

May 2008

PRIVACY

Alternatives Exist for Enhancing Protection of Personally Identifiable Information





Highlights of [GAO-08-536](#), a report to congressional requesters

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.

PRIVACY

Alternatives Exist for Enhancing Protection of Personally Identifiable Information

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 information¹ 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

¹For 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.

²In 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

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

⁴Congress 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).

⁵These 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

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

⁷GAO, *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 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 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 report⁸ 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.

⁸Department 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).

⁹OECD, *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.

¹⁰OECD, *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

¹¹European 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).

¹²“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 Architecture¹⁴ 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).

¹³Privacy 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).

¹⁴The 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.

¹⁵National 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

¹⁶Under 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

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

¹⁸The 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

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

²⁰For 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 regulation²¹ 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.

²¹5 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 to 1983) 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

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

²³U.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

²⁴The 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.

²⁵Computer 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 Committee²⁶ 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 Council²⁷ 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

²⁶The 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.

²⁷The 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.

²⁸National 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

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

³⁰FISMA, 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.

³¹Although 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

³²A *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

³³According 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).

³⁴An 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 agencies³⁶ 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

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

³⁶GAO, *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 Force⁴⁰ 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

³⁷The 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).

³⁸DHS 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).

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

⁴⁰The 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

⁴¹63 *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.

⁴³Section 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: 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: 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: 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:

⁴⁴TSA’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

⁴⁵GAO, *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.

⁴⁶66 *Federal Register* 53029 (Oct. 18, 2001).

⁴⁷63 *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.

⁴⁸See appendix III for a list of the specific exceptions where agencies do not need the consent of individuals to share their information.

Notwithstanding 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

⁴⁹GAO, *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 notices⁵¹ 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

⁵⁰5 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.”

⁵¹In 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,

⁵²OMB'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

⁵³If 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

⁵⁴Program 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).

⁵⁵GAO, *Homeland Security: Continuing Attention to Privacy Is Needed as Programs Are Developed*, [GAO-07-630T](#) (Washington, D.C.: Mar. 21, 2007).

⁵⁶Program 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

⁵⁷The 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*.

⁵⁸Kleimann 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
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 policies 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

**Appendix III: Privacy Act Exemptions and
Exceptions to the Prohibition Against
Disclosure without Consent of the Individual**

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.

**Appendix III: Privacy Act Exemptions and
Exceptions to the Prohibition Against
Disclosure without Consent of the Individual**

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 <i>Federal Register</i> 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) | <p>Agencies:</p> <ul style="list-style-type: none"> • 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; • may not maintain records describing how an individual exercises rights guaranteed by the First Amendment; • must establish rules of conduct for persons involved in the design, development, operation or maintenance of any system of records; • must establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records; and • must publish a notice of any new or intended routine use or intended use of the information in the system in the <i>Federal Register</i> and provide an opportunity for interested persons to comment at least 30 days before publication of the final notice. |
| U.S.C. §552a(i) | <p>Criminal penalties shall be imposed when:</p> <ul style="list-style-type: none"> • 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; • an employee of any agency willfully maintains a system of records without meeting the notice requirements of the act; and • 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:

- o M-08-16 of April 4, 2008, *Guidance for Trusted Internet Connection Statement of Capability Form (SOC)*,
- o M-08-10 of February 4, 2008, *Use of Commercial Independent Risk Analysis Services Blanket Purchase Agreements (BPA)*,
- o M-08-09 of January 18, 2008, *New FISMA Privacy Reporting Requirements for FY 2008*,
- o M-08-05 of November 20, 2007, *Implementation of Trusted Internet Connections (TIC)*,
- o M-07-20 of August 14, 2007, *FY 2007 E-Government Act Reporting Instructions*,
- o M-07-19 of July 25, 2007, *FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*,
- o M-07-18 of June 1, 2007, *Ensuring New Acquisitions Include Common Security Configurations*,
- o M-07-16 of May 22, 2007, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*,
- o 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.

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

See comment 1.
Now on p. 15.

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.

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."

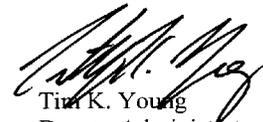
As noted earlier in our letter, Federal agencies are working diligently to implement the OMB Memorandum M-07-16 requirement to review and reduce the volume of PII they handle "to the minimum necessary for the proper performance of a documented agency function." In the aftermath of major data breaches 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

See comment 2.
Now on p. 19.

See comment 3.
Now on p. 36.

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.

¹GAO, *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.

Related GAO Products

Aviation Security: Efforts to Strengthen International Passenger Prescreening Are Under Way, but Planning and Implementation Issues Remain. [GAO-07-346](#). Washington, D.C.: May 16, 2007.

DHS Privacy Office: Progress Made but Challenges Remain in Notifying and Reporting to the Public. [GAO-07-522](#), Washington, D.C.: April 27, 2007.

Homeland Security: Continuing Attention to Privacy Concerns Is Needed as Programs Are Developed. [GAO-07-630T](#). Washington, D.C.: March 21, 2007.

Data Mining: Early Attention to Privacy in Developing a Key DHS Program Could Reduce Risks. [GAO-07-293](#). Washington, D.C.: February 28, 2007.

Border Security: US-VISIT Program Faces Strategic, Operational, and Technological Challenges at Land Ports of Entry. [GAO-07-248](#). Washington, D.C.: December 6, 2006.

Personal Information: Key Federal Privacy Laws Do Not Require Information Resellers to Safeguard All Sensitive Data. [GAO-06-674](#). Washington, D.C.: June 26, 2006.

Veterans Affairs: Leadership Needed to Address Information Security Weaknesses and Privacy Issues. [GAO-06-866T](#). Washington, D.C.: June 14, 2006.

Privacy: Preventing and Responding to Improper Disclosures of Personal Information. [GAO-06-833T](#). Washington, D.C.: June 8, 2006.

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

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.

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.: March 17, 2006.

Paperwork Reduction Act: New Approaches Can Strengthen Information Collection and Reduce Burden. [GAO-06-477T](#). Washington, D.C.: March 8, 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.

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.

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.

Related GAO Products

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.

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 "E-mail 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, DC 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

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548