. For example, the recipient agency may state different routine uses and purposes. Further, if data are disclosed to an agency and are not maintained in a system of records, the Privacy Act no longer provides protections for that information.

to develop such guidelines, and they were approved by the President in November 2006.[54] However, as we previously testified,[55] the guidelines as issued provide only a high-level framework for addressing privacy protection and do not include all of the Fair Information Practices.

More recently, in September 2007, the Program Manager for the Information Sharing Environment released a *Privacy and Civil Liberties Implementation Guide for the Information Sharing Environment.*[56] The guide describes the processes for information-sharing environment participants to follow when integrating privacy and civil liberties safeguards into their information sharing efforts, including an assessment of whether current activities comply with the privacy guidelines. However, as noted by our expert panel, these guidelines do not address the application of protections to Privacy Act data as they are shared within the information sharing environment, mentioning the act only in passing. In the absence of the adoption of more specific implementation guidelines or more explicit protections in the Privacy Act for data that are disclosed, agency information-sharing activities may not ensure that the use of personal information is sufficiently limited.

## Alternatives for Better Ensuring That Purpose Is Specified and That Collection and Use of Personal Information Are Limited

A number of options exist for addressing the issues associated with specifying the purpose for obtaining personal information, limiting the collection of such information, and limiting its use to specified purposes. Alternatives in each of these categories are as follows

### Purpose Specification

- *Require agencies to state the principal purpose for each system of records.* Having a specific stated purpose for each system of records

[54]Program Manager, Information Sharing Environment, *Guidelines to Ensure That the Information Privacy and Other Legal Rights of Americans Are Protected in the Development and Use of the Information Sharing Environment* (Nov. 22, 2006).

[55]GAO, *Homeland Security: Continuing Attention to Privacy Is Needed as Programs Are Developed*, GAO-07-630T (Washington, D.C.: Mar. 21, 2007).

[56]Program Manager, Information Sharing Environment, *Privacy and Civil Liberties Implementation Guide for the Information Sharing Environment* (Sept. 10, 2007).

would make it easier to determine whether planned uses were consistent with that purpose.

Collection Limitation

- *Require agencies to limit collection of personally identifiable information and to explain how such collection has been limited in system-of-records notices.* This requirement would more directly require agencies to limit their collection of personally identifiable information than the current requirement, which is simply to maintain only such information as is relevant and necessary to accomplish a purpose of the agency.

- *Revise the Paperwork Reduction Act to include specific requirements for limiting the collection of personally identifiable information.* The Paperwork Reduction Act currently does not specifically address limiting the collection of personally identifiable information but could serve as an established mechanism for incorporating such limits.

Use Limitation

- *Require agencies to justify the use of key elements of personally identifiable information.* Agencies could be required to state their reasons for collecting specific personally identifiable information, such as Social Security numbers and dates of birth. The Secure Flight program within DHS, for example, recently went through a process of analyzing specific data elements to be collected from airline passengers for pre-screening purposes and was able as a result to limit its requirements to only a few key elements for most passengers. Given concerns about data collection, it is likely that other government data collections could also be reduced based on such an analysis.

- *Set specific limits on routine uses and internal uses of information within agencies.* Sharing of information within an agency could be limited to purposes clearly compatible with the original purpose of a system of records. Agencies could also be required to be specific in describing purposes associated with routine uses.

- *Require agencies to establish formal agreements with external governmental entities before sharing personally identifiable information with them, as is already done at certain agencies.* These formal agreements would be a means to carry forward to external entities the privacy controls that applied to the information when it was in an agency system of records.

These requirements could be set explicitly in law or a legal requirement could be set for another agency, such as OMB, to develop specific implementation guidelines for agencies. Setting such requirements could

help ensure that a proper balance exists in allowing government agencies to collect and use personally identifiable information while also limiting that collection and use to what is necessary and relevant.

## The Privacy Act May Not Include Effective Mechanisms for Informing the Public

Transparency about government programs and systems that collect and use personal information is a key element in maintaining public trust and support for programs that use such information. A primary method for providing transparency is through public written notices. A clear and effective notice can provide individuals with critical information about what personal data are to be collected, how they are to be used, and the circumstances under which they may be shared. An effective notice can also provide individuals with information they need to determine whether to provide their personal information (if voluntary), or who to contact to correct any errors that could result in an adverse determination about them.

In formal terms, the openness principle states that the public should be informed about privacy policies and practices and that individuals should have a ready means of learning about the use of personal information. The openness principle underlies the public notice provisions of the Privacy Act. Specifically, the Privacy Act requires agencies to publish in the *Federal Register*, "upon establishment or revision, a notice of the existence and character of a system of records." This notice is to include, among other things, the categories of records in the system as well as the categories of sources of records. The notice is also required to explain agency procedures whereby an individual can gain access to any record pertaining to him or her contained in the system of records and contest its content. Agencies are further required to publish notice of any new use or intended use of the information in the system and provide an opportunity for interested persons to submit written data, views, or arguments to the agency.[57]

[57]The Privacy Act allows agencies to claim exemptions if the records are used for certain purposes. 5 U.S.C. § 552a (j) and (k). For example, records compiled by criminal law enforcement agencies for criminal law enforcement purposes can be exempt from the access and correction provisions. In general, the exemptions for law enforcement purposes are intended to prevent the disclosure of information collected as part of an ongoing investigation that could impair the investigation or allow those under investigation to change their behavior or take other actions to escape prosecution. See appendix III for a complete description of these exemptions.

In addition, when collection of personal information is received directly from the affected individual, agencies are required to notify the individual of the primary purposes for the collection and the planned routine uses of the information. The act encourages agencies, to the extent practicable, to collect information directly from the subject individual when the information may result in adverse determinations about the individual's rights, benefits, and privileges under federal programs.

It is critical that Privacy Act notices effectively communicate to the public the nature of agency collection and use of personal information because such notices are the fundamental mechanisms by which agencies are held accountable for specifying purpose, limiting collection and use, and providing a means to access and correct records. These notices can be seen as agreements between agencies and the public to provide protections for the data in the custody of the government.

System-of-records notices are especially important in cases where information is not obtained directly from individuals because there is no opportunity for them to be informed directly. As experts noted, collection from individuals may be less prevalent in an environment where agencies are encouraged to participate in cross agency e-government initiatives that promote a "collect once, use many" approach. Experts also noted that since the terrorist attacks on 9/11, agencies are charged with sharing information more readily, one of the major goals of the information sharing environment. In situations such as these, the system-of-records notice may be one of the only ways for individuals to learn about the collection of their personal information.

However, experts at our forum as well as agency privacy officials questioned the value of system-of-records notices as vehicles for providing information to the general public. Specifically, concerns were raised that the content of these notices and their publication in the *Federal Register* may not fully inform the public about planned government uses of personal information, for the following reasons:

- *System of record notices may be difficult to understand.* As with other legally-required privacy notices, such as the annual privacy notices provided to consumers by banks and other financial institutions, system-of-records notices have been criticized as hard to read and understand. For example, lay readers may have difficulty understanding the extent to which lists of "routine" uses actually explain how the government intends to collect and use personal information. Likewise, for an uninformed reader, a list of exemptions claimed for the system—cited only by the

corresponding paragraph number in the Privacy Act—could raise more questions than it answers. Agency senior privacy officials we interviewed frequently cited legal compliance as the primary function of a system-of-records notice, thus leading to legalistic descriptions of the controls on collection and use of personal information. These officials acknowledged that these descriptions of privacy protections may not be very useful to the general public. Privacy experts at our forum likewise viewed system-of-records notices as having limited value as a vehicle for public notification.

- *System-of-records notices do not always contain complete and useful information about privacy protections.* As discussed earlier in this report, system-of-records notices can be written to describe purposes and uses of information in such broad terms that it becomes questionable whether those purposes and uses have been significantly limited. Likewise, broad purpose statements contained in system-of-records notices may not contain enough information to usefully inform the public of the government's intended purposes, and the citation of multiple routine uses does little to aid individuals in learning about how the government is using their personal information. The Privacy Act does not require agencies to be specific in describing the purposes associated with routine uses. Further, individuals are limited in their ability to know how extensively their information may be used within an agency, since there are no requirements to publish all expected internal agency uses of personal information.

  Several agency privacy officials as well as experts at our forum noted that privacy impact assessments, when properly prepared, can lead to more meaningful discussions about privacy protections and may serve as a better vehicle to convey purposes and uses of information to the public. OMB guidance requires agency PIAs to identify what choices were made regarding an IT system or information collection as a result of performing a PIA, while a system-of-records notice contains no comparable requirement. As a result, a well-crafted PIA may provide more meaningful notice to the public not only about the planned purposes and uses of personal information, but also about how an agency's assessment was used to drive decisions about the system.

- *Publication in the Federal Register May Reach Only a Limited Audience.* Agency privacy officials questioned whether the required publication of system-of-records notices in the *Federal Register* would be useful to a broader audience than federal agency officials and public interest groups, such as privacy advocacy groups. Notices published in the *Federal Register* may not be very accessible and readable. The *Federal Register* Web site does not provide a ready means of determining what system-of-

records notices are current, when they were last updated, or which ones apply to any specific governmental function. Officials agreed that it can be difficult to locate a system-of-records notice on the *Federal Register* Web site, even when the name of the relevant system of records is known in advance. Privacy experts at our forum likewise agreed that the *Federal Register* is probably not effective with the general public and that a more effective technique for reaching a wide audience in today's environment is via consolidated publication on a governmentwide Web site devoted to privacy. Both agency officials and privacy experts also agreed, however, that the *Federal Register* serves a separate but important role as the official public record of federal agencies, and thus it would not be advisable to cease publishing system-of-records notices in the *Federal Register*. Notice in the *Federal Register* also serves an important role as the official basis for soliciting comments from the public on proposed systems of records.

## Alternatives for Improving Notice to the Public

Based on discussions with privacy experts, agency officials, and analysis of laws and related guidance, a number of options exist for addressing the issues associated with improving public notice regarding federal collection and use of personal information. As with the alternatives previously discussed, these could be addressed explicitly in law or a legal requirement could be set for another agency, such as OMB, to develop specific implementation guidelines for agencies. These alternatives are as follows:

- *Require layered public notices in conjunction with system-of-records notices.* Given the difficulty that a lay audience may face in trying to understand the content of notices, experts at our forum agreed that a new approach ought to be taken to designing notices for the public about use of personal information. Specifically, the use of layered notices, an approach that is actively being pursued in the private sector for consumer privacy notices, could also be effective for Privacy Act notices. Layering involves providing only the most important summary facts up front—often in a graphically oriented format—followed by one or more lengthier, more narrative versions. By offering both types of notices, the benefits of each can be realized: long notices have the advantage of being complete, but may not be as easy to understand, while brief notices may be easier to understand but may not capture all the detail that needs to be conveyed. A recent interagency research project on the design of easy-to-understand consumer financial privacy notices found, among other things, that providing context to the notice (explaining to consumers why they are receiving the notice and what to do with it) was key to comprehension, and that comprehension was aided by incorporating key visual design

elements, such as use of a tabular format, large and legible fonts, and appropriate use of white space and simple headings.[58]

The multilayered approach discussed and lessons learned could be applied to government privacy notices. For example, a multilayered government privacy notice could provide a brief description of the information required, the primary purpose for the collection, and associated uses and sharing of such data at one layer. The notice could also provide additional details about the system or program's uses and the circumstances under which data could be shared at a second layer. This would accomplish the purpose of communicating the key details in a brief format, while still providing complete information to those who require it. Aiming to improve comprehension of notices by citizens through clearer descriptions could better achieve the Privacy Act's objective of publishing a public notice of the "existence and character" of systems of records.

- *Set requirements to ensure that purpose, collection limitations, and use limitations are better addressed in the content of privacy notices.* Additional requirements could be established for the content and preparation of system-of-records notices, to include a specific description of the planned purpose of a system as well as what data needs to be collected to serve that purpose and how its use will be limited to that purpose, including descriptions of primary and secondary uses of information. Agencies may be able to use material developed for PIAs to help meet these requirements. Setting these requirements could spur agencies to prepare notices that include more meaningful descriptions of the intents and purposes of their systems of records.

- *Make all notices available on a governmentwide privacy Web site.* Experts at our forum and agency officials also agreed that the most effective and practical method for sharing information with the public is through the Web. Relevant privacy notices could be published at a central governmentwide location, such as www.privacy.gov, and at corresponding standard locations on agency Web sites, such as www.agency.gov/privacy. Given that adequate attention is paid to making the information searchable as well as easy to locate and peruse, such a Web site has the potential to reach a far broader spectrum of users than the *Federal Register*.

[58]Kleimann Communication Group, Inc., *Evolution of a Prototype Financial Privacy Notice: A Report on the Form Development Project* (Feb. 28, 2006).

## Conclusions

Current laws and guidance governing the federal government's collection, use, and disclosure of personal information have gaps and other potential shortcomings in three broad categories: (1) the Privacy Act and E-Government Act do not always provide protections for federal uses of personal information, (2) laws and guidance may not effectively limit agency collection and use of personal information to specific purposes, and (3) the Privacy Act may not include effective mechanisms for informing the public.

These issues merit congressional attention as well as continued public debate. Some of these issues—particularly those dealing with limitations on collection and use as well as mechanisms for informing the public—could be addressed by OMB through revisions or supplements to guidance. However, unilateral actions by OMB would not have the benefit of public deliberations regarding how best to achieve an appropriate balance between the government's need to collect, process, and share personally identifiable information and the rights of individuals to know about such collections and be assured that they are only for limited purposes and uses. Striking such a balance is properly the responsibility of Congress.

## Matter for Congressional Consideration

In assessing the appropriate balance between the needs of the federal government to collect personally identifiable information for programmatic purposes and the assurances that individuals should have that their information is being sufficiently protected and properly used, Congress should consider amending applicable laws, such as the Privacy Act and the E-Government Act, according to the alternatives outlined in this report, including:

- revising the scope of the laws to cover all personally identifiable information collected, used, and maintained by the federal government;
- setting requirements to ensure that the collection and use of personally identifiable information is limited to a stated purpose; and
- establishing additional mechanisms for informing the public about privacy protections by revising requirements for the structure and publication of public notices.

## Agency Comments and Our Evaluation

We received written comments on a draft of this report from the Deputy Administrator of the Office of E-Government and Information Technology and the Deputy Administrator of the Office of Information and Regulatory

Affairs of OMB. The letter is reprinted in appendix V. In their comments, the officials noted that they shared our concerns about privacy and listed guidance the agency has issued in the areas of privacy and information security. The officials stated they believe it would be important for Congress to consider potential amendments to the Privacy Act and the E-Government Act in the broader context of the several privacy statutes that Congress has enacted.

Though we did not make specific recommendations to OMB, the agency provided comments on the alternatives identified in conjunction with our matter for congressional consideration. Regarding alternatives for revising the scope of laws to cover all personally identifiable information collected, used, and maintained by the federal government, OMB stated that it would be important for Congress to evaluate fully the potential implications of revisions such as amending the Privacy Act's system-of-records definition. We believe that, given the Privacy Act's controls on the collection, use, and disclosure of personally identifiable information do not consistently protect such information in all circumstances of its collection and use throughout the federal government, amending the act's definition of a system of records is an important alternative for Congress to consider. However, we agree with OMB that such consideration should be thorough and include further public debate on all relevant issues.

Regarding alternatives for setting requirements to ensure that the collection and use of personally identifiable information is limited to a stated purpose, OMB stated that agencies are working to implement a requirement in a recent OMB memorandum to review and reduce the volume of personally identifiable information they handle "to the minimum necessary." The draft report notes that this requirement is in place; however, because significant concerns were raised about this issue by our previous work and by experts at our forum, we believe Congress should consider additional alternatives for ensuring that the collection and use of personally identifiable information is limited to a stated purpose.

Finally, regarding effective mechanisms for informing the public, OMB stated that it supports ensuring that the public is appropriately informed of how agencies are using their information. OMB stated that they will review agency practices in informing the public and review the alternatives outlined in our report.

OMB provided additional technical comments, which are addressed in appendix V. We also received technical comments from DHS, DOJ, DOT,

and IRS. We have addressed these comments in the final report as appropriate.

Unless you publicly announce the content of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies of this report to the Attorney General, the Secretaries of Homeland Security, Health and Human Services, and Transportation; the Commissioners of the Internal Revenue Service and the Social Security Administration; the Director, Office of Management and Budget; and other interested congressional committees. Copies will be made available at no charge on our Web site, www.gao.gov.

If you have any questions concerning this report, please call me at (202) 512-6240 or send e-mail to koontzl@gao.gov. Contact points for our office of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix VI.

Linda D. Koontz

Linda D. Koontz
Director, Information Management Issues

*List of Congressional Requesters*

The Honorable Harry Reid
Senate Majority Leader
United States Senate

The Honorable Daniel K. Akaka
Chairman
Committee on Veterans' Affairs
United States Senate

The Honorable Joseph I. Lieberman
Chairman
Committee on Homeland Security
and Governmental Affairs
United States Senate

The Honorable Bob Filner
Chairman
Committee on Veterans' Affairs
House of Representatives

The Honorable Hillary Rodham Clinton
United States Senate

The Honorable Byron L. Dorgan
United States Senate

The Honorable Patty Murray
United States Senate

The Honorable Barack Obama
United States Senate

The Honorable John D. Rockefeller, IV
United States Senate

The Honorable Ken Salazar
United States Senate

The Honorable Charles E. Schumer
United States Senate

# Appendix I: Objective, Scope, and Methodology

Our objective was to identify major issues regarding whether the Privacy Act of 1974, the E-Government Act of 2002, and related guidance consistently cover the federal government's collection and use of personal information and incorporate key privacy principles, and in doing so, to identify options for addressing these issues. Our objective was not focused on evaluating compliance with these laws; rather, it was to identify major issues concerning their sufficiency in light of current uses of personal information by the federal government.

To address our objective, we reviewed and analyzed the Privacy Act, section 208 of the E-Government Act, and related Office of Management and Budget (OMB) guidance to determine the types of activities and information they apply to and to identify federal agency privacy responsibilities. We compared privacy protection requirements of these laws and related OMB guidance with the Fair Information Practices to identify any issues or gaps in privacy protections for personal information controlled by the federal government. In this regard, we also assessed the role of the Paperwork Reduction Act in protecting privacy by limiting collection of information. We also drew upon our prior work to identify examples of potential gaps in addressing the Fair Information Practices. A list of related GAO products can be found at the end of this report.

We also obtained an operational perspective on these issues by analyzing agency privacy-related polices and procedures and through discussion sessions on the sufficiency of these laws with senior agency privacy officials at six federal agencies. These agencies were the Departments of Health and Human Services, Homeland Security, Justice, and Transportation; the Internal Revenue Service; and the Social Security Administration. We selected these agencies because they have large inventories of information collections, prominent privacy issues, and varied missions. Additionally, our colleagues at the National Academy of Sciences (NAS) agreed that this selection was appropriate for obtaining an operational perspective on these issues. The perspective obtained from the six agencies is not representative governmentwide. However, because we selected these agencies based on a rigorous set of selection criteria, the information we gathered during this discussion session provided us with an overview and operational perspective of key privacy-related policies and procedures. The design of our discussion session was informed by a small group meeting held with several agency privacy officials in June 2007.

To obtain a citizen-centered perspective on the impact of gaps in privacy laws and guidance, we contracted with NAS to convene an expert panel.

The panel, which was held in October 2007, consisted of 12 privacy experts, who were selected by NAS and were from varying backgrounds, such as academic, commercial, advocacy, and other private-sector communities. A list of the individuals participating in the expert forum can be found in appendix II. We developed an agenda and facilitated a detailed discussion concerning major issues with the existing framework of privacy laws. In addition, we met separately with Franklin Reeder, an expert involved in development of the Privacy Act and OMB guidance on the act, who was unable to participate in the expert forum.

To identify options for addressing major issues identified, we drew from our own analysis, our interviews with senior agency privacy officials, as well as feedback and suggestions brought forth during the expert forum.

We conducted this performance audit from March 2007 to May 2008, in Washington, D.C., in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

# Appendix II: National Academy of Sciences Expert Panel Participants

We contracted with NAS to convene a panel of privacy experts outside government to obtain a citizen-centered perspective on the impact of gaps in privacy laws and guidance. Below is a listing of panel participants and their current affiliations:

Jennifer Barrett, Privacy Leader, Acxiom Corporation

Fred Cate, Distinguished Professor, Indiana University School of Law-Bloomington

Daniel Chenok, Senior Vice President, Pragmatics

Robert Gellman, Privacy and Information Policy Consultant

Jim Harper, Director, Cato Institute, Information Policy Studies

Nuala O'Connor Kelly, Chief Privacy Leader, General Electric Company

Priscilla M. Regan, Professor of Government and Politics, George Mason University, Department of Public and International Affairs

Leslie Ann Reis, Director & Adjunct Professor of Law, The John Marshall Law School Center for Information Technology and Privacy Law

David Sobel, Senior Counsel, Electronic Frontier Foundation

John T. Sabo, Director, Global Government Relations, Computer Associates, Inc.

Barry Steinhardt, American Civil Liberties Union, Technology and Liberty Program

Peter Swire, C. William O'Neill Professor of Law, Ohio State University, Moritz College of Law

NAS staff assisting in coordinating the selection of experts and organizing the forum included, Joan Winston, Program Officer; Kristen Batch, Associate Program Officer; and Margaret Huynh, Senior Program Assistant.

**Forum Facilitators:**

John de Ferrari, Assistant Director

David Plocher, Senior Attorney

Andrew Stavisky, Methodologist

# Appendix III: Privacy Act Exemptions and Exceptions to the Prohibition Against Disclosure without Consent of the Individual

Agencies are allowed to claim exemptions from some of the provisions of the Privacy Act if the records are used for certain purposes such as law enforcement. The Privacy Act also provides that agencies not disclose information from a system of records without prior written consent of the individual to whom the record pertains, unless the disclosure falls under 1 of 12 exceptions defined by the act.

## The Privacy Act Provides Exemptions for Certain Sensitive Activities

Subsections (j) and (k) of the Privacy Act prescribe the circumstances under which exemptions can be claimed and identify the provisions of the act from which agencies can claim exemptions. When an agency uses the authority in the act to exempt a system of records from certain provisions, it is to issue a rule explaining the reasons for the exemption.

Subsection (k) of the Privacy Act permits agencies to claim specific exemptions from seven provisions of the act that relate to notice to an individual concerning the use of personal information, requirements that agencies maintain only relevant and necessary information, and procedures for permitting access to and correction of an individual's records, when the records are

1. subject to the exemption for classified information in b(1) of the Freedom of Information Act;
2. certain investigatory material compiled for law enforcement purposes other than material within the scope of a broader category of investigative records compiled for civil or criminal law enforcement purposes addressed in subsection (j);
3. maintained in connection with providing protective services to the President of the United States;
4. required by statute to be maintained and used solely as statistical records;
5. certain investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information;
6. certain testing or examination material used solely to determine individual qualifications for appointment or promotion in the federal service; and

7. certain evaluation material used to determine potential promotion in the armed services

Under these circumstances, agencies may claim exemptions from the provisions of the act, described in table 5.

**Table 5: Privacy Act Provisions Agencies May Claim an Exemption under Subsection (k)**

| Citation | Description of provision |
|---|---|
| 5 U.S. C. §552a(c)(3) | Agencies must make an accounting of disclosures available to the individual named in the record at his request. |
| 5 U.S.C. § 552a(d) | Agencies must permit an individual to have access to his record, request amendment, if necessary, and if the agency refuses to amend the record, permit the individual to request, review of such refusal. If a contested record is disclosed, agencies must note any portion of the record that is disputed prior making a disclosure. |
| 5 U.S.C. § 552a(e)(1) | Agencies must maintain in their records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President. |
| 5 U.S.C. § 552a(e)(4)(G),(H), and (I) | Agencies must publish a system-of-records notice including the procedures by which an individual can be notified at his request if the system of records contains a record pertaining to him; the procedures by which an individual can be notified at his request how he can gain access to any record pertaining to him and how he can contest its content; and the categories of sources in the system. |
| 5 U.S.C. §552a(f) | Agencies must issue rules to establish, among other things, procedures whereby an individual can gain access to his records and request amendment. |

Source: The Privacy Act of 1974.

Subsection (j) provides a broader set of general exemptions, which permits records maintained by the Central Intelligence Agency or certain records maintained by an agency which has enforcement of criminal laws as its principal function to be exempted from any provision of the act, except those described in table 6.

**Table 6: Privacy Act Provisions from Which Agencies May Not Claim Exemptions**

| Citation | Description of provision |
|---|---|
| 5 U.S.C. § 552a(b) | Agencies cannot disclose records without prior written consent of the individual to whom the record pertains unless disclosure of the records falls under 1 of 12 exceptions. |
| 5 U.S.C. § 552a(c)(1) and (2), | Agencies must account for certain disclosures including the date, nature, and purpose of each disclosure and the name and address of the person or agency to whom the disclosure is made. Agencies must retain the accounting for at least five years or the life of the record, whichever is longer. |
| 5 U.S.C. § 552a(e)(4)(A) through (F) | Agencies must publish a systems of records notice in the *Federal Register* including; the name and location of the system; the categories of individuals on whom records are maintained in the system; the categories of records maintained in the system; each routine use of the records contained in the system, including the categories of users and the purpose of such use; the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records; and the title and business address of the agency official who is responsible for the system of records. |
| U.S.C. §552a(e)(6),(7), (9), (10) and (11) | Agencies:<br>• must make reasonable efforts to assure that records are accurate, complete, timely, and relevant for agency purposes prior to disseminating any record to any person other than an agency;<br>• may not maintain records describing how an individual exercises rights guaranteed by the First Amendment;<br>• must establish rules of conduct for persons involved in the design, development, operation or maintenance of any system of records;<br>• must establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records; and<br>• must publish a notice of any new or intended routine use or intended use of the information in the system in the *Federal Register* and provide an opportunity for interested persons to comment at least 30 days before publication of the final notice. |
| U.S.C. §552a(i) | Criminal penalties shall be imposed when:<br>• an employee of the agency knowingly and willfully discloses individually identifiable information from agency records in any manner to any person or agency not entitled to receive it;<br>• an employee of any agency willfully maintains a system of records without meeting the notice requirements of the act; and<br>• any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses. |

Source: The Privacy Act of 1974, 5.U.S.C. §552a.

In general, the exemptions for law enforcement purposes are intended to prevent the disclosure of information collected as part of an ongoing investigation that could impair the investigation or allow those under investigation to change their behavior or take other actions to escape prosecution.

## Exceptions to the Prohibition against Disclosure without Prior Written Consent of the Individual

Subsection (b) of the Privacy Act provides that "No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be

1. to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties;
2. required under the Freedom of Information Act;
3. for a routine use as defined in the act;
4. to the Bureau of the Census for planning or carrying out a census or survey or related activity;
5. for statistical research, provided the information is not individually identifiable;
6. to the National Archives and Records Administration for historical preservation purposes;
7. to any government agency (e.g., federal, state, or local) for a civil or criminal law enforcement activity if the head of the agency has made a written request specifying the information desired and the law enforcement activity for which the record is sought;
8. to a person upon showing compelling circumstances affecting the health or safety of an individual if notice is transmitted to the last known address of such individual;
9. to either House of Congress or any committee or subcommittee with related jurisdiction;
10. to the Government Accountability Office;
11. pursuant to a court order; or
12. to a consumer reporting agency for the purpose of collecting a claim of the government."

# Appendix IV: OMB Privacy Guidance

Since its 1975 Privacy Act Implementation Guidelines, OMB has periodically issued guidance related to privacy addressing specific issues as they have arisen. Nearly all of this guidance can be found on the OMB Web site, www.whitehouse.gov/omb, by searching in the "Agency Information" and "Information and Regulatory Affairs" sections of the Web site.

*Memorandum M-08-09 — New FISMA Privacy Reporting Requirements for FY 2008.* January 18, 2008.

*Top Ten Risks Impeding the Adequate Protection of Government Information.* July 2007.

*Memorandum M-07-19 — FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management.* July 25, 2007.

*Guidance on Protecting Federal Employee Social Security Numbers and Combating Identity Theft.* June 18, 2007.

*OMB Implementation Guidance for Title V of the E-Government Act of 2002.* June 15, 2007.

*Memorandum M-07-16 — Safeguarding Against and Responding to the Breach of Personally Identifiable Information.* May 22, 2007.

*Use of Commercial Credit Monitoring Services Blanket Purchase Agreements (BPA).* December 22, 2006.

*Recommendations for Identity Theft Related Data Breach Notification.* September 20, 2006.

*Memorandum M-06-20 — FY 2006 Reporting Instructions for FISMA.* July 17, 2006.

*Memorandum M-06-19 — Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments.* July 12, 2006.

*Memorandum M-06-16 — Protection of Sensitive Agency Information.* June 23, 2006.

*Memorandum M-06-15 — Safeguarding Personally Identifiable Information.* May 22, 2006.

*Memorandum M-06-06 — Sample Privacy Documents for Agency Implementation of HSPD-12 Common Identification Standard.* February 17, 2006.

*Memorandum M-05-15 — FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management.* June 13, 2005.

*Memorandum M-05-08 — Designation of Senior Agency Officials for Privacy.* February 11, 2005.

*Memorandum M-03-22 — Guidance for Implementing the Privacy Provisions of the E-Government Act.* September 26, 2003.

*Memorandum M-03-18 — Implementation Guidance for the E-Government Act of 2002.* August 1, 2003.

*Guidance on Inter-Agency Sharing of Personal Data—Protection Personal Privacy.* December 20, 2000.

*Baker/Spotila Letters and Memorandum M-00-13 – Privacy Policies and Date Collection on Federal Websites.* June 22, July 28, and September 5, 2000.

*Status of Biennial Reporting Requirements Under the Privacy Act and the Computer Matching and Privacy Protection Act.* June 21, 2000.

*Memorandum M-99-18 — Privacy Policies on Federal Web Sites.* June 2, 1999.

*Memorandum M-99-05 — Instructions on Complying with "Privacy and Personal Information in Federal Records."* January 7, 1999.

*Biennial Privacy Act and Computer Matching Reports.* June 1998.

*Privacy in Personal Information in Federal Records.* May 4, 1998.

*Privacy Act Responsibilities for Implementing the Personal Responsibility and Work Opportunity Reconciliation Act (PRWORA) of 1996.* November 3, 1997.

*Office of Management and Budget Order Providing for the Confidentiality of Statistical Information and Extending the Coverage of Energy Statistical Programs Under the Federal Statistical Confidentiality Order.* June 27, 1997.

*Report of the Privacy Working Group: Principles for Providing and Using Personal Information.* June 1995.

*OMB Guidance on Computer Matching and Privacy Protection Amendments of 1990 and Privacy Act of 1974.* April 23, 1991.

*Office of Management and Budget Final Guidance Interpreting the Provisions of the Computer Matching and Privacy Protection Act of 1988.* June 19, 1989.

*OMB Guidance on the Privacy Act Implications of "Call Detail" Programs.* April 20, 1987.

*OMB Circular A-130, Management of Federal Information Resources, including Federal Agency Responsibilities for Maintaining Records About Individuals, and Implementation of the Paperwork Elimination Act.* November 28, 2000.

*Updates to Original OMB Privacy Act Guidance.* May 24, 1985.

*Revised Supplemental Guidance on Implementation of the Privacy Act of 1974.* March 29, 1984.

*Guidelines on the Relationship of the Debt Collection Act of 1982 to the Privacy Act of 1974.* April 11, 1983.

*OMB Supplemental Guidance for Conducting Matching Programs.* May 14, 1982.

*Supplementary Guidance for Implementation of the Privacy Act of 1974.* November 21, 1975.

*Congressional Inquiries Which Entail Access to Personal Information Subject to the Privacy Act.* October 3, 1975.

*Privacy Act Implementation Guidelines and Responsibilities.* July 9, 1975.

# Appendix V: Comments from the Office of Management and Budget

Note: GAO comments supplementing those in the report text appear at the end of this appendix.

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

May 2, 2008

Ms. Linda D. Koontz
Director
Information Management Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Koontz:

Thank you for the opportunity to comment on the draft GAO report "Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information" (GAO-08-536). The Office of Management and Budget (OMB) welcomes GAO's review of alternatives for better safeguarding individuals' personally identifiable information (PII).

OMB shares your concerns about privacy and information security, and we take seriously our responsibilities under the Privacy Act of 1974, the E-Government Act of 2002, and the Federal Information Security Management Act of 2002. In recent years, OMB has issued several memoranda addressing privacy and information security, including:

- M-08-16 of April 4, 2008, *Guidance for Trusted Internet Connection Statement of Capability Form (SOC)*,
- M-08-10 of February 4, 2008, *Use of Commercial Independent Risk Analysis Services Blanket Purchase Agreements (BPA)*,
- M-08-09 of January 18, 2008, *New FISMA Privacy Reporting Requirements for FY 2008*,
- M-08-05 of November 20, 2007, *Implementation of Trusted Internet Connections (TIC)*,
- M-07-20 of August 14, 2007, *FY 2007 E-Government Act Reporting Instructions*,
- M-07-19 of July 25, 2007, *FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*,
- M-07-18 of June 1, 2007, *Ensuring New Acquisitions Include Common Security Configurations*,
- M-07-16 of May 22, 2007, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*,
- M-07-11 of March 22, 2007, *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*,

- M-07-04 of December 22, 2006, *Use of Commercial Credit Monitoring Services Blanket Purchase Agreements (BPA)*,
- Memorandum for the Heads of Departments and Agencies of September 20, 2006, *Recommendations for Identity Theft Related Data Breach Notification*,
- M-06-25 of August 25, 2006, *FY 2006 E-Government Act Reporting Instructions*,
- M-06-20 of July 17, 2006, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*,
- M-06-19 of July 12, 2006, *Reporting Incidents Involving Personally Identifiable Information Incorporating the Cost for Security in Agency Information Technology Investments*,
- M-06-16 of June 23, 2006, *Protection of Sensitive Agency Information*,
- M-06-15 of May 22, 2006, *Safeguarding Personally Identifiable Information*,
- M-05-15 of June 13, 2005, *FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, and
- M-05-08 of February 11, 2005, *Designation of Senior Agency Officials for Privacy*.

We appreciate the careful consideration of privacy issues in the draft report. The draft report provides several matters for congressional consideration regarding privacy, specifically, suggesting Congress should consider revising the Privacy Act and the E-Government Act. Among the alternatives the draft report discusses would be for Congress to amend the Privacy Act so that it would apply to all PII collected, maintained, and used by Federal agencies.

During the course of a legislative consideration of possible amendments to the Privacy Act and the E-Government Act, along the lines of the alternatives in the draft report, we believe it would be important for Congress to consider these issues in the broader context of the several privacy statutes that Congress has enacted. In addition to such government-wide statutes as the Privacy Act, the Privacy Impact Assessment requirements of the E-Government Act, and the Federal Information Security Management Act (FISMA), Congress has also enacted privacy laws covering such areas as health-related information (the Health Insurance Portability and Accountability Act of 1996), statistical information about individuals (the Confidential Information Protection and Statistical Efficiency Act of 2002), and intelligence, law enforcement, and homeland security (the Intelligence Reform and Terrorism Prevention Act of 2004 and the Implementing Recommendations of the 9/11 Commission Act of 2007), as well as statutes that apply specifically to information about individuals that is collected by particular agencies, such as the Census Bureau, the Internal Revenue Service, and the Social Security Administration.

In addition, during legislative consideration of possible revisions to privacy laws, we believe that it would be important for Congress to evaluate fully the potential implications of such revisions. For example, one of the alternatives that the draft report discusses would have Congress amend the Privacy Act in a very fundamental way. This alternative would involve

abandoning the Act's framework that has been in place for over 30 years, which has been to safeguard information about individuals that is found in a "system of records," and instead to have the Act apply to all PII, however maintained by an agency. We believe it would be important for Congress, in considering such a fundamental change to the Privacy Act, to consider the full range of implications flowing from that change. It may be that, based on this consideration, other legislative alternatives might be identified that would be more desirable in terms of strengthening privacy protections in the most effective and efficient manner.

The draft report also offers alternatives for ensuring that the purpose of agency use of PII is specified and agency collection and use of personal information is limited. As OMB stated in recent guidance in response to recommendations from the President's Identity Theft Task Force, agencies must review and reduce the volume of PII they handle "to the minimum necessary for the proper performance of a documented agency function." (Please see OMB Memorandum M-07-16 of May 22, 2007, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*.) Agencies are currently working to implement this guidance and the recommendations of the Task Force. In our annual reporting instructions last year to agencies on FISMA and privacy management, OMB required agencies to submit copies of policies and plans required by M-07-16, including an agency breach notification policy, an implementation plan to eliminate unnecessary use of social security numbers, an implementation plan and progress update on the review and reduction of agency holdings of PII, and an agency policy outlining rules of behavior for safeguarding PII. (Please see OMB Memorandum M-07-19 of July 25, 2007, *FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*.)

We also support ensuring the public is appropriately informed of how agencies are using their information. The publication of System of Records Notices and Privacy Impact Assessments is a crucial piece of the Federal privacy framework. We will review agency practices in informing the public and review the alternatives the draft report provides.

Finally, we would like to respond to several statements in the draft report.

See comment 1.
Now on p. 15.

On page 19, the draft report discusses draft guidance on the Paperwork Reduction Act (PRA) that OMB had prepared in 1999: "Further, [OMB] developed guidance, which while remaining in draft, is widely used as a handbook for agencies on compliance with the law, according to OMB officials." The draft report continues by stating in footnote 23 that "[a]lthough this guidance is draft, OMB officials stated that agencies are generally aware of the guidance and are expected to follow it."

The draft report is incorrect when it states that agencies "are expected to follow" the draft 1999 guidance. The draft guidance has not been finalized, and thus remains a draft. GAO made this exact same (incorrect) statement in its draft of a 2005 report on the Paperwork Reduction Act, and OMB pointed out its disagreement with this statement in OMB comments to GAO on the draft report. (See "Paperwork Reduction Act: New Approach May Be Needed to Reduce Government Burden on Public," GAO 05-424 (May 2005), Appendix III (OMB letter of April 20, 2005), pages 53-54.) However, GAO did not correct this statement in the final version of the 2005 report (see page 22 footnote 34), and the current draft report repeats this incorrect

3

statement. To be clear, agencies are expected to follow the Paperwork Reduction Act, OMB's implementing PRA regulations at 5 C.F.R. Part 1320, and OMB's January 2006 guidance to agencies on surveys conducted under the PRA.

See comment 2.
Now on p. 19.

On page 23, the draft report refers to a prior GAO conclusion from a 2003 GAO report: "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." We would note here that, in the comment letter that OMB submitted to GAO on the draft of the referenced 2003 report, OMB expressed concerns with the report's methodology and conclusions. (OMB's comment letter of June 20, 2003, is enclosed as Appendix VII of the final report.)

On page 48, the draft report states that "OMB guidance does not provide specific measures for limiting information collections . . . OMB's recent guidance to limit collection of personally identifiable information did not include plans to monitor agency actions or take other proactive steps to ensure that agencies are effectively limiting their collections of personally identifiable information. Without a legal requirement to limit collection of personally identifiable information, it is unclear the extent to which agencies will follow OMB's guidance."

See comment 3.
Now on p. 36.

As noted earlier in our letter, Federal agencies are working diligently to implement the OMB Memorandum M-07-16 requirement to review and reduce the volume of PII they handle "to the minimum necessary for the proper performance of a documented agency function." In the aftermath of major data breaches in 2006 and the findings of the President's Identity Theft Task Force, agencies have become sensitized to limiting collections of personally identifiable information. Limiting the collection of personally identifiable information to what is authorized and necessary will require on-going attention by departments and oversight by OMB, as part of its Paperwork Reduction Act and Privacy Act responsibilities.

In closing, thank you again for the opportunity to comment on the draft report.

Sincerely,

Kevin F. Neyland
Deputy Administrator
Office of Information
and Regulatory Affairs

Tim K. Young
Deputy Administrator
Office of E-Government and
Information Technology

4

The following is GAO's response to OMB's additional comments.

## GAO Comments

1. Statements in the 2005 report regarding the draft OMB Paperwork Reduction Act guidance were accurate for that review and supported by the evidence gathered. For that report, among other things, we selected detailed case reviews of 12 OMB-approved collections and compared the agencies' processes and practices in these case studies with the (1) act's requirements, (2) OMB's regulation and draft guidance to agencies, and (3) agencies' written directives and orders. Nevertheless, in its written response to the 2005 report, OMB officials stated that OMB's draft PRA guidance to agencies had become outmoded. Further, in its response, OMB stated that the report had convinced them that its draft PRA guidance did not serve its intended purpose and that it would explore alternative approaches to advising agencies on their PRA responsibilities. Accordingly, because the draft guidance has not been in effect since the 2005 report was issued, we have removed statements from our current draft regarding this guidance.

2. As we stated in our response to OMB's comments on our 2003 report,[1] we consider this report to be a comprehensive and accurate source of information on agencies' implementation of the Privacy Act. Our conclusions were based on the results of a comprehensive analysis of agency compliance with a broad range of requirements.

3. We agree that the responsibility for limiting the collection of personally identifiable information to what is authorized and necessary will require ongoing attention by agencies and oversight by OMB. We also believe that Congress should consider alternatives, as identified in our report, to improve controls on the collection and use of personally identifiable information.

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

# Appendix VI: GAO Contact and Staff Acknowledgments

## GAO Contact

Linda D. Koontz (202) 512-6240 or KoontzL@gao.gov

## Staff Acknowledgments

In addition to the contact person named above, John de Ferrari (Assistant Director), Shaun Byrnes, Susan Czachor, Barbara Collier, Tim Eagle, Matt Grote, Rebecca LaPaze, David Plocher, Jamie Pressman, and Andrew Stavisky made key contributions to this report.