United States Government Accountability Office

GAO

Testimony

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

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

PRIVACY

Key Challenges Facing Federal Agencies

Statement of Linda D. Koontz
Director, Information Management Issues

May 17, 2006

PRIVACY

Key Challenges Facing Federal Agencies

GAO Accountability·Integrity·Reliability

Highlights

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

Why GAO Did This Study

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

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

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

What GAO Recommends

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

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

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

What GAO Found

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

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

Mr. Chairman and Members of the Subcommittee:

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

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

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

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

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

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

Results in Brief

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

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

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

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

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

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

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

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

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

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

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

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

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

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

system. More specifically, according to Office of Management and Budget (OMB) guidance,[5] a PIA is an analysis of how information is handled. Specifically, a PIA is to (1) ensure that handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (2) determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (3) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Agencies must conduct PIAs (1) before developing or procuring information technology that collects, maintains, or disseminates information that is in a personally identifiable form; or (2) before initiating any new data collections involving personal information that will be collected, maintained, or disseminated using information technology if the same questions are asked of 10 or more people. To the extent that PIAs are made publicly available,[6] they provide explanations to the public about such things as the information that will be collected, why it is being collected, how it is to be used, and how the system and data will be maintained and protected.

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

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

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

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

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

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

Privacy Officers Have Gained Prominence at Several Federal Agencies

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

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

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

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

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

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

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

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

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

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

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

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

Agency Privacy Officers Face a Number of Challenges

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

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

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

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

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

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

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

[16] GAO-06-421, p. 59-61.

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

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

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

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

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

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

Ensuring that Data Mining Efforts Do Not Compromise Privacy Protections

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

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

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

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

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

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

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

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

[20] GAO-05-866.

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

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

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

We recently testified before this subcommittee on critical issues surrounding the federal government's acquisition and use of personal information from information resellers.[22] In our review of the acquisition of personal information from resellers by DHS, Justice, the Department of State, and the Social Security Administration, agency practices for handling this information did not always reflect the Fair Information Practices. For example, although agencies issued public notices on information collections, these did not always notify the public that information resellers were among the sources to be used, a practice inconsistent with the principle that individuals should be informed about privacy policies and the collection of information. And again, a contributing factor

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

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

In July 2005, we reported on shortcomings at DHS's Transportation Security Administration (TSA) in connection with its test of the use of reseller data for the Secure Flight airline passenger screening program.[23] TSA did not fully disclose to the public its use of personal information in its fall 2004 privacy notices, as required by the Privacy Act. In particular, the public was not made fully aware of, nor had the opportunity to comment on, TSA's use of personal information drawn from commercial sources to test aspects of the Secure Flight program. In September 2004 and November 2004, TSA issued privacy notices in the *Federal Register* that included descriptions of how such information would be used. However, these notices did not fully inform the public before testing began about the procedures that TSA and its contractors would follow for collecting, using, and storing commercial data. In addition, the scope of the data used during commercial data testing was not fully disclosed in the notices. Specifically, a TSA contractor, acting on behalf of the agency, collected more than 100 million commercial data records containing personal information such as name, date of birth, and telephone number without informing the public. As a result of TSA's actions, the public did not receive the full protections of the Privacy Act. In its comments on our findings, DHS stated that it recognized the merits of the issues we raised, and that TSA acted immediately to address them.

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

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

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

Addressing Concerns about Radio Frequency Identification Technology

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

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

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

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

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

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

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

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

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

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

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

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

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

Contacts and Acknowledgements

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

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

Attachment I: Selected GAO Products Related to Privacy Issues

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Attachment 2: The Fair Information Practices

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

Table 1: The Fair Information Practices

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

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

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

Source: Organization for Economic Cooperation and Development.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Mail or Phone

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

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

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Congressional Relations

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

Public Affairs

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