United States Government Accountability Office

GAO

Testimony

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

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

PRIVACY

Congress Should Consider Alternatives for Strengthening Protection of Personally Identifiable Information

Statement of Linda Koontz
Director, Information Management Issues

June 18, 2008

PRIVACY

Congress Should Consider Alternatives for Strengthening Protection of Personally Identifiable Information

GAO Accountability • Integrity • Reliability

Highlights

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

Why GAO Did This Study

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

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

What GAO Recommends

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

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

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

What GAO Found

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

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

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

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

June 18, 2008

Mr. Chairman and Members of the Committee:

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

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

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

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

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

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

The provisions of the Privacy Act are largely based on a set of principles for protecting the privacy and security of personal information known as the Fair Information Practices, which were first proposed in 1973 by a U.S. government advisory committee.[4] These principles, with some variation, are used by organizations to address privacy considerations in their business practices and are also the basis of privacy laws and related policies in many countries, including the United States, Germany, Sweden, Australia, and New Zealand, as well as the European Union.

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

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

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

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

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

Results in Brief

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

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

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

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

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

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

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

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

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

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

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

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

Background

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

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

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

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

Table 1: The Fair Information Practices

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

Source: Organization for Economic Cooperation and Development.

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

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

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

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

The Fair Information Practices are not legal requirements but provide a framework of principles for balancing the need for privacy with other public policy interests, such as national security, law enforcement, and administrative efficiency. Striking that balance varies among countries and among types of information.

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

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

The Privacy Act places limitations on agencies' collection, disclosure, and use of personal information maintained in systems of records. The act describes a "record" as any item, collection, or grouping of information about an individual that is maintained by an agency and contains his or her name or another personal identifier. It also defines a "system of records" as a group of records under the control of any agency from which information is retrieved by the name of the individual or by an individual identifier. The Privacy Act requires that when agencies establish or make changes to a system of records, they must notify the public through a system-of-records notice in the *Federal Register* that identifies, among other things, the categories of data collected, the categories of individuals about whom information is collected, the intended "routine" uses of data,

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

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

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

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

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

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

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

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

In addition, the Paperwork Reduction Act applies to federal information collections and was designed to help ensure that when the government asks the public for information, the burden of providing this information is as small as possible and the information itself is used effectively.[13] Among the act's provisions is the requirement that agencies not establish information collections without having them approved by OMB, and that before submitting them for approval, agencies' chief information officers certify that the collections meet 10 specified standards. The law also requires agencies both to publish notices in the *Federal Register* and to otherwise consult with the public about their planned collections.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Prior GAO Reports Have Identified Privacy Challenges at Federal Agencies

We have previously reported on a number of agency-specific and governmentwide privacy-related issues at federal agencies. For example, in 2003, we reported that agencies generally did well with certain aspects of the Privacy Act's requirements—such as issuing systems-of-records notices when required—but did less well at other requirements, such as ensuring that information is complete, accurate, relevant, and timely before it is disclosed to a nonfederal organization.[18] In discussing this uneven compliance, agency officials reported the need for additional OMB leadership and guidance to assist in difficult implementation issues in a rapidly changing environment. For example, officials had questions about the act's applicability to electronic records. We have also reported on key privacy challenges facing federal agencies, federal Web site privacy, notification of individuals in the event of a data breach, and government data-mining initiatives.

Key Terms in the Privacy Act May Be Defined Too Narrowly

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Amending Privacy Laws Could Address Gaps and Shortcomings in Privacy Protections

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

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

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

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

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

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

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

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

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

Contacts and Acknowledgements

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

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