United States Government Accountability Office

GAO

Testimony

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

For Release on Delivery
Expected at 12 p.m. EST
Tuesday, April 4, 2006

# PERSONAL INFORMATION

# Agencies and Resellers Vary in Providing Privacy Protections

Statement of Linda D. Koontz
Director, Information Management Issues

April 2006

# PERSONAL INFORMATION

# Agencies and Resellers Vary in Providing Privacy Protections

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-06-609T, a report to the Subcommittee on Commercial and Administrative Law and the Subcommittee on the Constitution, Committee on the Judiciary, House of Representatives

## Why GAO Did This Study

Federal agencies collect and use personal information for various purposes from information resellers—companies that amass and sell data from many sources. GAO was asked to testify on its report being issued today on agency use of reseller data. For that report, GAO was asked to determine how the Departments of Justice, Homeland Security, and State and the Social Security Administration use personal data from resellers and to review the extent to which information resellers' policies and practices reflect the Fair Information Practices, a set of widely accepted principles for protecting the privacy and security of personal data. GAO also examined agencies' policies and practices for handling personal data from resellers to determine whether these reflect the Fair Information Practices.

## What GAO Recommends

In its report, GAO suggests that the Congress consider the extent to which resellers should adhere to the Fair Information Practices. In addition, GAO is making recommendations to the Office of Management and Budget and the four agencies to establish policy to address agency use of personal information from commercial sources.
Agency officials generally agreed with the content of the report. Resellers questioned the applicability of the Fair Information Practices, especially with regard to public records.

www.gao.gov/cgi-bin/getrpt?GAO-06-609T.

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

## What GAO Found

In fiscal year 2005, the Departments of Justice, Homeland Security, and State and the Social Security Administration reported that they used personal information obtained from resellers for a variety of purposes, including performing criminal investigations, locating witnesses and fugitives, researching assets held by individuals of interest, and detecting prescription drug fraud. The agencies spent approximately $30 million on contractual arrangements with resellers that enabled the acquisition and use of such information. About 91 percent of the planned fiscal year 2005 spending was for law enforcement (69 percent) or counterterrorism (22 percent).

The major information resellers that do business with the federal agencies GAO reviewed have practices in place to protect privacy, but these measures are not fully consistent with the Fair Information Practices. For example, the principles that the collection and use of personal information should be limited and its intended use specified are largely at odds with the nature of the information reseller business, which is based on obtaining personal information from many sources and making it available to multiple customers for multiple purposes. Resellers believe it is not appropriate for them to fully adhere to these principles because they do not obtain their information directly from individuals. Nonetheless, in many cases, resellers take steps that address aspects of the Fair Information Practices. For example, resellers reported that they have taken steps recently to improve their security safeguards, and they generally inform the public about key privacy principles and policies. However, resellers generally limit the extent to which individuals can gain access to personal information held about themselves, as well as the extent to which inaccurate information contained in their databases can be corrected or deleted.

Agency practices for handling personal information acquired from information resellers did not always fully reflect the Fair Information Practices. That is, for some of these principles, agency practices were uneven. For example, although agencies issued public notices when they systematically collected personal information, these notices did not always notify the public that information resellers were among the sources to be used. This practice is not consistent with the principle that individuals should be informed about privacy policies and the collection of information. Contributing to the uneven application of the Fair Information Practices are ambiguities in guidance from the Office of Management and Budget regarding the applicability of privacy requirements to federal agency uses of reseller information. In addition, agencies generally lack policies that specifically address these uses.

Mr. Chairmen and Members of the Subcommittees:

I appreciate the opportunity to discuss critical issues surrounding the federal government's purchase of personal information[1] from businesses known as information resellers. As you are aware, the ease and speed with which people's personal information can be collected by information resellers from a wide variety of sources and made available to government and other customers has accelerated with technological advances in recent years. Recent security breaches at large information resellers such as ChoicePoint and LexisNexis have raised questions about how resellers and their federal customers handle people's personal information—especially whether their practices are fully consistent with widely accepted practices for protecting the privacy and security of personal information.

Federal agency use of such information is governed primarily by the Privacy Act of 1974,[2] which requires that the use of personal information be limited to predefined purposes and involve only information germane to those purposes. The provisions of the Privacy Act, in turn, 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.[3] These principles, now widely accepted, include

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

[2] The Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a) provides safeguards against an invasion of privacy through the misuse of records by federal agencies and allows citizens to learn how their personal information is collected, maintained, used, and disseminated by the federal government.

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

1. collection limitation,
2. data quality,
3. purpose specification,
4. use limitation,
5. security safeguards,
6. openness,
7. individual participation, and
8. accountability.[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, New Zealand, and the European Union.

My testimony is based on a report that we are issuing today.[5] In that report, we analyzed fiscal year 2005 contracts and other vehicles for the acquisition of personal information from information resellers by the Departments of Justice, Homeland Security (DHS), and State and the Social Security Administration (SSA). We also compared relevant agency guidelines and management policies and procedures to the Fair Information Practices.

We also identified the extent to which reseller[6] polices and procedures were consistent with the key privacy principles of the Fair Information Practices and assessed the potential effect of any

[4] Descriptions of these principles are shown in table 1.

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

[6] The five information resellers we reviewed were ChoicePoint, LexisNexis, Acxiom, Dun & Bradstreet, and West. Our results may not apply to other resellers who do very little or no business with the federal agencies we reviewed.

inconsistencies. However, we did not attempt to determine whether or how information reseller practices should change. Such determinations are a matter of policy based on balancing the public's right to privacy with the value of services provided by resellers to customers such as government agencies. Our work was performed in accordance with generally accepted government auditing standards.

Today, after a brief summary and a discussion of how the selected agencies use the personal information that they buy from resellers, my remarks will focus on the extent to which the agencies and resellers have policies and practices that reflect the Fair Information Practices.

## Results in Brief

In fiscal year 2005, Justice, DHS, State, and SSA reported that they planned to spend a combined total of approximately $30 million[7] to purchase personal information from resellers. The vast majority—approximately 91 percent—of the planned spending was for purposes of law enforcement (69 percent) or counterterrorism (22 percent). For example, components of the Department of Justice (the largest user of resellers) used the information for criminal investigations, locating witnesses and fugitives, researching assets held by individuals of interest, and detecting fraud in prescription drug transactions. DHS acquired personal information to aid its immigration fraud detection and border screening programs. SSA and State purchased personal information from information resellers to detect and investigate fraud, verify identities, and determine benefit eligibility.

[7] This figure may include uses that do not involve personal information. Except for instances where the reported use was primarily for legal research, agency officials were unable to separate the dollar values associated with use of personal information from uses for other purposes (for example, LexisNexis and West provide news and legal research in addition to public records). The four agencies obtained personal information from resellers primarily through two general-purpose governmentwide contract vehicles—the Federal Supply Schedule of the General Services Administration and the Library of Congress's Federal Library and Information Network.

The major information resellers that do business with the agencies reviewed have measures in place to protect privacy, but the measures are not always fully consistent with the Fair Information Practices. For example, the nature of the information reseller business is largely at odds with the principles of *collection limitation*, *data quality, purpose specification,* and *use limitation*. These principles center on limiting the collection and use of personal information, and they link data quality (for example, accuracy) requirements to these limitations. Resellers said they believe that it may not be appropriate or practical for them to fully adhere to these principles because they do not obtain their information directly from individuals. In fact, the information reseller industry is based on the multi-purpose collection and use of personal information from multiple sources.[8] In many cases, resellers take steps that address aspects of the Fair Information Practices. For example, resellers reported that they have taken steps recently to improve their security safeguards, and they generally inform the public about key privacy principles and policies. However, resellers generally limit the extent to which individuals can gain access to their own personal information and the extent to which inaccurate information contained in reseller databases can be corrected or deleted.

Agency practices for handling personal information acquired from information resellers reflected four of eight principles established by the Fair Information Practices. Agency practices generally reflected the *collection limitation*, *data quality*, *use limitation*, and *security safeguards* principles. For example, law enforcement agencies (including the Federal Bureau of Investigation and the U.S. Secret Service) generally reported that they corroborate information obtained from resellers to ensure that it is accurate when it is used as part of an investigation, reflecting the *data quality* principle that data should be accurate, current, and complete, as needed for the defined purpose. However, agencies did not always have practices for handling reseller information to fully address the *purpose*

[8] In certain circumstances, laws restrict the collection and use of specific kinds of personal information. For example, the Fair Credit Reporting Act regulates access to and use of consumer information under certain circumstances.

*specification*, *individual participation*, *openness,* and *accountability* principles. For example:

- Although agencies notify the public through *Federal Register* notices and published privacy impact assessments that they collect personal information from various sources, they do not always indicate specifically that information resellers are among those sources.
- Some agencies lack robust audit mechanisms to ensure that use of personal information from information resellers is for permissible purposes, reflecting an uneven application of the *accountability* principle.

Contributing to agencies' uneven application of the Fair Information Practices are ambiguities in guidance from OMB on how privacy requirements apply to federal agency uses of reseller information. In addition, agencies generally lack policies that specifically address these uses.

We made recommendations to OMB to revise privacy guidance and to the four agencies to develop specific policies for the use of personal information from resellers, and suggested that Congress consider the extent to which information resellers should adhere to the Fair Information Practices. The five agencies generally agreed with the report and described actions initiated to address our recommendations.

We also obtained comments on excerpts of our draft report from the five information resellers we reviewed. Several resellers raised concerns regarding the version of the Fair Information Practices we used to assess their practices. As discussed in our report, the version of the Fair Information Practices we used has been widely adopted and cited within the federal government as well as internationally. Further, we use it as an analytical framework for identifying potential privacy issues for further consideration by Congress—not as criteria for strict compliance.

# Background

Before advanced computerized techniques, obtaining people's personal information usually required visiting courthouses or other government facilities to inspect paper-based public records, and information contained in product registrations and other business records was not generally available at all. Automation of the collection and aggregation of multiple-source data, combined with the ease and speed of its retrieval, have dramatically reduced the time and effort needed to obtain such information. Information resellers provide services based on these technological advances.

We use the term "information resellers" to refer to businesses that vary in many ways but have in common the fact that they collect and aggregate personal information from multiple sources and make it available to their customers. These businesses do not all focus exclusively on aggregating and reselling personal information. For example, Dun & Bradstreet primarily provides information on commercial enterprises for the purpose of contributing to decision making regarding those enterprises. In doing so, it may supply personal information about individuals associated with those commercial enterprises. To a certain extent, the activities of information resellers may also overlap with the functions of consumer reporting agencies, also known as credit bureaus—entities that collect and sell information about individuals' creditworthiness, among other things. To the extent that information resellers perform the functions of consumer reporting agencies, they are subject to legislation specifically addressing that industry, particularly the Fair Credit Reporting Act.

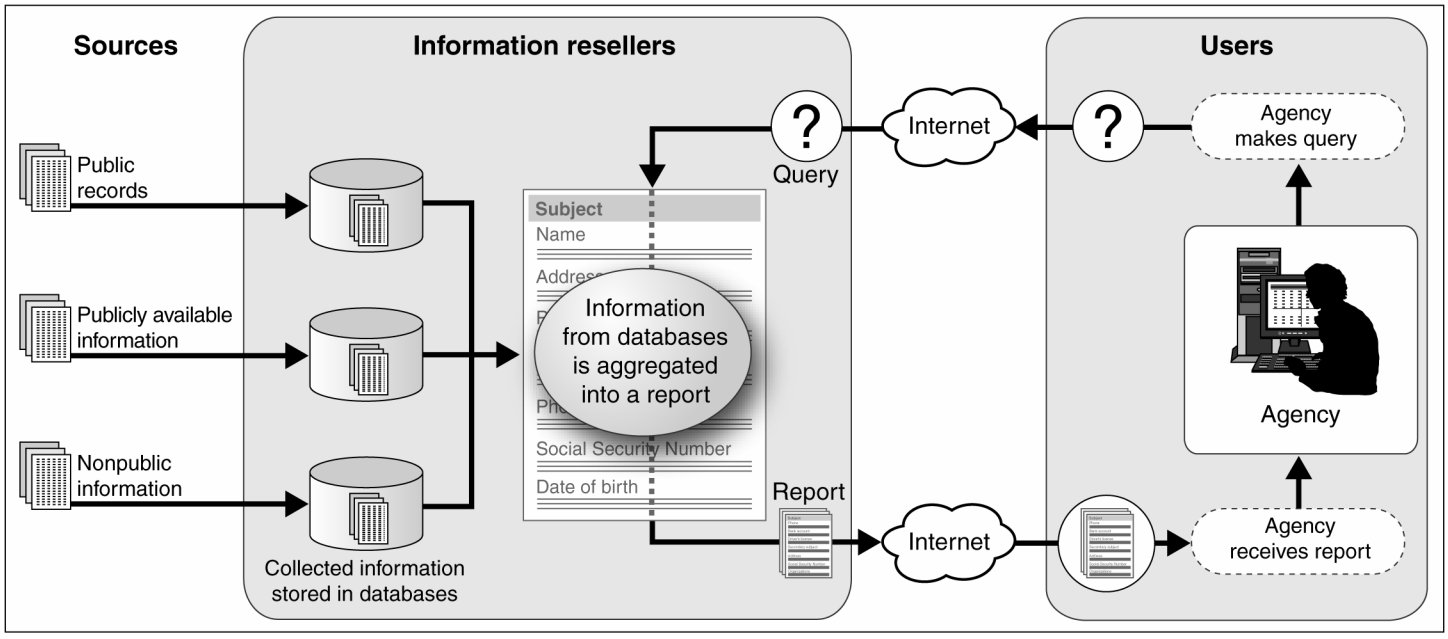
Information resellers have now amassed extensive amounts of personal information about large numbers of Americans. They supply it to customers in both government and the private sector, typically via a centralized online resource. Generally, three types of information are collected:

- *Public records* such as birth and death records, property records, motor vehicle and voter registrations, criminal records, and civil case files.

- *Publicly available information* not found in public records but nevertheless publicly available through other sources, such as telephone directories, business directories, classified ads or magazines, Internet sites, and other sources accessible by the general public.
- *Nonpublic information* derived from proprietary or nonpublic sources, such as credit header data, product warranty registrations, and other application information provided to private businesses directly by consumers.

Figure 1 illustrates how these types of information are collected and aggregated into reports that are ultimately accessed by customers, including government agencies, through contractual agreements.

**Figure 1: Typical Information Flow through Resellers to Government Customers**




Source: GAO analysis of information reseller and agency-provided data.

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

No single federal law governs all use or disclosure of personal information. The major requirements for the protection of personal

privacy by federal agencies come from the Privacy Act of 1974 and the privacy provisions of the E-Government Act of 2002.

Federal use of personal information is governed primarily by the Privacy Act of 1974,[9] which places limitations on agencies' collection, disclosure, and use of personal information maintained in systems of records. The act describes a "record" as any item, collection, or grouping of information about an individual that is maintained by an agency and contains his or her name or another personal identifier. It also defines "system of records" as a group of records under the control of any agency from which information is retrieved by the name of the individual or by an individual identifier. The Privacy Act requires that when agencies establish or make changes to a system of records, they must notify the public by placing a notice in the *Federal Register* identifying, among other things, the type of data collected, the types of individuals about whom information is collected, the intended uses of data, and procedures that individuals can use to review and correct personal information. Additional provisions of the Privacy Act are discussed in the report we are issuing today.

The E-Government Act of 2002 requires that agencies conduct privacy impact assessments (PIA). A PIA is an analysis of how personal information is collected, stored, shared, and managed in a federal system. Under the E-Government Act and related OMB guidance, agencies must conduct PIAs (1) before developing or procuring information technology that collects, maintains, or disseminates information that is in a personally identifiable form; (2) before initiating any new data collections involving personal information that will be collected, maintained, or disseminated using information technology if the same questions are asked of 10 or more people; or (3) when a system change creates new privacy risks, for example, by changing the way in which personal information is being used.

[9] The Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a) provides safeguards against an invasion of privacy through the misuse of records by federal agencies and allows citizens to learn how their personal information is collected, maintained, used, and disseminated by the federal government.

OMB is tasked with providing guidance to agencies on how to implement the provisions of the Privacy Act and the E-Government Act and has done so, beginning with guidance on the Privacy Act, issued in 1975.[10] OMB's guidance on implementing the privacy provisions of the E-Government Act of 2002 identifies circumstances under which agencies must conduct PIAs and explains how to conduct them.

## The Fair Information Practices Are Widely Agreed to Be Key Principles for Privacy Protection

The Privacy Act of 1974 is largely based on a set of internationally recognized principles for protecting the privacy and security of personal information known as the Fair Information Practices. A U.S. government advisory committee first proposed the practices in 1973 to address what it termed a poor level of protection afforded to privacy under contemporary law.[11] The Organization for Economic Cooperation and Development (OECD)[12] developed a revised version of the Fair Information Practices in 1980 that has, with some variation, formed the basis of privacy laws and related policies in many countries, including the United States, Germany, Sweden, Australia, New Zealand, and the European Union.[13] The eight

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

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

[12] 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.

[13] 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).

principles of the OECD Fair Information Practices are shown in table 1.

**Table 1: The OECD 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: OECD.

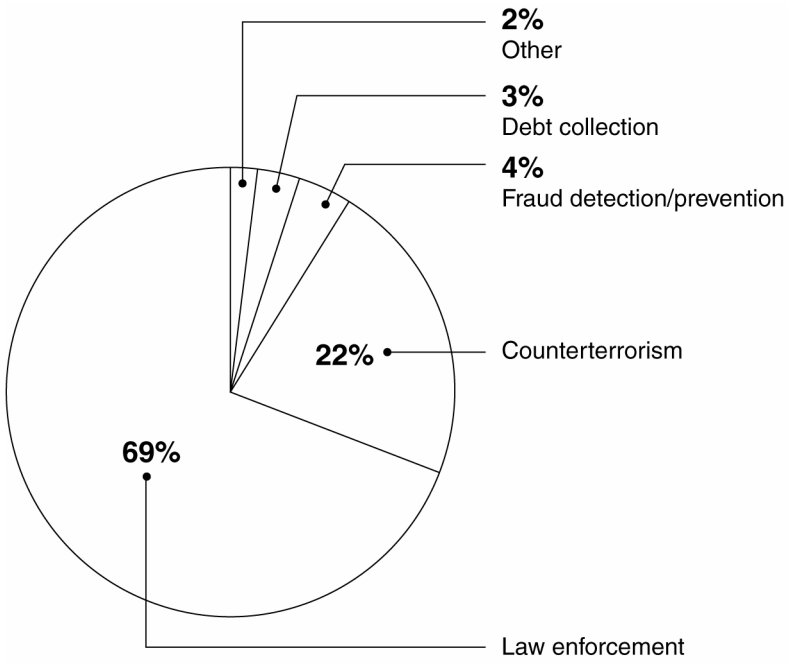
The Fair Information Practices are not precise legal requirements. Rather, they provide a framework of principles for balancing the need for privacy with other public policy interests, such as national security, law enforcement, and administrative efficiency. Ways to strike that balance vary among countries and according to the type of information under consideration.

## Agencies Use Governmentwide Contracts to Obtain Personal Information from Information Resellers for a Variety of Purposes

The Departments of Justice, Homeland Security, State, and the Social Security Administration reported approximately $30 million in contractual arrangements with information resellers in fiscal year 2005.[14] The agencies reported using personal information obtained from resellers for a variety of purposes including law enforcement, counterterrorism, fraud detection/prevention, and debt collection. In all, approximately 91 percent of agency uses of reseller data were in the categories of law enforcement (69 percent) or counterterrorism (22 percent). Figure 2 details contract values categorized by their reported use.

[14] This figure comprises contracts and task orders with information resellers that included the acquisition and use of personal information. However, some of these funds may have been spent on uses that do not involve personal information; we could not omit all such uses because agency officials were not always able to separate the amounts associated with use of personal information from those for other uses (for example, LexisNexis and West provide news and legal research in addition to public records). In some instances, where the reported use was primarily for legal research, we omitted these funds from the total.

**Figure 2: Fiscal Year 2005 Contractual Vehicles Enabling the Use of Personal Information from Information Resellers, Categorized by Reported Use**




Source: GAO analysis of agency-provided data.

The Department of Justice, which accounted for about 63 percent of the funding, mostly used the data for law enforcement and counterterrorism. DHS also used reseller information primarily for law enforcement and counterterrorism. State and SSA reported acquiring personal information from information resellers for fraud prevention and detection, identity verification, and benefit eligibility determination.

## Justice and DHS Use Information Resellers Primarily for Law Enforcement and Counterterrorism

In fiscal year 2005, the Department of Justice and its components reported approximately $19 million in acquisitions from a wide variety of information resellers, primarily for purposes related to law enforcement (75 percent) and counterterrorism (18 percent). The Federal Bureau of Investigation (FBI), which is Justice's largest user of information resellers, uses reseller information to, among other things, analyze intelligence and detect terrorist activities in

support of ongoing investigations by law enforcement agencies and the intelligence community. In this capacity, resellers provide the FBI's Foreign Terrorist Tracking Task Force with names, addresses, telephone numbers, and other biographical and demographical information as well as legal briefs, vehicle and boat registrations, and business ownership records. [15]

The Drug Enforcement Administration (DEA), the second largest Justice user of information resellers in fiscal year 2005, obtains reseller data primarily to detect fraud in prescription drug transactions.[16] Agents use reseller data to detect irregular prescription patterns for specific drugs and trace this information to the pharmacy and prescribing doctor.[17]

DHS and its components reported that they used information reseller data in fiscal year 2005 primarily for law enforcement purposes, such as developing leads on subjects in criminal investigations and detecting fraud in immigration benefit applications (part of enforcing the immigration laws). DHS's largest investigative component, the U.S. Immigration and Customs Enforcement, is also its largest user of personal information from resellers. It collects data such as address and vehicle information for criminal investigations and background security checks. U.S. Customs and Border Protection conducts queries on people, businesses, property, and corresponding links via a secure Internet connection. The Federal Emergency Management Agency uses an information reseller to detect fraud in disaster assistance applications.

DHS also reported using information resellers in its counterterrorism efforts. For example, the Transportation Security Administration (TSA) used data obtained from information resellers

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

[16] DEA's mission involves enforcing laws pertaining to the manufacture, distribution, and dispensing of legally produced controlled substances.

[17] The personal information contained in this information reseller database is limited to the prescribing doctor and does not contain personal patient information.

as part of a test associated with the development of its domestic passenger prescreening program, called "Secure Flight."[18] TSA plans for Secure Flight to compare domestic flight reservation information submitted to TSA by aircraft operators with federal watch lists of individuals known or suspected of activities related to terrorism.

## SSA and State Use Information Resellers Primarily for Fraud Prevention and Detection

In an effort to ensure the accuracy of Social Security benefit payments, the Social Security Administration and its components reported approximately $1.3 million in contracts with information resellers in fiscal year 2005 for purposes relating to fraud prevention (such as skiptracing),[19] confirming suspected fraud related to workers compensation payments, obtaining information on criminal suspects for follow-up investigations, and collecting debts. For example, the Office of the Inspector General (OIG), the largest user of information reseller data at SSA, uses several information resellers to assist investigative agents in detecting benefit abuse by Social Security claimants and to assist agents in locating claimants. Regional office agents may also use reseller data in investigating persons suspected of claiming disability fraudulently.

The Department of State and its components reported approximately $569,000 in contracts with information resellers for fiscal year 2005, mainly to support investigations of passport-related activities. For example, several components accessed personal information to validate familial relationships, birth and identity data, and other information submitted on immigrant and nonimmigrant visa petitions. State also uses reseller data to investigate passport and visa fraud cases.

[18] For an assessment of privacy issues associated with the Secure Flight commercial data test, see GAO, *Aviation Security: Transportation Security Administration Did Not Fully Disclose Uses of Personal Information during Secure Flight Program Testing in Initial Privacy Notices, but Has Recently Taken Steps to More Fully Inform the Public*, GAO-05-864R (Washington, D.C.: July 22, 2005).

[19] Skiptracing is the process of locating people who have fled in order to avoid paying debts.

## Resellers Take Steps to Protect Privacy, but These Measures Are Not Fully Consistent With the Fair Information Practices

Although the information resellers that do business with the federal agencies we reviewed have taken steps to protect privacy, these measures were not fully consistent with the Fair Information Practices. Most significantly, the first four principles, relating to *collection limitation*, *data quality, purpose specification,* and *use limitation*, are largely at odds with the nature of the information reseller business. These principles center on limiting the collection and use of personal information and require data accuracy based on that limited purpose and limited use of the information. However, the information reseller industry presupposes that the collection and use of personal information is not limited to specific purposes, but instead can be made available to multiple customers for multiple purposes. Resellers make it their business to collect large amounts of personal information[20] and to combine that information in new ways so that it serves purposes other than those for which it was originally collected. Further, they are limited in their ability to ensure the accuracy, currency, or relevance of their holdings, because these qualities may vary based on customers' varying uses.

Information reseller policies and procedures were consistent with aspects of the remaining four Fair Information Practices. Large resellers reported implementing a variety of security safeguards, such as stringent customer credentialing, to improve protection of personal information. Resellers also generally provided public notice of key aspects of their privacy policies and practices (relevant to the *openness* principle), and reported taking actions to ensure internal compliance with their own privacy policies (relevant to the *accountability* principle). However, while information resellers generally allow individuals limited access to their personal information, they generally limit the opportunity to correct or delete

[20]Resellers are constrained from collecting certain types of information and aggregating it with other personal information. For example, the Fair Credit Reporting Act and the Gramm-Leach-Bliley Act constrain the collection and use of personal information, such as financial information.

inaccurate information contained in reseller databases (relevant to the *individual participation* principle).

In brief, reseller practices compare with the Fair Information Practices as follows:

*Collection limitation*. Resellers do not limit collections to specific purposes but collect large amounts of personal information. In practice, resellers are limited in the personal information that they can obtain by laws that apply to specific kinds of information (for example, the Fair Credit Reporting Act and the Gramm-Leach-Bliley Act, which restrict the collection, use, and disclosure of certain consumer and financial data). However, beyond specific legal restrictions, information resellers generally attempt to aggregate large amounts of personal information so as to provide useful information to a broad range of customers. Resellers do not make provisions to notify the individuals involved when they obtain personal data from their many sources, including public records. Concomitantly, individuals are not afforded an opportunity to express or withhold their consent when the information is collected. Resellers said they believe it is not appropriate or practical for them to provide notice or obtain consent from individuals because they do not collect information directly from them.

Under certain conditions, some information resellers offer consumers an "opt-out" option—that is, individuals may request that information about themselves be suppressed from selected databases. However, resellers generally offer this option only with respect to certain types of information, such as marketing products, and only under limited circumstances, such as if the individual is a law enforcement officer or a victim of identity theft. Two resellers stated their belief that under certain circumstances it may not be appropriate to provide consumers with opportunities for opting out, such as when information products are designed to detect fraud or locate criminals. These resellers stated that if individuals were permitted to opt out of fraud prevention databases, some of those opting out could be criminals, which would undermine the effectiveness and utility of these databases.

*Data quality*. Information resellers reported taking steps to ensure that they generally receive accurate data from their sources and that they do not introduce errors in the process of transcribing and aggregating information. However, they generally provide their customers with exactly the same data they obtain and do not claim or guarantee that the information is accurate for a specific purpose. Some resellers' privacy policies state that they expect their data to contain some errors. Further, resellers varied in their policies regarding correction of data determined to be inaccurate as obtained by them. One reseller stated that it would delete information in its databases that was found to be inaccurate. Another stated that even if an individual presents persuasive evidence that certain information is in error, the reseller generally does not make changes if the information comes directly from an official public source (unless instructed to do so by that source). Because they are not the original source of the personal information, information resellers generally direct individuals to the original sources to correct any errors. Several resellers stated that they would correct any identified errors introduced through their own processing and aggregation of data.

*Purpose specification*. While information resellers specify purpose in a general way by describing the types of businesses that use their data, they generally do not designate specific intended uses for each of their data collections. Resellers generally obtain information that has already been collected for a specific purpose and make that information available to their customers, who in turn have a broader variety of purposes for using it. For example, personal information originally submitted by a customer to register a product warranty could be obtained by a reseller and subsequently made available to another business or government agency, which might use it for an unrelated purpose, such as identity verification, background checking, or marketing. It is difficult for resellers to provide greater specificity because they make their data available to many customers for a wide range of legitimate purposes. As a result, the public is made aware only of the broad range of potential uses to which their personal information may be put, rather than a specific use, as envisioned in the Fair Information Practices.

*Use limitation*. Because information reseller purposes are specified very broadly, it is difficult for resellers to ensure that use of the information in their databases is limited. As previously discussed, information reseller data may have many different uses, depending on the types of customers involved. However, resellers do take steps to ensure that their customers' use of personal information is limited to legally sanctioned purposes. Information resellers pass this responsibility to their customers through licensing agreements and contract terms and agreements. Customers are usually required to certify that they will only use information obtained from the reseller in ways permissible under laws such as the Gramm-Leach-Bliley Act and the Driver's Privacy Protection Act. The information resellers used by the federal agencies we reviewed generally also reported taking steps to ensure that access to certain sensitive types of personally identifiable information—particularly Social Security numbers—is limited to certain customers and uses.

*Security safeguards*. While we did not evaluate the effectiveness of resellers' information security programs, resellers we spoke with said they employ various safeguards to protect consumers' personal information. They implemented these safeguards in part for business reasons but also because federal laws require such protections. Resellers describe these safeguards in various policy statements, such as online and data privacy policies or privacy statements posted on Internet sites. Given recent incidents, large information resellers also reported having recently taken steps to improve their safeguards against unauthorized access. Two resellers reported that they had taken steps to improve their procedures for authorizing customers to have access to sensitive information, such as Social Security numbers. For example, one reseller established a credentialing task force with the goal of centralizing its customer credentialing process. In addition to enhancing safeguards on customer access authorizations, resellers have instituted a variety of other security controls. For example, three large information resellers have implemented physical safeguards at their data centers, such as continuous monitoring of employees entering and exiting facilities, monitoring of activity on customer accounts, and strong authentication of users entering and exiting secure areas within the data centers.

*Openness*. To address openness, information resellers took steps to inform the public about key aspects of their privacy policies. They used means such as company Web sites and brochures to inform the public of specific policies and practices regarding the collection and use of personal information. Reseller Web sites also generally provided information about the types of information products the resellers offered—including product samples—as well as general descriptions about the types of customers served.

*Individual participation*. Although information resellers allow individuals access to their personal information, this access is generally limited. Resellers may provide an individual a report containing certain types of information—such as compilations of public records information—however, the report may not include all information maintained by the resellers about that individual. Further, because they obtain their information from other sources, most resellers have limited provisions for correcting or deleting inaccurate information contained in their databases. If individuals find inaccuracies in such reports, they generally cannot have these corrected by the resellers.[21] Resellers, as a matter of policy, do not make corrections to data obtained from other sources, even if the individual provides evidence that the data are wrong. Instead, they direct individuals wishing to make corrections to contact the original sources of the data. Several resellers stated that they would correct any identified errors resulting from their own processing and aggregation of data (for example, transposing numbers or letters or incorrectly aggregating information).

*Accountability*. Although information resellers' overall application of the Fair Information Practices varied, each reseller we spoke with reported actions to ensure compliance with its own privacy policies. For example, resellers reported designating chief privacy officers to monitor compliance with internal privacy policies and applicable laws. Information resellers reported that these officials had a range

[21] One reseller reported that, for certain products, it will delete information that has been identified as inaccurate. For example, if the reseller is able to verify that data contained within its directory or fraud products are inaccurate, it will delete the inaccurate data and keep a record of this in a maintenance file so the erroneous data are not reentered at a future date.

of responsibilities aimed at ensuring accountability for privacy policies, such as establishing consumer access and customer credentialing procedures, monitoring compliance with federal and state laws, and evaluating new sources of data (for example, cell phone records). Although there are no industrywide standards requiring resellers to conduct periodic audits of their compliance with privacy policies, one information reseller reported using a third party to conduct privacy audits on an annual basis. Using a third party to audit compliance with privacy policies further helps to ensure that an information reseller is accountable for the implementation of its privacy practices.

In commenting on excerpts of our draft report, several resellers raised concerns regarding the version of the Fair Information Practices we used to assess their practices, stating their view that it applied more appropriately to organizations that collect information directly from consumers and that they were not legally bound to adhere to the Fair Information Practices. As discussed in our report, the version of the Fair Information Practices we used has been widely adopted and cited within the federal government as well as internationally. Further, we use it as an analytical framework for identifying potential privacy issues for further consideration by Congress—not as criteria for strict compliance. Resellers also stated that the draft did not take into account their view that public record information is open to all for any use not prohibited by state or federal law. However, we believe it is not clear that individuals give up all privacy rights to personal information contained in public records, and we believe it is important to assess the status of privacy protections for all personal information being offered commercially to the government so that informed policy decisions can be made about the appropriate balance between resellers' services and the public's right to privacy. In our report we suggest that Congress consider the extent to which information resellers should adhere to the Fair Information Practices.

## Agencies Lack Policies on Use of Reseller Data, and Practices Do Not Consistently Reflect the Fair Information Practices

Agencies generally lacked policies that specifically address their use of personal information from commercial sources (although DHS Privacy Office officials have reported that they are drafting such a policy), and agency practices for handling personal information acquired from information resellers did not always fully reflect the Fair Information Practices. Specifically, agency practices generally reflected four of the eight Fair Information Practices.

As table 2 shows, the *collection limitation*, *data quality*, *use limitation*, and *security safeguards* principles were generally reflected in agency practices. For example, several agency components (specifically, law enforcement agencies such as the FBI and the U.S. Secret Service) reported that in practice, they generally corroborate information obtained from resellers when it is used as part of an investigation. This practice is consistent with the principle of *data quality*.

Agency policies and practices with regard to the other four principles were uneven. Specifically, agencies did not always have policies or practices in place to address the *purpose specification*, *openness,* and *individual participation* principles with respect to reseller data. The inconsistencies in applying these principles as well as the lack of specific agency policies can be attributed in part to ambiguities in OMB guidance regarding the applicability of the Privacy Act to information obtained from resellers. Further, privacy impact assessments, a valuable tool that could address important aspects of the Fair Information Practices, are not conducted often. Finally, components within each of the four agencies did not consistently hold staff accountable by monitoring usage of personal information from information resellers and ensuring that it was appropriate; thus, their application of the *accountability* principle was uneven.

**Table 2: Application of Fair Information Practices to the Reported Handling of Personal Information from Data Resellers at Four Agencies**

| Principle | Agency application of principle | Agency practices |
|---|---|---|
| *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. | General | Agencies limited personal data collection to individuals under investigation or their associates. |
| *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. | General | Agencies corroborated information from resellers and did not take actions based exclusively on such information. |
| *Purpose specification*. The purpose 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 that purpose and compatible purposes. | Uneven | Agency system of records notices did not generally reveal that agency systems could incorporate information from data resellers. Agencies also generally did not conduct privacy impact assessments for their systems or programs that involve use of reseller data. |
| *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. | General | Agencies generally limited their use of personal information to specific investigations (including law enforcement, counterterrorism, fraud detection, and debt collection). |
| *Security safeguards*. Personal information should be protected with reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification, or disclosure. | General | Agencies had security safeguards such as requiring passwords to access databases, basing access rights on need to know, and logging search activities (including "cloaked logging," which prevents the vendor from monitoring search content). |
| *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. | Uneven | See *Purpose specification* above. Agencies did not have established policies specifically addressing the use of personal information obtained from resellers. |
| *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. | Uneven | See *Purpose specification* above. Because agencies generally did not disclose their collections of personal information from resellers, individuals were often unable to exercise these rights. |
| *Accountability*. Individuals controlling the collection or use of personal information should be accountable for taking steps to ensure the implementation of these principles. | Uneven | Agencies do not generally monitor usage of personal information from information resellers to hold users accountable for appropriate use; instead, they rely on users to be responsible for their behavior. For example, agencies may instruct users in their responsibilities to use personal information appropriately, have them sign statements of responsibility, and have them indicate what permissible purpose a given search fulfills. |

**Legend:**

General = policies or procedures to address all major aspects of a particular principle.

Uneven = policies or procedures addressed some but not all aspects of a particular principle or some but not all agencies and components had policies or practices in place addressing the principle.

Source: GAO analysis of agency-supplied data.

Note: We did not independently assess the effectiveness of agency information security programs. Our assessment of overall agency application of the Fair Information Practices was based on the policies and management practices described by the Department State and SSA as a whole and by major components of Justice and DHS. We did not obtain information on smaller components of Justice and DHS.

Agency procedures generally reflected the *collection limitation*, *data quality*, *use limitation*, and *security safeguards* principles. Regarding collection limitation, for most law-enforcement and counterterrorism purposes (which accounted for 90 percent of usage in fiscal year 2005), agencies generally limited their personal data collection in that they reported obtaining information only on specific individuals under investigation or associates of those individuals. Regarding *data quality*, agencies reported taking steps to mitigate the risk of inaccurate information reseller data by corroborating information obtained from resellers. Agency officials described the practice of corroborating information as a standard element of conducting investigations. Likewise, for non-law-enforcement use, such as debt collection and fraud detection and prevention, agency components reported that they mitigated potential problems with the accuracy of data provided by resellers by obtaining additional information from other sources when necessary. As for *use limitation*, agency officials said their use of reseller information was limited to distinct purposes, which were generally related to law enforcement or counterterrorism. Finally, while we did not assess the effectiveness of information security at any of these agencies, we found that all four had measures in place intended to safeguard the security of personal information obtained from resellers.[22]

[22] Although we did not assess the effectiveness of information security 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, including Justice, DHS, State, and SSA. For additional information see GAO, *Information Security: Weaknesses Persist at Federal Agencies Despite Progress Made in Implementing Related Statutory Requirements*, GAO-05-552 (Washington, D.C.: July 15, 2005) and *Information Security: Department of Homeland Security Needs to Fully Implement Its Security Program*, GAO-05-700 (Washington, D.C.: June 17, 2005).

## Limitations in the Applicability of the Privacy Act and Ambiguities in OMB Guidance Contribute to an Uneven Adherence to the *Purpose Specification*, *Openness*, and *Individual Participation* Principles

The *purpose specification, openness*, and *individual participation* principles stipulate that individuals should be made aware of the purpose and intended uses of the personal information being collected about them, and, if necessary, have the ability to access and correct their information. These principles are reflected in the Privacy Act requirement for 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.[23]

In a number of cases, agencies using reseller information did not adhere to the *purpose specification* or *openness* principles in that they did not notify the public that they were using such information and did not specify the purpose for their data collections. Agency officials said that they generally did not prepare system-of-records notices that would address these principles because they were not required to do so by the Privacy Act. The act's vehicle for public notification—the system-of-records notice—becomes binding on an agency only when the agency collects, maintains, and retrieves personal data in the way defined by the act or when a contractor does the same thing explicitly on behalf of the government. Agencies generally did not issue system-of-records notices specifically for their use of information resellers largely because information reseller databases were not considered "systems of records operated by or on behalf of a government agency" and thus were not considered subject to the provisions of the Privacy Act.[24] OMB guidance on implementing the Privacy Act does not

[23] 5 U.S.C. § 552a(e)(4)(C) & (I). The Privacy Act allows agencies to claim an exemption from identifying the categories of sources of records for records compiled for criminal law enforcement purposes, as well as for a broader category of investigative records compiled for criminal or civil law enforcement purposes.

[24] The act provides for its requirements to apply to government contractors when agencies contract for the operation by or on behalf of the agency, a system of records to accomplish an agency function. 5 U.S.C. § 552a(m).

specifically refer to the use of reseller data or how it should be treated. According to OMB and other agency officials, information resellers operate their databases for multiple customers, and federal agency use of these databases does not amount to the operation of a system of records on behalf of the government. Further, agency officials stated that merely querying information reseller databases did not amount to agency "maintenance" of the personal information being queried and thus also did not trigger the provisions of the Privacy Act. In many cases, agency officials considered their use of resellers to be of this type—essentially "ad hoc" querying or "pinging" of reseller databases for personal information about specific individuals, which they believed they were not doing in connection with a formal system of records.

In other cases, however, agencies maintained information reseller data in systems for which system-of-records notices had been previously published. For example, law enforcement agency officials stated that, to the extent they retain the results of reseller data queries, this collection and use is covered by the system of records notices for their case file systems. However, in preparing such notices, agencies generally did not specify that they were obtaining information from resellers. Among system of records notices that were identified by agency officials as applying to the use of reseller data, only one—TSA's system of records notice for the test phase of its Secure Flight program—specifically identified the use of information reseller data.[25]

In several of these cases, agency sources for personal information were described only in vague terms, such as "private organizations," "other public sources," or "public source material," when information was being obtained from information resellers.

The inconsistency with which agencies specify resellers as a source of information in system-of-records notices is due in part to

[25] As we previously reported, this notice did not fully disclose the scope of the use of reseller data during the test phase. See GAO, *Aviation Security: Transportation Security Administration Did Not Fully Disclose Uses of Personal Information during Secure Flight Program Testing in Initial Privacy Notices, but Has Recently Taken Steps to More Fully Inform the Public*, GAO-05-864R (Washington, D.C.: July 22, 2005).

ambiguity in OMB guidance, which states that "for systems of records which contain information obtained from sources other than the individual to whom the records pertain, the notice should list the types of sources used."[26] Although the guidance is unclear what would constitute adequate disclosure of "types of sources," OMB and DHS Privacy Office officials agreed that to the extent that reseller data is subject to the Privacy Act, agencies should specifically identify information resellers as a source and that merely citing public records information does not sufficiently describe the source.

Aside from certain law enforcement exemptions[27] to the Privacy Act, adherence to the *purpose specification* and *openness* principles is critical to preserving a measure of individual control over the use of personal information. Without clear guidance from OMB or specific policies in place, agencies have not consistently reflected these principles in their collection and use of reseller information. As a result, without being notified of the existence of an agency's information collection activities, individuals have no ability to know that their personal information could be obtained from commercial sources and potentially used as a basis, or partial basis, for taking action that could have consequences for their welfare.

## Privacy Impact Assessments Could Address Openness and Purpose Specification Principles but Often Are Not Conducted

PIAs can be an important tool to help agencies to address *openness and purpose specification* principles early in the process of developing new information systems. To the extent that PIAs are

[26] OMB, "Privacy Act Implementation: Guidelines and Responsibilities," *Federal Register,* Volume 40, Number 132, Part III, p. 28964 (Washington, D.C.: July 9, 1975).

[27] The Privacy Act allows agencies to claim exemptions if the records are used for certain purposes. 5 U.S.C. § 552a (j) and (k). For example, records compiled 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. In most cases where officials identified system-of-record notices associated with reseller data collection for law enforcement purposes, agencies claimed this exemption.

made publicly available,[28] they provide explanations to the public about such things as the information that will be collected, why it is being collected, how it is to be used, and how the system and data will be maintained and protected.

However, few agency components reported developing PIAs for their systems or programs that make use of information reseller data. As with system-of-records notices, agencies often did not conduct PIAs because officials did not believe they were required. Current OMB guidance on conducting PIAs is not always clear about when they should be conducted. According to guidance from OMB, a PIA is required by the E-Government Act when agencies "systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources."[29] However, the same guidance also instructs agencies that "merely querying a database on an ad hoc basis does not trigger the PIA requirement." Reported uses of reseller data were generally not described as a "systematic" incorporation of data into existing information systems; rather, most involved querying a database and in some cases retaining the results of these queries. OMB officials stated that agencies would need to make their own judgments on whether retaining the results of searches of information reseller databases constituted a "systematic incorporation" of information.

The DHS Privacy Office[30] has been working to clarify guidance on the use of reseller information in general as well as the specific requirements for conducting PIAs. DHS recently issued guidance

[28] The E-Government Act requires agencies, if practicable, to make privacy impact assessments publicly available through agency Web sites, publication in the *Federal Register*, or by other means. Pub. L. No. 107-347, § 208 (b)(1)(B)(iii).

[29] OMB, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, Memorandum M-03-22 (Washington, D.C.: Sept. 26, 2003).

[30] The DHS Privacy Officer position was created by the Homeland Security Act of 2002, Pub. L. No 107-296, § 222, 116 Stat. 2155. The Privacy Officer is responsible for, among other things, "assuring that the use of technologies sustain[s], and do[es] not erode privacy protections relating to the use, collection, and disclosure of personal information, and assuring that personal information contained in Privacy Act systems of records is handled in full compliance with Fair Information Practices as set out in the Privacy Act of 1974."

requiring PIAs to be conducted whenever reseller data are involved. However, although the DHS guidance clearly states that PIAs are required when personally identifiable information is obtained from a commercial source, it also states that "merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement."[31] Like OMB's guidance, the DHS guidance is not clear, because agency personnel are left to make individual determinations as to whether queries are "on an ad hoc basis."

Until PIAs are conducted more thoroughly and consistently, the public is likely to remain incompletely informed about agency purposes and uses for obtaining reseller information.

In our report we recommended that the Director, OMB, revise privacy guidance to clarify the applicability of requirements for public notices and privacy impact assessments to agency use of personal information from resellers and direct agencies to review their uses of such information to ensure it is explicitly referenced in privacy notices and assessments. Further, we recommended that agencies develop specific policies for the use of personal information from resellers.

## Agencies Often Did Not Have Practices in Place to Ensure Accountability for Proper Handling of Information Reseller Data

According to the *accountability* principle, individuals controlling the collection or use of personal information should be accountable for ensuring the implementation of the Fair Information Practices. This means that agencies should take steps to ensure that they use personal information from information resellers appropriately.

Agencies described using activities to oversee their use of reseller information that were largely based on trust in the individual user to use the information appropriately, rather than management oversight of usage details. For example, in describing controls placed on the use of commercial data, officials from component

[31] Department of Homeland Security Privacy Office, *Privacy Impact Assessments: Official Guidance* (March 2006), p. 34.

agencies identified measures such as instructing users that reseller data are for official use only, and requiring users to sign statements attesting 1) to their need to access information reseller databases and 2) that their use will be limited to official business. Additionally, agency officials reported that their users are required to select from a list of vendor-defined "permissible purposes" (for example, law enforcement, transactions authorized by the consumer) before conducting a search on reseller databases.

While these practices appear consistent with the accountability principle, they are focused on individual user responsibility instead of monitoring and oversight. Agencies did not have practices in place to obtain reports from resellers that would allow them to monitor usage of reseller databases at a detailed level. Although agencies generally receive usage reports from the information resellers, these reports are designed primarily for monitoring costs. Further, these reports generally contained only high-level statistics on the number of searches and databases accessed, not the contents of what was actually searched, thus limiting their utility in monitoring usage.

To the extent that federal agencies do not implement methods such as user monitoring or auditing of usage records, they provide limited accountability for their usage of information reseller data and have limited assurance that the information is being used appropriately.

In summary, services provided by information resellers are important to federal agency functions such as law enforcement and fraud protection and identification. Resellers have practices in place to protect privacy, but these practices are not fully consistent with the Fair Information Practices, which resellers are not legally required to follow. Among other things, resellers collect large amounts of information about individuals without their knowledge or consent, do not ensure that the data they make available are accurate for a given purpose, and generally do not make corrections to the data when errors are identified by individuals. Information resellers believe that application of the relevant principles of the Fair Information Practices is inappropriate or impractical in these

situations. However, given that reseller data may be used for a variety of purposes, determining the appropriate degree of control or influence individuals should have over the way in which their personal information is obtained and used—as envisioned in the Fair Information Practices—is critical. As Congress weighs various legislative options, adherence to the Fair Information Practices will be an important consideration in determining the appropriate balance between the services provided by information resellers to customers such as government agencies and the public's right to privacy.

While agencies take steps to adhere to Fair Information Practices such as the *collection limitation*, *data quality*, *use limitation*, and *security safeguards* principles, they have not taken all the steps they could to reflect others—or to comply with specific Privacy Act and e-Government Act requirements—in their handling of reseller data. Because OMB privacy guidance does not clearly address information reseller data, agencies are left largely on their own to determine how to satisfy legal requirements and protect privacy when acquiring and using reseller data. Without current and specific guidance, the government risks continued uneven adherence to important, well-established privacy principles and lacks assurance that the privacy rights of individuals are adequately protected.

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

## Contacts and Acknowledgements

If you have any questions concerning this testimony, please contact Linda Koontz, Director, Information Management, at (202) 512-6240, or koontzl@gao.gov. Other individuals who made key contributions to this testimony were Mathew Bader, Barbara Collier, John de Ferrari, Pamlutricia Greenleaf, David Plocher, Jamie Pressman, and Amos Tevelow.

## GAO's Mission

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

## Obtaining Copies of GAO Reports and Testimony

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

## Order by Mail or Phone

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

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

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

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

## Congressional Relations

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

## Public Affairs

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