

April 2006

PERSONAL  
INFORMATION

Agency and Reseller  
Adherence to Key  
Privacy Principles



G A O

Accountability \* Integrity \* Reliability



Highlights of [GAO-06-421](#), a report to congressional committees

## Why GAO Did This Study

Federal agencies collect and use personal information for various purposes, both directly from individuals and from other sources, including information resellers—companies that amass and sell data from many sources. In light of concerns raised by recent security breaches involving resellers, GAO was asked to determine how the Departments of Justice, Homeland Security, and State and the Social Security Administration use personal data from these sources. In addition, GAO reviewed 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

The Congress should consider the extent to which resellers should adhere to the Fair Information Practices. In addition, GAO is making recommendations to OMB 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 this report. Resellers questioned the applicability of the Fair Information Practices, especially with regard to public records.

[www.gao.gov/cgi-bin/getrpt?GAO-06-421](http://www.gao.gov/cgi-bin/getrpt?GAO-06-421).

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](mailto:koontzl@gao.gov).

## PERSONAL INFORMATION

# Agency and Reseller Adherence to Key Privacy Principles

## 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. Components of the Department of Justice (the largest user of resellers) used such information in performing criminal investigations, locating witnesses and fugitives, researching assets held by individuals of interest, and detecting prescription drug fraud. The Department of Homeland Security used reseller information for immigration fraud detection and border screening programs. Uses by the Social Security Administration and the Department of State were to prevent and detect fraud, verify identity, and determine eligibility for benefits. 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 we 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 presupposes that personal information can be made available to multiple customers and for multiple purposes. Resellers said they 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, some of these principles were mirrored in agency practices, but for others, agency practices were uneven. For example, although agencies issued public notices on information collections, these did not always notify the public that information resellers were among the sources to be used. 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 (OMB) regarding the applicability of privacy requirements to federal agency uses of reseller information. In addition, agencies generally lack policies that specifically address these uses.

---

# Contents

---

---

## Letter

Results in Brief	1
Background	4
Using Governmentwide Contracts, Federal Agencies Obtain Personal Information from Information Resellers for a Variety of Purposes	7
Resellers Take Steps to Protect Privacy, but These Measures Are Not Fully Consistent with the Fair Information Practices	19
Agencies Lack Policies on Use of Reseller Data, and Practices Do Not Consistently Reflect the Fair Information Practices	37
Conclusions	49
Matter for Congressional Consideration	62
Recommendations for Executive Action	63
Agency Comments and Our Evaluation	63
Comments from Information Resellers	64
	66

---

## Appendixes

<b>Appendix I: Objectives, Scope, and Methodology</b>	70
<b>Appendix II: Federal Laws Affecting Information Resellers</b>	74
Gramm-Leach-Bliley Act	74
Health Insurance Portability and Accountability Act	76
Fair Credit Reporting Act	77
Fair and Accurate Credit Transactions Act	78
<b>Appendix III: Comments from the Department of Justice</b>	79
<b>Appendix IV: Comments from the Department of Homeland Security</b>	81
<b>Appendix V: Comments from the Social Security Administration</b>	83
<b>Appendix VI: Comments from the Department of State</b>	85

---

## Tables

Table 1: Federal Laws Addressing Private Sector Disclosure of Personal Information	15
Table 2: The OECD Fair Information Practices	16
Table 3: Reported Uses of Personal Information: Department of Justice Contracts with Information Resellers, Fiscal Year 2005	24
Table 4: Reported Uses of Personal Information: DHS Contracts with Information Resellers, Fiscal Year 2005	29
Table 5: Reported Uses of Personal Information: SSA Contracts with Information Resellers, Fiscal Year 2005	32

---

Table 6: Reported Uses of Personal Information: Department of State Contracts with Information Resellers, Fiscal Year 2005	34
Table 7: Information Resellers' Application of Principles of the Fair Information Practices	38
Table 8: Application of Fair Information Practices to the Reported Handling of Personal Information from Data Resellers at Four Agencies	50

---

## Figures

Figure 1: Typical Information Flow through Resellers to Government Customers	10
Figure 2: Fiscal Year 2005 Contractual Vehicles Enabling the Use of Personal Information from Information Resellers, Categorized by Reported Use	20
Figure 3: Total Dollar Values, Categorized by Agency, of Fiscal Year 2005 Acquisition of Personal Information from Information Resellers	35

---

**Abbreviations**

APEC	Asia-Pacific Economic Cooperation
ATF	Bureau of Alcohol, Tobacco, Firearms, and Explosives
CBP	Customs and Border Protection
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
FBI	Federal Bureau of Investigation
FEDLINK	Federal Library and Information Network
FEMA	Federal Emergency Management Agency
FISMA	Federal Information Security Management Act
FTTTF	Foreign Terrorist Tracking Task Force
GSA	General Services Administration
ICE	Immigration and Customs Enforcement
OECD	Organization for Economic Cooperation and Development
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PIA	privacy impact assessment
SSA	Social Security Administration
TSA	Transportation Security Administration
USCIS	Citizenship and Immigration Services

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



April 4, 2006

Congressional Committees:

Recent security breaches at large information resellers, such as ChoicePoint and LexisNexis, have highlighted the extent to which such companies collect and disseminate personal information.<sup>1</sup> Information resellers are companies that collect information, including personal information about consumers, from a wide variety of sources for the purpose of reselling such information to their customers, which include both private-sector businesses and government agencies. Before advanced computerized techniques made aggregating and disseminating such information relatively easy, much personal information was less accessible, being stored in paper-based public records at courthouses and other government offices or in the files of nonpublic businesses. However, information resellers have now amassed extensive amounts of personal information about large numbers of Americans, and federal agencies access this information for a variety of reasons. Federal agency use of such information is governed primarily by the Privacy Act of 1974,<sup>2</sup> 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 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.<sup>3</sup> These principles, now widely accepted, include

---

<sup>1</sup>For purposes of this report, 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.

<sup>2</sup>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.

<sup>3</sup>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).

- 
- collection limitation,
  - data quality,
  - purpose specification,
  - use limitation,
  - security safeguards,
  - openness,
  - individual participation, and
  - accountability.<sup>4</sup>

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.

Given recent events involving information resellers and federal agencies' use of information obtained from these resellers, you asked us to review how selected federal agencies use such information. Specifically, our objectives were to determine (1) how the Departments of Justice, Homeland Security (DHS), and State and the Social Security Administration (SSA) are making use of personal information obtained through contracts with information resellers; (2) the extent to which information resellers providing personal information to these agencies have policies and practices in place that reflect the Fair Information Practices; and (3) the extent to which these agencies have policies and practices in place for the handling of personal data from resellers that reflect the Fair Information Practices.

To address our first objective, we analyzed fiscal year 2005 contracts and other vehicles for the acquisition of personal information from information resellers by DHS, Justice, State, and SSA to identify their purpose, scope, and value. We obtained additional information on these contracts and uses

---

<sup>4</sup>Descriptions of these principles are shown in table 2.

---

in discussions with agency officials to ensure that all relevant information had been provided to us.

To address our second objective, we reviewed documentation from five major information resellers<sup>5</sup> and conducted site visits at three of them<sup>6</sup> to obtain information on privacy and security policies and procedures and compared these with the Fair Information Practices. In conducting our analysis, we identified the extent to which reseller practices were consistent with the key privacy principles of the Fair Information Practices. We also assessed the potential effect of any inconsistencies; however, we did not attempt to make determinations of 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. We determined that the five resellers we reviewed accounted for most of the contract value of personal information obtained from resellers in fiscal year 2005 by the four agencies we reviewed. We did not evaluate the effectiveness of resellers' information security programs.

To address our third objective, we identified and evaluated agency guidelines and management policies and procedures governing the use of personal information obtained from information resellers and compared these to the Fair Information Practices. We also conducted interviews at the four agencies with senior agency officials designated for privacy issues as well as officials of the Office of Management and Budget (OMB) to obtain their views on the applicability of federal privacy laws and related guidance to agency use of information resellers. We performed our work from May 2005 to March 2006 in the Washington, D.C., metropolitan area; Little Rock, Arkansas; Alpharetta, Georgia; and Miamisburg, Ohio. Our work was performed in accordance with generally accepted government auditing standards. Our objectives, scope, and methodology are discussed in more detail in appendix I.

---

<sup>5</sup>The five information resellers we reviewed were ChoicePoint, LexisNexis, Acxiom, Dun & Bradstreet, and West. While these resellers were all reported by federal agencies to be sources of personal information, their businesses vary. A discussion of this variance in business practices appears in the background section of this report. Our results may not apply to other resellers who do very little or no business with these federal agencies.

<sup>6</sup>ChoicePoint, LexisNexis, and Acxiom.



---

---

## Results in Brief

In fiscal year 2005, Justice, DHS, State, and SSA reported using personal information from information resellers for a variety of purposes, including law enforcement, counterterrorism, fraud prevention, and debt collection. Taken together, approximately 91 percent of planned spending on resellers reported by the agencies for fiscal year 2005 was for law enforcement (69 percent) or counterterrorism (22 percent). For example, components of the Department of Justice (the largest user of resellers) made use of such information for criminal investigations, location of witnesses and fugitives, research of assets held by individuals of interest, and detection of fraud in prescription drug transactions. Examples of uses by the DHS include immigration fraud detection and border screening programs. SSA and State acquire personal information from information resellers for fraud detection and investigation, identity verification, and benefit eligibility determination. 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 (GSA) and the Library of Congress’s Federal Library and Information Network. Collectively, the four agencies reported approximately \$30 million<sup>7</sup> in fiscal year 2005 in contractual arrangements with information resellers that enabled the acquisition and use of personal information.

The major information resellers that do business with the federal agencies we reviewed have practices in place to protect privacy, but these measures are not 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 (e.g., accuracy) requirements to these limitations. Resellers said they believe 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 multipurpose

---

<sup>7</sup>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 (e.g., LexisNexis and West provide news and legal research in addition to public records).

---

collection and use of personal and other information<sup>8</sup> information from multiple sources. 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 (relevant to the *openness* principle). 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 (relevant to the *individual participation* principle).

Agency practices for handling personal information acquired from information resellers reflected the principles of the Fair Information Practices in four cases and in the other four did not. Specifically, regarding the *collection limitation*, *data quality*, *use limitation*, and *security safeguards* principles, agency practices generally reflected the Fair Information Practices. For example, regarding the *data quality* principle that data should be accurate, current, and complete, as needed for the defined purpose, 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.

Regarding other principles, however, agency practices were uneven. Specifically, agencies did not always have practices in place to fully address the *purpose specification*, *individual participation*, *openness*, and *accountability* principles with regard to use of reseller information. 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, and
- some agencies lack robust audit mechanisms to ensure that use of personal information from information resellers is for permissible

---

<sup>8</sup>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.

---

purposes, reflecting an uneven application of the *accountability* principle.

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

The Congress should consider the extent to which information resellers should adhere to the Fair Information Practices. We are also recommending 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 are recommending that agencies develop specific policies for the use of personal information from resellers.

We obtained written comments on a draft of this report from Justice, DHS, SSA, and State. We also received comments via E-mail from OMB. Comments from Justice, DHS, SSA, and State are reproduced in appendixes III to VI, respectively. Justice, DHS, SSA, and OMB all generally agreed with the report and described actions initiated to address our recommendations. In its comments, Justice recommended that prior to issuance of any new or revised policy, careful consideration be given to its impact on Justice. We believe the policy clarifications we are proposing are unlikely to result in an adverse impact on law enforcement activities at Justice. Justice and SSA also provided technical comments, which were incorporated in the final report as appropriate.

State interpreted our draft report to “rest on the premise that records from ‘information resellers’ should be accorded special treatment when compared with sensitive information from other sources.” State also indicated that it does not distinguish between types of information or sources of information in complying with privacy laws. However, our report does not suggest that data from resellers should receive special treatment. Instead, our report takes the widely accepted Fair Information Practices as a universal benchmark of privacy protections and assesses agency practices in comparison with them.

---

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, stating their view that it was more appropriate for organizations that collection 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 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 decision can be made about the appropriate balance between resellers' services and the public's right to privacy. Resellers also offered technical comments, which were incorporated in the final report as appropriate.

---

## Background

Before advanced computerized techniques for aggregating, analyzing, and disseminating data came into widespread use, personal information contained in paper-based public records at courthouses or other government offices was relatively difficult to obtain, usually requiring a personal visit to inspect the records. Nonpublic information, such as personal information contained in product registrations, insurance applications, and other business records, was also generally inaccessible. In recent years, however, advances in technology have spawned information reseller businesses that systematically collect extensive amounts of personal information from a wide variety of sources and make it available electronically over the Internet and by other means to customers in both government and the private sector. This 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 information of this type. Among the primary customers of information resellers are financial institutions (including insurance companies), retailers, law offices, telecommunications and technology companies, and marketing firms.

---

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. As is discussed further below, 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 obtain personal information from many different sources. Generally, three types of information are collected: public records, publicly available information, and nonpublic information.

- *Public records* are a primary source of information about consumers, available to anyone, and can be obtained from governmental entities. What constitutes public records is dependent upon state and federal laws, but generally these include birth and death records, property records, tax lien records, motor vehicle registrations, voter registrations, licensing records, and court records (including criminal records, bankruptcy filings, civil case files, and legal judgments).
- *Publicly available information* is information not found in public records but nevertheless publicly available through other sources. These sources include telephone directories, business directories, print publications such as classified ads or magazines, Internet sites, and other sources accessible by the general public.
- *Nonpublic information* is derived from proprietary or nonpublic sources, such as credit header data,<sup>9</sup> product warranty registrations, and

---

<sup>9</sup>Credit header data are the nonfinancial identifying information located at the top of a credit report, such as name, current and prior addresses, telephone number, and Social Security number.

---

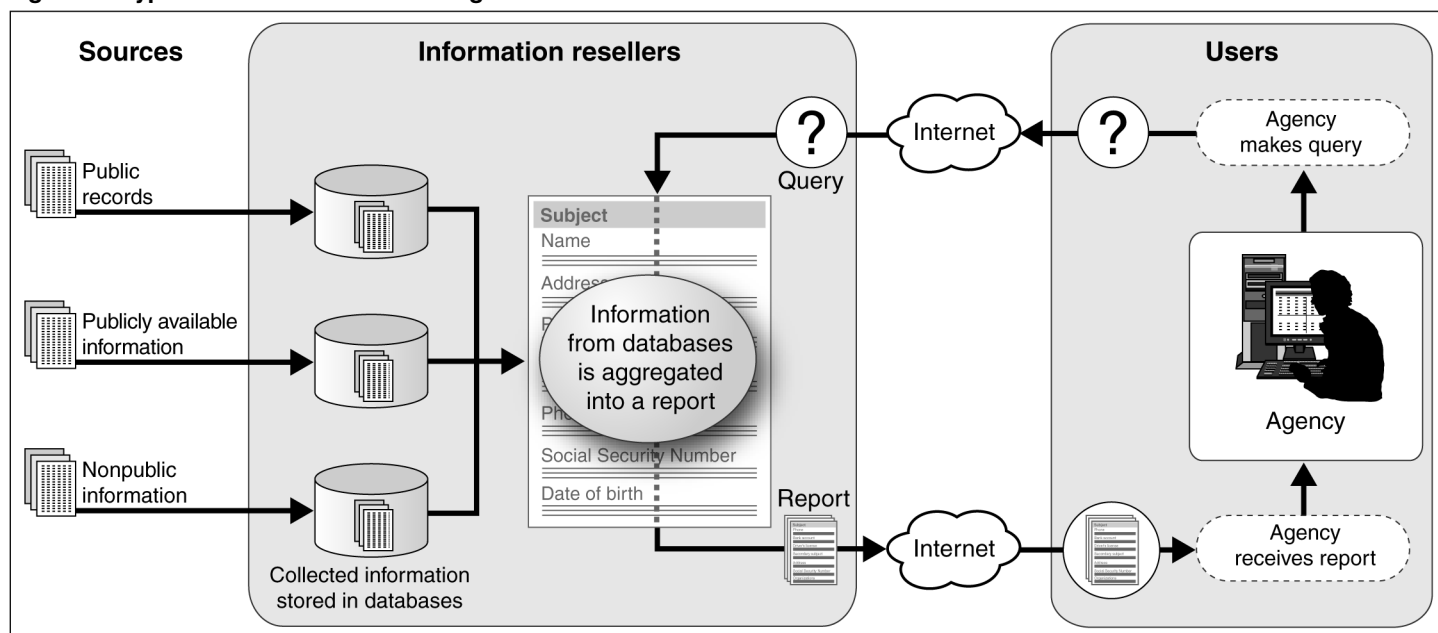
other application information provided to private businesses directly by consumers.

Private sector businesses rely on information resellers for information to support a variety of activities, such as

- conducting pre-employment background checks on prospective employees,
- verifying individuals' identities by reviewing records of their personal information;
- marketing commercial products to consumers matching specified demographic characteristics; and
- preventing financial fraud by examining insurance, asset, and other financial record information.

Typically, while information resellers may collect and maintain personal information in a variety of databases, they provide their customers with a single, consolidated online source for a broad array of personal information. Figure 1 illustrates how information is collected from multiple sources and 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.

In addition to providing consolidated access to personal information through Internet-based Web sites, information resellers offer a variety of products tailored to the specific needs of various lines of business. For example, an insurance company could obtain different products covering police and accident reports, insurance carrier information, vehicle owner verification or claims history, or online public records. Typically, services offered to law enforcement officers include more information—including sensitive information, such as full Social Security numbers and driver’s license numbers—than is offered to other customers.

## 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 types of entities. The major requirements for the protection of personal privacy by federal agencies come from two laws, the Privacy Act of 1974 and the privacy provisions of the E-Government Act of 2002. The Federal Information Security Management Act of 2002 (FISMA)

---

also addresses the protection of personal information in the context of securing federal agency information and information systems.

The Privacy Act places limitations on agencies' collection, disclosure, and use of personal information maintained in systems of records. The act describes a "record" as any item, collection, or grouping of information about an individual that is maintained by an agency and contains his or her name or another personal identifier. It also defines "system of records" as a group of records under the control of any agency from which information is retrieved by the name of the individual or by an individual identifier. The Privacy Act requires that when agencies establish or make changes to a system of records, they must notify the public by a notice in the *Federal Register* identifying, among other things, the type of data collected, the types of individuals about whom information is collected, the intended "routine" uses of data, and procedures that individuals can use to review and correct personal information.<sup>10</sup>

The act's requirements also apply to government contractors when agencies contract for the development and maintenance of a system of records to accomplish an agency function.<sup>11</sup> The act limits its applicability to cases in which systems of records are maintained specifically on behalf of a government agency.

Several provisions of the act require agencies to define and limit themselves to specific predefined purposes. For example, the act requires that to the greatest extent practicable, personal information should be collected directly from the subject individual when it may affect an individual's rights or benefits under a federal program. The 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

---

<sup>10</sup>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)).

<sup>11</sup>5 U.S.C. § 552a(m).



---

provided with sufficient information about the request to make a decision about whether to respond.

In handling collected information, the Privacy Act also requires agencies 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 in their information. Such provisions can provide a strong incentive for agencies to correct any identified errors.

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

The E-Government Act of 2002 strives to enhance protection for personal information in government information systems or information collections by requiring that agencies conduct privacy impact assessments (PIA). A PIA is an analysis of how personal information is collected, stored, shared, and managed in a federal system. More specifically, according to OMB guidance,<sup>12</sup> a PIA is an analysis of how

...information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic

---

<sup>12</sup>OMB, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, M-03-22 (Sept. 26, 2003).

---

information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Agencies must conduct PIAs (1) before developing or procuring information technology that collects, maintains, or disseminates information that is in a personally identifiable form or (2) before initiating any new data collections involving personal information that will be collected, maintained, or disseminated using information technology if the same questions are asked of 10 or more people. OMB guidance also requires agencies to conduct PIAs when a system change creates new privacy risks, for example, changing the way in which personal information is being used. The requirement does not apply to all systems. For example, no assessment is required when the information collected relates to internal government operations, the information has been previously assessed under an evaluation similar to a PIA, or when privacy issues are unchanged.

FISMA also addresses the protection of personal information. FISMA defines federal requirements for securing information and information systems that support federal agency operations and assets; it requires agencies to develop agencywide information security programs that extend to contractors and other providers of federal data and systems.<sup>13</sup> Under FISMA, information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction, including controls necessary to preserve authorized restrictions on access and disclosure to protect personal privacy, among other things.

OMB is tasked with providing guidance to agencies on how to implement the provisions of the Privacy Act and the E-Government Act and has done so, beginning with guidance on the Privacy Act, issued in 1975.<sup>14</sup> The guidance provides explanations for the various provisions of the law as well as detailed instructions for how to comply. OMB's guidance on implementing the privacy provisions of the E-Government Act of 2002

---

<sup>13</sup>FISMA, Title III, E-Government Act of 2002, Pub. L. No. 107-347 (Dec. 17, 2002).

<sup>14</sup>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>.

---

identifies circumstances under which agencies must conduct PIAs and explains how to conduct them. OMB has also issued guidance on implementing the provisions of FISMA.

---

### Additional Laws Provide Privacy Protections for Specific Types and Uses of Information

Although federal laws do not specifically regulate the information reseller industry as a whole, they provide safeguards for personal information under certain specific circumstances, such as when financial or health information is involved, or for such activities as pre-employment background checks. Specifically, the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, the Driver's Privacy Protection Act, and the Health Insurance Portability and Accountability Act all restrict the ways in which businesses, including information resellers, may use and disclose consumers' personal information (see app. II for more details about these laws). The Gramm-Leach-Bliley Act, for example, limits financial institutions' disclosure of nonpublic personal information to nonaffiliated third parties and requires companies to give consumers privacy notices that explain the institutions' information sharing practices. Consumers then have the right to limit some, but not all, sharing of their nonpublic personal information.

As shown in table 1, these laws either restrict the circumstances under which entities such as information resellers are allowed to disclose personal information or restrict the parties with whom they are allowed to share information.

---

---

**Table 1: Federal Laws Addressing Private Sector Disclosure of Personal Information**

<b>Federal laws</b>	<b>Provisions</b>
Fair Credit Reporting Act	Consumer reporting agencies are limited to providing data only to their customers that have a permissible purpose for using the data. With few exceptions, government agencies are treated like other parties and must have a permissible purpose in order to obtain a consumer report.
Gramm-Leach-Bliley Act	Sets limitations on financial institutions' disclosure of customer data to third parties, such as information resellers. Requires companies to give consumers privacy notices that explain the institutions' information-sharing practices. In turn, consumers have the right to limit some, but not all, sharing of their nonpublic personal information.
Driver's Privacy Protection Act	Restricts a third party's ability to obtain Social Security numbers and other driver's license information from state motor vehicle offices unless doing so for a permissible purpose under the law; restricts state motor vehicle offices' ability to disclose driver's license information.
Health Insurance Portability and Accountability Act	Health care organizations are restricted from disclosing a patient's health information without the patient's consent, except for permissible reasons, and are required to inform individuals of privacy practices.
Fair and Accurate Credit Transactions Act	Consumers may obtain one free annual consumer report from nationwide consumer reporting agencies.

Source: GAO analysis.

Note: Appendix II provides additional details on the requirements of these laws.

Information resellers are also affected by various state laws. For example, California state law requires businesses to notify consumers about security breaches that could directly affect them. Legal requirements, such as the California law, led ChoicePoint, a large information reseller, to notify its customers in mid-February 2005 of a security breach in which unauthorized persons gained access to personal information from its databases. Since the ChoicePoint notification, bills were introduced in at least 35 states and enacted in at least 22 states<sup>15</sup> that require some form of notification upon a security breach.

---

<sup>15</sup>States that enacted breach of information legislation in 2005 include Arkansas, Connecticut, Delaware, Florida, Georgia, Illinois, Indiana (applies to state agencies only), Louisiana, Maine, Minnesota, Montana, Nevada, New Jersey, New York, North Carolina, North Dakota, Ohio, Pennsylvania, Rhode Island, Tennessee, Texas, and Washington.

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

The Fair Information Practices are a set of internationally recognized privacy protection principles. First proposed in 1973 by a U.S. government advisory committee, the Fair Information Practices were intended to address what the committee termed a poor level of protection afforded to privacy under contemporary law.<sup>16</sup> A revised version of the Fair Information Practices, developed by the Organization for Economic Cooperation and Development (OECD)<sup>17</sup> in 1980, has been widely adopted. The OECD principles are shown in table 2.

**Table 2: 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.

<sup>16</sup>*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).

<sup>17</sup>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.

---

(Continued From Previous Page)

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

Source: OECD.

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, New Zealand, and the European Union.<sup>18</sup> They are also reflected in a variety of federal agency policy statements, beginning with an endorsement of the OECD principles by the Department of Commerce in 1981,<sup>19</sup> and including policy statements of the DHS, Justice, Housing and Urban Development, and Health and Human Services.<sup>20</sup> In 2004, the Chief Information Officers Council issued a coordinating draft of their Security and Privacy Profile for the Federal Enterprise Architecture<sup>21</sup> that links privacy protection with a set of acceptable privacy principles corresponding to the OECD's version of the Fair Information Practices.

---

<sup>18</sup>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).

<sup>19</sup>"Report on OECD Guidelines Program," Memorandum from Bernard Wunder, Jr., Assistant Secretary for Communications and Information, Department of Commerce (Oct. 30, 1981).

<sup>20</sup>Privacy Office Mission Statement, U.S. Department of Homeland Security; "Privacy Policy Development Guide," Global Information Sharing Initiative, U.S. Department of Justice, [www.it.ojp.gov/global](http://www.it.ojp.gov/global) (Sept. 2005); "Homeless Management Information Systems, U.S. Department of Housing and Urban Development (*Federal Register*, July 30, 2004); and "Options for Promoting Privacy on the National Information Infrastructure," Health and Human Services Privacy Committee, Office of the Assistant Secretary for Planning and Evaluation, Department of Health and Human Services (April 1997).

<sup>21</sup>The Federal Enterprise Architecture is intended to provide a common frame of reference or taxonomy for agencies' individual enterprise architecture efforts and their planned and ongoing information technology investment activities. An enterprise architecture is a blueprint, defined largely by interrelated models, that describes (in both business and technology terms) an entity's "as is" or current environment, its "to be" or future environment, and its investment plan for transitioning from the current to the future environment.

---

The Fair Information Practices are not precise legal requirements. Rather, they provide a framework of principles for balancing the need for privacy with other public policy interests, such as national security, law enforcement, and administrative efficiency. Striking that balance varies among countries and among types of information (e.g., medication versus employment information).

The Fair Information Practices also underlie the provisions of the Privacy Act of 1974. For example, the system of records notice required under the Privacy Act embodies the *purpose specification*, *openness*, and *individual participation* principles in that it provides a public accounting through the *Federal Register* of the purpose and uses for personal information, and procedures by which individuals may access and correct, if necessary, information about themselves. Further, the E-Government Act's requirement to conduct PIAs likewise reflects the Fair Information Practices. Under the act, agencies are to make these assessments publicly available, if practicable, through agency Web sites or by publication in the *Federal Register*, or other means. To the extent that such assessments are made publicly available, they also provide notice to the public about the purpose of planned information collections and the planned uses of the information being collected.

---

### Congressional Interest in the Information Reseller Industry Has Been Heightened

A number of congressional hearings were held and bills introduced in 2005 in the wake of widely publicized data security breaches at major information resellers such as ChoicePoint and LexisNexis as well as other firms. In March 2005, the House Subcommittee on Commerce, Trade, and Consumer Protection of the House Energy and Commerce Committee held a hearing entitled "Protecting Consumers' Data: Policy Issues Raised by ChoicePoint," which focused on potential remedies for security and privacy concerns regarding information resellers. Similar hearings were held by the House Energy and Commerce Committee and by the U.S. Senate Committee on Commerce, Science, and Transportation in spring 2005.

The heightened interest in this subject led a number of Members of Congress to propose a variety of bills aimed at regulating companies that handle personal information, including information resellers. Several of these bills require companies such as information resellers to notify the public of security breaches, while a few also allow consumers to "freeze" their credit (i.e., prevent new credit accounts from being opened without special forms of authentication), or see and correct personal information

---

contained in reseller data collections. Other proposed legislation includes (1) the Data Accountability and Trust Act,<sup>22</sup> requiring security policies and procedures to protect computerized data containing personal information and nationwide notice in the event of a security breach, and (2) the Personal Data Privacy and Security Act of 2005,<sup>23</sup> requiring data brokers to disclose personal electronic records pertaining to an individual and inform individuals on procedures for correcting inaccuracies.

---

## Using Governmentwide Contracts, Federal Agencies Obtain Personal Information from Information Resellers for a Variety of Purposes

Primarily through governmentwide contracts, Justice, DHS, State, and SSA reported using personal information obtained from resellers for a variety of purposes, including law enforcement, counterterrorism, fraud detection/prevention, and debt collection. Most uses by Justice were for law enforcement and counterterrorism, such as investigations of fugitives and obtaining information on witnesses and assets held by individuals of interest. DHS also used reseller information primarily for law enforcement and counterterrorism, such as screening vehicles entering the United States. State and SSA reported acquiring personal information from information resellers for fraud detection and investigation, identity verification, and benefit eligibility determination. The four agencies reported approximately \$30 million in contractual arrangements with information resellers in fiscal year 2005.<sup>24</sup> Justice accounted for most of the funding (about 63 percent).

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. (Details on uses by each agency are given in the individual agency discussions.)

---

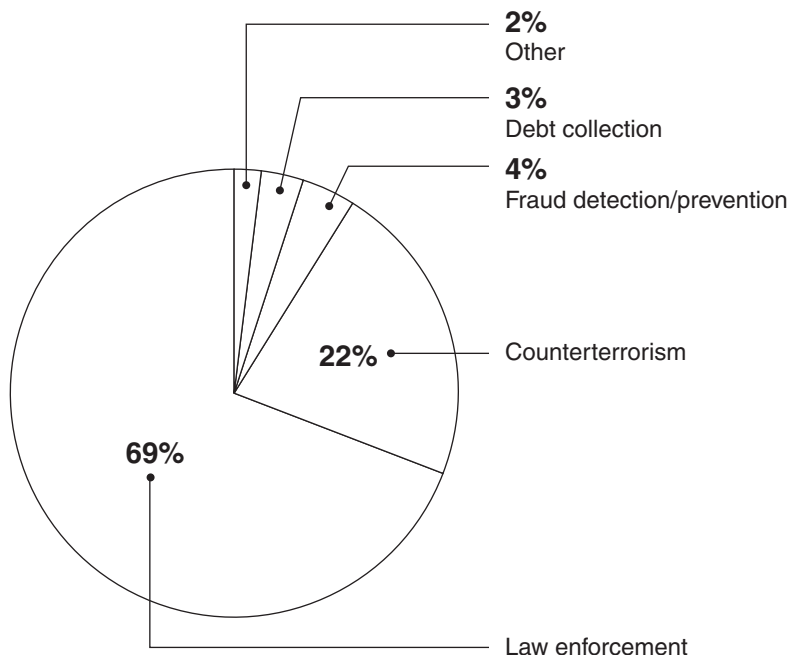
<sup>22</sup>H.R. 4127; introduced by Representative Clifford B. Stearns on October 25, 2005.

<sup>23</sup>S. 1789; introduced by Senator Arlen Specter on September 29, 2005, and reported from the Senate Judiciary Committee on November 17, 2005.

<sup>24</sup>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 (e.g., 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.

### Department of Justice Uses Information Resellers Primarily for Law Enforcement and Counterterrorism Purposes

According to Justice contract documentation, access to up-to-date and comprehensive public record information is a critical ongoing mission requirement, and the department relies on a wide variety of information resellers—including ChoicePoint, Dun & Bradstreet, LexisNexis, and West—to meet that need. Departmental use of information resellers was primarily for purposes related to law enforcement (75 percent) and counterterrorism (18 percent), including support for criminal investigations, location of witnesses and fugitives, information on assets held by individuals under investigation, and detection of fraud in prescription drug transactions. In fiscal year 2005, Justice and its components reported approximately \$19 million in acquisitions from information resellers involving personal information. The department acquired these services primarily through use of GSA's Federal

---

SupplySchedule<sup>25</sup> offerings including a blanket purchase agreement<sup>26</sup> with ChoicePoint valued at approximately \$15 million.<sup>27</sup> Several component agencies, such as the Federal Bureau of Investigation (FBI), the Drug Enforcement Administration (DEA), and the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) placed orders with information resellers based on the schedules. In addition, for fiscal year 2005, Justice established separate departmentwide contracts with LexisNexis and West valued at \$4.5 million and \$5.2 million, respectively.<sup>28</sup>

Tasked to protect and defend the United States against terrorist and foreign intelligence threats and to enforce criminal laws, the FBI is Justice's largest user of information resellers, with about \$11 million in contracts in fiscal year 2005. The majority of FBI's use involves two major programs, the Public Source Information Program and the Foreign Terrorist Tracking Task Force (FTTTF). In support of the investigative and intelligence missions of the FBI, the Public Source Information Program provides all offices of the FBI with access via the Internet to public record, legal, and news media information available from various online commercial databases. These databases are used to assist with investigations by identifying the location of individuals and identifying alias names, Social Security numbers, relatives, dates of birth, telephone numbers, vehicles, business affiliations, other associations, and assets. Public Source Information Program officials reported that use of these commercial databases often results in new information regarding the subject of the investigation. Officials noted that commercial databases are used in

---

<sup>25</sup>GSA's Federal Supply Schedule allows agencies to take advantage of prenegotiated contracts with a variety of vendors, including information resellers.

<sup>26</sup>A GSA schedule blanket purchase agreement simplifies the filling of recurring needs for supplies or services, while leveraging a customer's buying power by taking advantage of quantity discounts, saving administrative time, and reducing paperwork.

<sup>27</sup>The ChoicePoint blanket purchase agreement is also available to non-Justice agencies, whose use accounted for approximately \$2.8 million in fiscal year 2005.

<sup>28</sup>The total value of ChoicePoint, LexisNexis, and West contracts—\$24.7 million—exceeds the value of \$19 million reported above because this figure omits the \$2.8 million used by non-Justice agencies (see footnote 27) as well as uses that were reported not to involve personal information. Justice officials responsible for administering the departmentwide contracts with LexisNexis and West reported that these agreements are used by multiple components whose business needs vary and may not require use of databases that include public records about individuals. In cases where Justice officials were able to separate these costs, we omitted these costs from the total.

---

preliminary investigations, and that subsequently, investigative personnel must verify the results of each search.

The FBI's FTTTF also contracts with several information resellers (1) to assist in fulfilling its mission of assisting federal law enforcement and intelligence agencies in locating foreign terrorists and their supporters who are in or have visited the United States and (2) to provide information to other law enforcement and intelligence community agencies that can lead to their surveillance, prosecution, or removal. As we previously reported,<sup>29</sup> FTTTF makes use of personal information from several commercial sources to analyze intelligence and detect terrorist activities in support of ongoing investigations by law enforcement agencies and the intelligence community. Information resellers provide FTTTF with names, addresses, telephone numbers, and other biographical and demographical information as well as legal briefs, vehicle and boat registrations, and business ownership records.

Other Justice components reported using personal information from information resellers to support the conduct of investigations and other law enforcement-related activities. For example, the U.S. Marshals Service uses an information reseller to, among other things, locate fugitives by identifying a fugitive's relatives and their addresses.<sup>30</sup> Through interviews with relatives, a U.S. Marshal may be able to ascertain the location of a fugitive and subsequently apprehend the individual.

DEA, the second largest Justice user of information resellers in fiscal year 2005, obtains reseller data to detect fraud in prescription drug transactions.<sup>31</sup> Through these data, DEA agents can detect irregular prescription patterns for specific drugs and trace this information to the pharmacy and prescribing doctor.<sup>32</sup> DEA also uses an information reseller

---

<sup>29</sup>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).

<sup>30</sup>The U.S. Marshals Service is the federal government's primary agency for conducting investigations involving escaped federal prisoners; probation, parole, and bond violators; and fugitives named in warrants generated during drug investigations.

<sup>31</sup>DEA's mission involves enforcing laws pertaining to the manufacture, distribution, and dispensing of legally produced controlled substances.

<sup>32</sup>The personal information contained in this information reseller database is limited to the prescribing doctor and does not contain personal patient information.

---

to locate individuals in asset forfeiture cases.<sup>33</sup> Reseller data allows DEA to identify all possible addresses for an individual in order to meet the agency's obligation to make a reasonable effort to notify individuals of seized property and inform them of their rights to contest the seizures.

Other uses reported by Justice components are not related to law enforcement. For example, uses by the U.S. Trustees, Antitrust, Civil, Tax, and Criminal Divisions include ascertaining the financial status of individuals for debt collection purposes or bankruptcy proceedings or for the location of individuals for court proceedings. The Executive Office for U.S. Attorneys uses information resellers to ascertain the financial status of those indebted to the United States in order to assess the debtor's ability to repay the debt. According to officials, information reseller databases may reveal assets that a debtor is attempting to conceal. Further, the U.S. Attorneys use information resellers to locate victims of federal crime in order to notify these individuals of relevant court proceedings pursuant to the Justice for All Act.<sup>34</sup>

Table 3 details in aggregate the vendors, fiscal year 2005 contract values, and reported uses for contracts with information resellers by major Justice components.

---

<sup>33</sup>To ensure that criminals do not benefit financially from their illegal acts, federal law provides that profits from drug-related crimes, as well as property used to facilitate certain crimes, are subject to forfeiture to the government.

<sup>34</sup>Justice for All Act of 2004, Pub. L. No. 108-405 (Oct. 30, 2004). Section 102 of the act establishes rights for crime victims including the right to "reasonable, accurate, and timely notice of any public court proceeding, or any parole proceeding, involving the crime of or any release or escape of the accused."

**Table 3: Reported Uses of Personal Information: Department of Justice Contracts with Information Resellers, Fiscal Year 2005**

Major component	Information resellers	Aggregate contract value	Uses involving personal information
Federal Bureau of Investigation	ChoicePoint, LexisNexis, West, Credit Bureau Reports, Dun & Bradstreet, Seisint <sup>a</sup>	\$11,248,000	<p><i>Public Source Information Program.</i> Find individuals and identify alias names, Social Security numbers, relatives, dates of birth, telephone numbers, vehicles, business affiliations, associations, and assets.</p> <p>The program provides FBI units with access to public record, legal, and news media information from various online commercial databases.</p> <p><i>Criminal Investigative Division.</i> Same use.</p> <p><i>Foreign Terrorist Tracking Task Force.</i> Obtain such information as names, addresses, telephone numbers, other biographical information, vehicle and boat registrations, and business ownership records.</p>
Drug Enforcement Administration	ChoicePoint, LexisNexis, Dun & Bradstreet	\$4,283,000	<p>Conduct investigations of drug diversions and improper drug transactions:</p> <p>For example, identifying cases in which physicians sell prescriptions to drug dealers or abusers, pharmacists falsely report legitimate drug sales and subsequently sell the drugs illegally, and employees steal from inventory and falsify orders to hide illicit sales.</p> <p>Support criminal investigations of specific individuals and companies. Locate an individual's address in asset removal cases.</p>
U.S. Marshals Service	ChoicePoint, LexisNexis, West	\$1,661,000	<p>Generate leads related to fugitive investigations (e.g., a fugitive's relatives and their contact information).</p> <p><i>Asset Forfeiture Office.</i> Obtain information on preseized, seized, and forfeited property.</p> <p>The Marshals Service offers property for sale to the public that has been forfeited under laws enforced or administered by Justice and its investigative agencies.</p> <p><i>Office of General Counsel.</i> Research assets to administer tort claims against the service.</p> <p>For example, if a claimant makes an assertion that the service is responsible for damaging property and does not provide supporting documentation, General Counsel personnel may use commercial data to verify tax assessment records, proof of ownership, etc.</p>
Executive Office for U.S. Attorneys	ChoicePoint, CBR Information Services	\$855,000	<p><i>Financial Litigation Units.</i> Ascertain the financial status of individuals and uncover concealed assets for civil and criminal debt collection efforts. Locate and notify crime victims of relevant court proceedings pursuant to the Justice for All Act of 2004.</p>
Bureau of Alcohol, Tobacco, Firearms, and Explosives	ChoicePoint, Dun & Bradstreet, LexisNexis, West	\$791,000	<p>Support investigative activities such as locating and apprehending fugitives or obtaining data on businesses (such as in arson investigations), which may include personal information about business owners.</p>

(Continued From Previous Page)

Major component	Information resellers	Aggregate contract value	Uses involving personal information
Executive Office of the United States Trustees	ChoicePoint, Equifax, <sup>b</sup> Real Data Corp, MLS Hawaii	\$303,000	Obtain information on assets (openly held or concealed) of individuals in bankruptcy proceedings (as part of office's mission to enforce bankruptcy laws and provide oversight of private trustees).  Obtain credit reports on employees as part of a security clearance process.
Office of the Inspector General	ChoicePoint, LexisNexis, West	\$43,000	<i>Investigations Division.</i> Support investigations of alleged violations of fraud, abuse, and integrity laws that govern Justice employees, operations, grantees, and contractors.
U.S. National Central Bureau	ChoicePoint	\$31,000	Conduct business and address checks on individuals who may be potentially involved in fraud or fugitive cases.  The bureau facilitates international law enforcement cooperation as the U.S. representative of the International Criminal Police Organization (INTERPOL).
National Drug Intelligence Center	ChoicePoint	\$28,000	<i>Document Exploitation Division.</i> Locate individuals, identify assets, and investigate fraud.  The Document Exploitation Division specializes in analyzing information seized in major federal drug investigations.
Office of Justice Programs	Dun & Bradstreet	\$22,000	<i>Office of Comptroller, Financial Management Division.</i> Obtain credit reports to assess new grantees' (nongovernmental or nontribal) financial integrity. These credit reports may include personal information on company owners.  This information is used to support the new grantee's ability to operate the grant programs of the Office of Justice Programs, to confirm the existence of the company, and to determine any outstanding liens or obligations that might influence the success of the grant program.
Litigating Divisions (Civil, Criminal, Antitrust, and Tax)	ChoicePoint, Credit Bureau Reports (division of CBC Companies)	\$21,000	<i>Civil Division.</i> Locate individuals and assets in connection with litigation for purposes such as obtaining depositions, debt collection, and identifying assets that a debtor may be concealing in bankruptcy proceedings.  <i>Criminal Division, Office of Special Investigations.</i> Locate individuals who may have taken part in Nazi-sponsored acts of persecution abroad before and during World War II and who subsequently entered, or seek to enter, the United States illegally and/or fraudulently.  <i>Antitrust Division.</i> Locate witnesses for trials.  <i>Tax Division.</i> Obtain credit bureau reports for debt collection purposes.

Source: Department of Justice.

Notes: The table represents fiscal year 2005 contract values and may not reflect actual expenditures. We did not verify the accuracy or completeness of the dollar figures provided to us.

Contract values were rounded to the nearest thousand. Several Justice components use departmentwide contracts with LexisNexis and West, which provide, among other things, access to public records information. Several components, including the litigating divisions (Civil, Criminal, Antitrust, and Tax), the Office of Justice Programs, and the Executive Office for U.S. Attorneys, reported that their use of these departmentwide contracts was primarily for legal research, and therefore we did not include these uses in the table.

---

<sup>a</sup>Seisint is now owned by LexisNexis.

<sup>b</sup>Equifax is an example of a consumer reporting agency. Consumer reporting agencies, also known as credit bureaus, are entities that collect and sell information about the creditworthiness, among other things, of individuals and are required by the Fair Credit Reporting Act to disclose such information only for permissible purposes.

---

## DHS Uses Information Resellers Primarily for Law Enforcement and Counterterrorism

In fiscal year 2005, DHS and its components reported that they used information reseller data primarily for law enforcement purposes, such as for developing leads on subjects in criminal investigations and detecting fraud in immigration benefit applications (part of enforcing the immigration laws). Counterterrorism uses involved screening programs at the northern and southern borders as well as at the nation's airports. DHS reported planning to spend about \$9 million acquiring personal information from resellers in fiscal year 2005. DHS acquired these services primarily for law enforcement (63 percent) and counterterrorism (35 percent) purposes through FEDLINK—a governmentwide contract vehicle provided by the Library of Congress—and GSA's Federal Supply Schedule contracts as well as direct purchases by its components. DHS's primary vehicle for acquiring data from information resellers was the FEDLINK contract vehicle, which DHS used to acquire reseller services from Choicepoint (\$4.1 million), Dun & Bradstreet (\$640,000), LexisNexis (\$2 million), and West (\$1 million).

U.S. Immigration and Customs Enforcement (ICE) is DHS's largest user of personal information from resellers, with acquisitions worth over \$4.3 million. The largest investigative component of DHS, ICE has as its mission to prevent acts of terrorism by targeting the people, money, and materials that support terrorist and criminal activities. ICE uses information resellers to collect personal information for criminal investigative purposes and to perform background security checks. Data commonly obtained include address and vehicle information; according to officials, this information is either used to verify data already collected or is itself verified by investigators through other means. For example, ICE's Federal Protective Service has about 50 users who access an information reseller database to assist in properly identifying and locating potential criminal suspects. Investigators may verify an address obtained from the database by confirming billing information with a utility company or by conducting "drive-by" surveillance. The Federal Protective Service views information obtained from resellers as "raw" or "unverified" data, which may or may not be of use to investigators.

Other DHS components likewise reported using personal information from resellers to support investigations and other law enforcement-related

---

activities. For example, U.S. Customs and Border Protection (CBP)—tasked with managing, controlling, and protecting the nation’s borders at and between the official ports of entry—uses information resellers for law enforcement, intelligence gathering, and prosecution support. Using these databases, investigators conduct queries on people, businesses, property, and corresponding links via a secure Internet connection. According to officials, information obtained is corroborated with other previously obtained data, open-source information, and investigative leads.

CBP also uses a specially developed information reseller product to assist law enforcement officials in vehicle identification at northern and southern land borders. CBP uses electronic readers to capture license plate data on vehicles entering or exiting U.S. borders, converts the data to an electronic format, and transmits the data to an information reseller, which returns U.S. motor vehicle registration information to CBP. The license plate data, merged with the associated motor vehicle registration data provided by the reseller, are then checked against government databases in order to help assess risk related to vehicles (i.e., a vehicle whose license plate is associated with a law enforcement record might be referred for secondary examination).

The Federal Emergency Management Agency (FEMA), charged with building and supporting the nation’s emergency management system, uses an information reseller to detect fraud in disaster assistance applications. FEMA uses this service to verify information that individuals present in their applications for disaster assistance via the Internet. At the time of application, an individual is required to pass an identity check that determines whether the presented identity exists, followed by an identity validation quiz to better ensure that the applicant corresponds to the identity presented. The information reseller is used to verify the applicant’s name, address, and Social Security number.

DHS is also using information resellers in its counterterrorism efforts. For example, the Transportation Security Administration (TSA), tasked with protecting the nation’s transportation systems, used data obtained from information resellers as part of a test associated with the development of



---

its domestic passenger prescreening program, called “Secure Flight.”<sup>35</sup> TSA’s plans for Secure Flight involve the submission of passenger information by an aircraft operator to TSA whenever a reservation is made for a flight in which the origin and destination are domestic airports. In the prescreening of airline passengers, this information would be compared with federal watch lists of individuals known or suspected of activities related to terrorism. TSA conducted a test designed to help determine the extent to which information resellers could be used to authenticate passenger identity information provided by air carriers. It plans to use the test results to determine whether commercial data can be used to improve the effectiveness of watch-list matching by identifying passengers who would not have been identified from passenger name records and government data alone. The test results also may be used to identify items of personally identifying information that should be required of passengers to improve aviation security.

Table 4 provides detailed information about DHS uses of information resellers in fiscal year 2005, as reported by officials of the department’s components.

---

<sup>35</sup>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).

**Table 4: Reported Uses of Personal Information: DHS Contracts with Information Resellers, Fiscal Year 2005**

Major component	Information reseller	Aggregate contract value	Uses involving personal information
U.S. Immigration and Customs Enforcement	ChoicePoint, Dun & Bradstreet, LexisNexis, West	\$4,389,000	<p>Acquire data (generally, address and vehicle information) for criminal investigations and background security checks.</p> <p>According to officials, information is either used to verify data already collected or is itself verified by investigators through other means.</p> <p><i>Federal Protective Service.</i> Identify and locate potential criminal suspects using address, vehicle, and other information.</p> <p><i>Office of Detention and Removal.</i> Locate and remove illegal aliens from the United States using address, vehicle, and other information.</p>
U.S. Customs and Border Protection	ChoicePoint, LexisNexis, Dun & Bradstreet, and West	\$2,375,000	<p>Conduct queries on people, businesses, property, and corresponding links in support of law enforcement, intelligence gathering, and prosecution support.</p> <p><i>Border Patrol Del Rio Sector.</i> Obtain information such as addresses, telephone numbers, and names of relatives in support of investigations involving registered owners of seized vehicles and property.</p> <p><i>National Targeting Center.</i> Look up information associated with license plate data to assist in vehicle identification at northern and southern land borders.</p> <p>License plate readers capture data on vehicles and cross-check against information reseller and government databases. Data captured are used to help assess risk related to these vehicles (e.g., a car whose license plate is associated with a law enforcement record might be referred for secondary examination).</p>
U.S. Citizenship and Immigration Services	ChoicePoint, LexisNexis, West	\$960,000	<p><i>Offices of Fraud Detection and National Security and Asylum.</i> Detect fraud in applications for immigrant benefits and obtain court records (including judgments and conviction documents) to support a broad range of evidentiary requirements for official adjudication proceedings.</p>
Transportation Security Administration	Acxiom, Insight America, Qsent <sup>a</sup>	\$897,000	<p>Test the feasibility of using commercial data sources to authenticate identity information contained in passenger records to support passenger prescreening.</p> <p>As part of the Secure Flight Program, TSA conducted a test to determine whether commercial data could be used to improve the effectiveness of watch list matching by identifying passengers who would not have been identified from passenger name records and government data alone. TSA plans to use the results of the test to identify what personally identifying information should be required in passenger name records to maximize aviation security.</p>

(Continued From Previous Page)

Major component	Information reseller	Aggregate contract value	Uses involving personal information
U.S. Secret Service	ChoicePoint, Dallas Computer Services, Dun & Bradstreet, LocatePLUS, and APPRISS	\$471,000	Provide investigative leads to field agents and other Secret Service personnel in conducting their investigations (e.g., to develop background information on persons, locations, or businesses).  Acquire jail data that are used as a cross-check against state and federal databases on warrants, sex offenders, child support, probations, and paroles.
Federal Emergency Management Agency	ChoicePoint	\$113,000	Acquire information such as name, address, and Social Security number to help verify and validate the identities of individuals applying for disaster assistance via the Internet.
Office of Inspector General	ChoicePoint, LexisNexis	\$39,000	Generate leads in law enforcement investigations.
U.S. Coast Guard	ChoicePoint	\$19,000	Obtain up-to-date credit reports as needed to assist in the resolution of financial issues that are of a security concern in adjudications.
Federal Law Enforcement Training Center—Special Investigations Division	ChoicePoint	\$7,900	Verify addresses, conduct background checks, criminal and administrative investigations.

Source: DHS.

Notes: The table represents fiscal year 2005 contract values and may not reflect actual expenditures. We did not verify the accuracy or completeness of the dollar figures provided to us.

Contract values were rounded to the nearest thousand.

Several DHS components use the departmentwide contracts with LexisNexis and West. Components such as the Science and Technology and Management Directorates reported that their use of these departmentwide contracts did not involve the use of personal information (e.g., reported uses were for legal or scientific research); accordingly, we did not include these values in the table.

To the extent possible, we excluded uses that did not involve personal information; however, since DHS officials responsible for administering departmentwide FEDLINK contracts were unable to provide a breakdown of component billings by information reseller, the values reflected in the table may include uses that do not involve personal information. For example, U.S. Citizenship and Immigration Services' fiscal year 2005 use of departmentwide FEDLINK contracts totaled approximately \$960,000, but contract officials could not provide specific amounts for this organization's use of ChoicePoint, LexisNexis, and West. Although U.S. Citizenship and Immigration Services described use of West as primarily for legal research, we could not separate costs associated with use of personal information.

<sup>a</sup>Acxiom, Insight America (now owned by Acxiom), and Qsent were subcontractors on the EagleForce Associates contract to conduct a commercial data test for the Secure Flight Program. Although EagleForce is not an information reseller, we included the contract value because the commercial data test involved the acquisition of personal information from resellers.

---

---

## SSA Uses Information Resellers Primarily for Fraud Prevention and Identity Verification

In an effort to ensure the accuracy of Social Security benefit payments, SSA and its components reported using approximately \$1.3 million in contracts in fiscal year 2005 with information resellers for a variety of purposes relating to fraud prevention (66 percent), such as skiptracing,<sup>36</sup> confirming suspected fraud related to workers compensation payments, obtaining information on criminal suspects for follow-up investigations (18 percent), and collecting debts (16 percent). SSA and its components acquired these services through the use of the GSA and FEDLINK governmentwide contracts and their own contracts. In fiscal year 2005, SSA contracted with ChoicePoint, LexisNexis, SourceCorp, and Equifax.

The Office of the Inspector General (OIG), the largest user of information reseller data at SSA, supports the agency's efforts to prevent fraud, waste, and abuse. The OIG uses several information resellers to assist investigative agents in detecting benefit abuse by Social Security claimants and to assist agents in locating claimants. For example, OIG agents access reseller data to verify the identity of subjects undergoing criminal investigations.

Regional office agents may also use reseller data in investigating persons suspected of claiming disability fraudulently and draw upon assistance from OIG headquarters staff and state investigators from the state Attorney General's office in these investigations. For example, the Northeastern Program Service Center, located in the New York branch of SSA, obtains New York State Workers Compensation Board data from SourceCorp, the only company legally permitted to maintain the physical and electronic records for New York State Workers Compensation. Through the use of this information, SSA can identify persons collecting workers compensation benefits but not reporting those benefits, as required, to the SSA.

Table 5 details in aggregate the vendors, fiscal year 2005 contract values, and uses of contracts with information resellers reported by major SSA components.

---

<sup>36</sup>Skiptracing is the process of locating people who have fled in order to avoid paying debts.

**Table 5: Reported Uses of Personal Information: SSA Contracts with Information Resellers, Fiscal Year 2005**

User	Information reseller	Contract value	Uses involving personal information
Agencywide	LexisNexis	\$848,000 <sup>a</sup>	<p><i>Field Office Staff.</i> Obtain resource information (i.e., real property ownership, values, real property transfers, and information concerning the ownership of automobiles and boats) to verify the validity of Supplemental Security Income applicants and recipients.</p> <p><i>Office of Inspector General.</i> Access public records information to assist with investigations of fraud and abuse within the SSA programs.</p> <p><i>Office of Hearings and Appeals.</i> Access public records information to locate the addresses of individuals.</p>
Office of the Inspector General	ChoicePoint	\$240,000	Acquire information on subjects of criminal investigations (e.g., locations, assets, relatives) and help corroborate fraud allegations that are submitted to the Office of the Inspector General by SSA or the general public. <sup>b</sup>
Agencywide <sup>c</sup>	Equifax	\$204,000	Obtain address verification reports for the most current address of delinquent debtors for undeliverable overpayment-related notices and follow up billing and teleprinter profile reports (standard credit reports) that show the credit history of the debtor referred to Justice for enforced collection via civil suit.
Northeastern Program Service Center	SourceCorp	\$14,000	Access New York State Worker Compensation Board payment data to ensure that persons claiming Social Security benefits are correctly reporting workers compensation benefits on their forms.
Office of the Inspector General New Jersey Cooperative Disability Investigation Unit <sup>d</sup>	ChoicePoint	\$4,000	Access information on disability claimants and their physicians to determine if the claimants may be hiding assets and other sources of income that may make them ineligible for disability benefits.

Source: SSA.

Notes: The table represents fiscal year 2005 contract values and may not reflect actual expenditures. We did not verify the accuracy or completeness of the dollar figures provided to us.

Contract values were rounded to the nearest thousand.

<sup>a</sup>This figure may include uses that do not involve personal information since LexisNexis provides news and legal research in addition to public records. SSA was unable to separate the dollar values associated with use of personal information from uses for other purposes.

<sup>b</sup>In addition to initiating its own investigations, the Office of the Inspector General receives notices from the general public about suspected fraud. According to one agency official, a large portion of these fraud allegations are either incomplete or unfounded and must be supported by substantial evidence. Before moving ahead with an investigation, officials obtain data from an information reseller to verify the legitimacy of the fraud allegations, fill in any missing information on the submitted forms and develop leads that would further the development of the allegation and any subsequent investigation if warranted.

<sup>c</sup>The Equifax data are accessible by the Northeastern Program Service Center, Mid-Atlantic Program Service Center, Southeastern Program Service Center, Great Lakes Program Service Center, Western Program Service Center, Mid-America Program Service Center, Office of Central Operations, and Office of Financial Policy and Operations.

---

<sup>d</sup>This is an SSA-funded joint investigation between SSA and the New Jersey State Attorney General's Office.

---

## The Department of State Uses Information Resellers Primarily for Passport Fraud Detection and Investigation

The Department of State and its components reported approximately \$569,000 in contracts in fiscal year 2005 with information resellers, primarily for assistance in fraud related activities through criminal investigations (51 percent), fraud detection (26 percent), and other uses (23 percent) such as background screening. State acquired information reseller services through the GSA schedule and a Justice blanket-purchase agreement. In fiscal year 2005, the majority of State contracts were with ChoicePoint; the agency also had contracts with LexisNexis, Equifax and Metronet.

State's components reported use of these contracts mainly for passport-related activities. For example, several components of State accessed personal information to validate information submitted on immigrant and nonimmigrant visa petitions, such as marital or familial relationships, birth and identity information, and address validation. A major use of reseller data at State is by investigators acquiring information on suspects in passport and visa fraud cases. According to State, information reseller data are increasingly important to its operations, because the number of passport and visa fraud cases has increased, and successful investigations of passport and visa fraud are critical to combating terrorism.

In addition to these uses, State acquires personal information through Equifax to support the financial background screening of its job applicants.

Table 6 details the vendors, fiscal year 2005 contract values, and uses of contracts with information resellers reported by major State components.

**Table 6: Reported Uses of Personal Information: Department of State Contracts with Information Resellers, Fiscal Year 2005**

Component	Information reseller	Contract value	Uses involving personal information
Diplomatic Security	ChoicePoint	\$288,000	<i>Criminal Investigations Division.</i> Obtain leads on addresses, locations, identity, etc., used in the conduct of criminal investigations of passport and visa fraud.  <i>Diplomatic Security Command Center and Diplomatic Security agents at 26 overseas posts.</i> Same use.
Office of Personnel Security and Suitability	Equifax	\$132,000	Obtain credit checks on applicants and new hires to support background screening processes.
Bureau of Consular Affairs	ChoicePoint, Metronet	\$89,000	Check the validity of selected passport applications, particularly two categories of high-risk applications. <sup>a</sup>
National Visa Center	ChoicePoint	\$40,000	Verify information submitted on immigrant and nonimmigrant visa petitions.
Office of Consular Fraud Prevention Programs	LexisNexis	\$21,000	Investigate claims of marital and familial relationships on immigrant visa applications and determine the bona fides of prospective employers for employment-based nonimmigrant visas.

Source: Department of State.

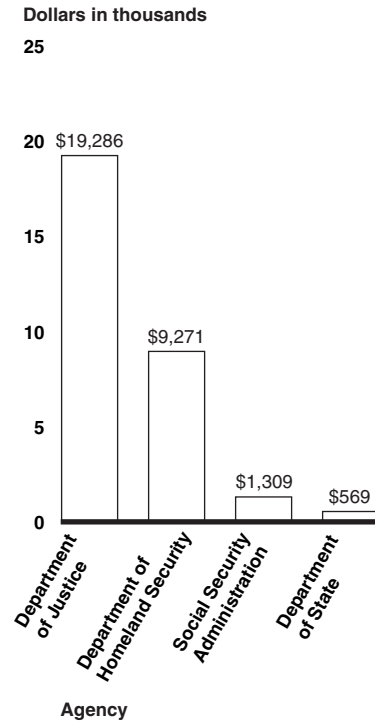
Note: The table represents fiscal year 2005 contract values and may not reflect actual expenditures. We did not verify the accuracy or completeness of the dollar figures provided to us.

<sup>a</sup>The two categories of high-risk passport applications include those with birth certificates from Puerto Rico and those from applicants lacking acceptable primary identification documents, who include affidavits from family or associates attesting to their identity.

**Agencies Contract with Information Resellers Primarily through Use of GSA's Federal Supply Schedules and the Library of Congress's FEDLINK Service**

In fiscal year 2005, the four agencies acquired personal information primarily through governmentwide contracts, including GSA's Federal Supply Schedule (52 percent) contracts and the Library of Congress's FEDLINK contracts (28 percent). Components within these agencies also initiated separate contracts with resellers as well. The Department of Justice was the largest user, accounting for approximately \$19 million of the \$30 million total for all four agencies. Figure 3 shows the values of reseller data acquisition by agency for fiscal year 2005.

**Figure 3: Total Dollar Values, Categorized by Agency, of Fiscal Year 2005 Acquisition of Personal Information from Information Resellers**



Source: GAO analysis of agency-provided data.

In fiscal year 2005, the most common vehicles used among all four agencies to acquire personal information from information resellers were the governmentwide contracts made available through GSA's Federal Supply Schedule. The GSA schedule provides agencies with simplified, streamlined contracting vehicles, allowing them to obtain access to information resellers' services either by issuing task or purchase orders or by establishing blanket purchase agreements based on the schedule contracts. The majority of Justice's acquisition of information reseller services was obtained through the GSA schedule, including a blanket purchase agreement with ChoicePoint that was also made available to non-Justice agencies (for example, the Departments of State and Health and Human Services). In addition, components of DHS such as the U.S. Secret Service and the SSA's Office of Inspector General made use of GSA schedule contracts with information resellers.



---

The Federal Supply Schedule allows agencies to take advantage of prenegotiated contracts with a variety of vendors, including information resellers. GSA does not assess fees for the use of these contracts; rather it funds the operation of the schedules in part by obtaining administrative fees from vendors on a quarterly basis. According to GSA officials, use of the schedule contracts allows agencies to obtain the best price and reduce their procurement lead time. Since these contracts have been prenegotiated, agencies do not need to issue their own solicitation. Instead, agencies may simply place a task order directly with the vendor, citing the schedule number. GSA's role in administering these contracts is primarily to negotiate baseline contract requirements and pricing; it does not monitor which agencies are using its schedule contracts. GSA officials noted that the requirements contained in the schedule contracts are baseline, and agencies may add more stringent requirements to their individual task orders.

Another contract vehicle commonly used to obtain personal information from information resellers was the Library of Congress's FEDLINK service (28 percent). This vehicle was used by both DHS and SSA.<sup>37</sup> FEDLINK, an intragovernmental revolving fund,<sup>38</sup> is a cooperative procurement, accounting, and training program designed to provide access to online databases, periodical subscriptions, books, and other library and information support services from commercial suppliers, including information resellers. At DHS, use of the FEDLINK service was the primary vehicle for contracting with information resellers. DHS also used GSA schedule buys, and some smaller purchases were made directly between DHS components and information resellers. The majority of SSA's fiscal year 2005 acquisitions from information resellers were through FEDLINK, with some use of the GSA schedule contracts.

FEDLINK allows agencies to take advantage of prenegotiated contracts at volume discounts with a variety of vendors, including information resellers. As with the GSA schedule contracts, the requirements of the FEDLINK

---

<sup>37</sup>Although the Library of Congress indicated that the Department of State also used FEDLINK contracts with Dun & Bradstreet and LexisNexis, State officials reported that their use of these contracts did not involve access to personal information.

<sup>38</sup>Section 103 of Pub. L. 106-481 (2 U.S.C. 182c) establishes FEDLINK as a revolving fund. The law authorizes the FEDLINK revolving fund to provide "the procurement of commercial information services, publications in any format, and library support services, related accounting services, related education, information and support services" to federal offices and to other organizations entitled to use federal sources of supply.

---

contracts serve as a baseline, and agencies may add more stringent requirements if they so choose.

FEDLINK offers two different options for using its contracts: direct express and transfer pay. The direct express option is similar to the GSA schedule process, in which the agency issues a purchase order directly to the vendor and cites the underlying FEDLINK contract. Under direct express, the ordering agency is responsible for managing the delivery of products and services and paying invoices, and the vendor pays an administrative fee to the Library. Under the transfer pay option, ordering agencies must sign an interagency agreement and pay an administrative fee to the Library. In turn, the ordering agencies receive additional administrative services. DHS used both the direct express and transfer pay options in fiscal year 2005, while SSA used transfer pay exclusively.

---

## 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<sup>39</sup> have practices in place 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 that information can be collected and made available to multiple customers for multiple purposes. Resellers make it their business to collect large amounts of personal information<sup>40</sup> 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

---

<sup>39</sup>We reviewed the practices of five major information resellers: ChoicePoint, LexisNexis, Acxiom, Dun & Bradstreet, and West. While these resellers were all reported by federal agencies to be sources of personal information, their businesses vary. A discussion of this variance in business practices appears in the background section of this report.

<sup>40</sup>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.

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, resellers generally limited the extent to which individuals could gain access to personal information held about themselves, and because they obtain their information from other sources, most resellers also had limited provisions for correcting or deleting inaccurate information contained in their databases (relevant to the *individual participation* principle).<sup>41</sup> Instead, they directed individuals wishing to make corrections to contact the original sources of the data. Table 7 provides an overview of information resellers' application of the Fair Information Practices.

**Table 7: Information Resellers' Application of Principles of the Fair Information Practices**

Principle	Resellers' application
<i>Collection limitation.</i> 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.	Resellers do not limit collections to specific purposes but collect large amounts of personal information, within the bounds of the law. Further, in many cases, individuals do not know that their personal information is being collected by the reseller, even though they may have known of the original (source) collection.
<i>Data quality.</i> 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.	Although they often have measures in place for ensuring data accuracy in the aggregate, resellers do not ensure that the information they provide is accurate, complete, and current for a specific purpose. Instead, they monitor and rely on the quality controls of the original data source.
<i>Purpose specification.</i> 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.	Resellers disclose general categories of purposes for their data collection rather than specific purposes. They obtain information originally collected for specific purposes and generally offer it for a much wider range of purposes.

<sup>41</sup>Several information resellers reported that if the inaccuracy was a result of their error (e.g., transposing numbers or letters or incorrectly aggregating information), they would correct the data in their databases.

---

(Continued From Previous Page)

Principle	Resellers' application
<i>Use limitation.</i> Personal information should not be disclosed or otherwise used for other than a specified purpose without consent of the individual or legal authority.	Resellers generally limit the use of information as required by law rather than on the basis of the purposes originally specified when the information was collected. Resellers generally pass responsibility for legal use restrictions to customers through licensing and contract terms and agreements. Customers must contractually agree to appropriate uses of the data and must agree to comply with applicable laws.
<i>Security safeguards.</i> Personal information should be protected with reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification, or disclosure.	Resellers reported implementing a variety of security safeguards, such as stringent customer credentialing, to improve protection of personal information.
<i>Openness.</i> The public should be informed about privacy policies and practices, and individuals should have ready means of learning about the use of personal information.	Resellers generally inform the public of key aspects of privacy policies through Web sites, brochures, and so on.
<i>Individual participation.</i> 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.	Although information resellers allow individuals access to their personal information, this access is generally limited, as is the opportunity to make corrections. Generally, resellers only correct errors they may have introduced in the process of obtaining and aggregating data.
<i>Accountability.</i> Individuals controlling the collection or use of personal information should be accountable for taking steps to ensure the implementation of these principles.	Resellers reported taking actions, such as designating a chief privacy officer or equivalent, to ensure compliance with their privacy policies. Annual privacy audits were conducted in one case.

Source: GAO analysis of reseller information.

Note: We did not evaluate the effectiveness of information reseller practices, only the extent to which resellers applied the Fair Information Practices.

---

## Information Resellers Generally Did Not Report Limiting Their Data Collection to Specific Purposes or Notifying Individuals about Them

According to the *collection limitation* principle of the Fair Information Practices, the collection of personal information should be limited, information should be obtained by lawful and fair means, and, where appropriate, it should be collected with the knowledge and consent of the individual. The collection limitation principle also suggests that organizations could limit collection to the minimum amount of data necessary to process a transaction.

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). One reseller reported that it also restricts collection of Social Security number information from public records, as well as collection of identifying information on children from public sources, such as telephone directories.

---

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. For example, resellers collect personal information from a wide variety of sources, including state motor vehicle records; local government records on births, real property, and voter registrations; and various court records. Information resellers may also obtain information from telephone directories, Internet sites, and consumer applications for products or services. The widely varying sources and types of information demonstrate the broad nature of the collection of personal information. The amount and scope of information collected vary from company to company, and resellers use this information to offer a range of products tailored to different markets and uses.<sup>42</sup>

Regarding the principle that information should be obtained by lawful and fair means, resellers stated that they take steps to ensure that their collection of information is legal. For example, resellers told us that they obtain assurances from their data suppliers that information is legally collected from reputable sources. Further, they design their products and services to ensure they are in conformance with laws such as the Gramm-Leach-Bliley Act and the Fair Credit Reporting Act.

Regarding the principle that, where appropriate, information should be collected with the knowledge and consent of the individual, 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 may not be appropriate or practical for them to provide notice or obtain consent from individuals because they do not collect information directly from them. One reseller noted that in many instances the company does not have a direct relationship with the data subject and is therefore not in a position to interact with the consumer for purposes

---

<sup>42</sup>One reseller reported that it maintains discrete databases developed and tailored toward its specific product offerings in marketing, fraud prevention, and directory services. These product offerings are geared toward specific clients. For example, the reseller's fraud prevention product makes use of public record and publicly available information as well as credit header information. The fraud prevention product provides identity verification and investigative tools primarily to the financial and insurance industries and to law enforcement agencies involved in fraud or criminal investigations. Within the four agencies, use of this reseller was reported only as part of TSA's Secure Flight commercial data test.

---

such as providing notice. Further, this reseller stated its belief that requiring resellers to notify and obtain consent from each individual about whom they obtain information would result in consumers being overwhelmed with notices and negate the value of notice.

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 and only under limited circumstances. For example, one reseller allows consumers to opt out of its marketing products but not other products, such as background screening and fraud detection products. The privacy policy for another information reseller states that it will allow certain individuals to opt out of its nonpublic information databases containing sensitive information under specific conditions: if the individual is a state, local, or federal law enforcement officer or public official whose position exposes him or her to a threat of imminent harm; if the individual is a victim of identity theft; or if the individual is at risk of physical harm. In order to exercise this option, consumers generally must provide satisfactory documentation to support the basis for their request. In any event, the reseller retains the right to determine (1) whether to grant or deny any request, (2) to which databases the request for removal will apply, and (3) the duration of the removal. Two resellers stated their belief that under certain circumstances it may not be appropriate to provide consumers with opportunities for opting out, such as for information products 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.

---

### Information Resellers Do Not Ensure That Personal Information They Provide Is Accurate for Specific Purposes

According to the *data quality* principle, 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. 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.

While not providing specific assurance of the accuracy of the data they provide, information resellers reported that they take steps to ensure that their suppliers have data quality controls in place. For example, officials from one information reseller said they use a screening process to help determine whether they should use a particular supplier.<sup>43</sup> As part of this process, the reseller assesses whether the supplier has internal controls in place that are in line with the reseller's policies. Information resellers also reported that they conduct annual audits of their suppliers aimed at assessing the integrity and quality of the information they receive. If these audits show that a supplier has failed to provide accurate, complete, and timely information, the reseller may discontinue using that supplier.

Resellers also noted that data accuracy is contingent upon intended use. That is, data that may be perfectly adequate for one purpose may not be precise enough or appropriate for another purpose. While end users, such as federal agencies, may address data quality for their specific purposes, resellers—who maintain personal information for multiple purposes—are less able to achieve accuracy because they support multiple uses. Thus, resellers generally disclaim data accuracy and leave it to their customers to ensure that the data are accurate for their intended uses. One reseller stated that their customers understand the accuracy limitations of the data they obtain and take the potential for data inaccuracy into account when using the data.

---

<sup>43</sup>While a significant amount of reseller information comes from public records, resellers also use private companies, including other companies that aggregate information, as suppliers. For example, a reseller may contract with another private firm to obtain telephone book information. Further, resellers may contract with other private firms to collect information from public records sources.

---

---

## Information Resellers' Specification of the Purpose of Data Collection Consists of Broad Descriptions of Business Categories

According to the *purpose specification* principle, 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. 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.

In a general sense, information resellers specify their purpose by indicating (on company Web sites, for example) the business categories of the customers for whom they collect information. For example, reseller privacy policies generally state that resellers make personal information available for legitimate uses by business and government organizations. Examples of business categories may be provided, but resellers do not specify which types of information are to be used in which business categories. 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 applied, rather than a specific use, as envisioned in the Fair Information Practices.

---

---

## Information Resellers Generally Limit the Use of Information as Required by Law, Rather Than on the Basis of Purposes Originally Specified When the Information Was Collected

Under the *use limitation* principle, personal information should not be disclosed or used for other than the originally specified purpose without consent of the individual or legal authority. However, 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. 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.



---

According to two large information resellers, customers are generally contractually required to use data from resellers appropriately and must agree to comply with applicable laws, such as the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, and the Driver's Privacy Protection Act. For example, one information reseller uses a service agreement that includes provisions governing permissible use of information sought by the customer, the confidentiality of information provided, legal requirements under federal and state laws, and other customer obligations. The reseller reported that the company monitors its customers' compliance by conducting periodic audits and taking appropriate actions in response to any audit findings.

In a standardized agreement form used by another reseller, federal agencies must certify that they will use information obtained from the reseller only as permissible under the Gramm-Leach-Bliley Act and the Driver's Privacy Protection Act. The service agreement identifies permissible purposes for information whose use is restricted by these laws and requires agencies to agree that they will use the information only in the performance or the furtherance of appropriate government activities. In conformance with the Gramm-Leach-Bliley Act permissible uses, the information reseller requires agencies to certify that they will use personal information "only as requested or authorized by the consumer."

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 is limited to certain customers and uses. For example, two resellers reported that they provide full Social Security numbers and driver's license numbers only to specific types of customers, including law enforcement agencies and insurance companies, and for purposes such as employment or tenant screening. While actions such as these are useful in protecting privacy and are consistent with the use limitation principle in that they narrow the range of potential uses for this type of information, they are not equivalent to limiting use only to a specific predefined purpose. Without limiting use to predefined purposes, resellers cannot provide individuals with assurance that their information will only be accessed and used for the purpose originally specified when the information was collected.

---

---

## Information Resellers Reported Taking Steps to Improve Security Safeguards

According to the *security safeguards* principle, personal information should be protected with reasonable safeguards against risks such as loss or unauthorized access, destruction, use, modification, or disclosure. 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. Resellers also generally had information security plans describing, among other things, access controls for information and systems, document management practices, incident reporting, and premises security.

Given recent incidents, large information resellers reported having recently taken steps to improve their safeguards against unauthorized access. In a well-publicized incident, in February 2005, ChoicePoint disclosed that unauthorized individuals had gained access to personal information by posing as a firm of private investigators. In the following month, LexisNexis disclosed that unauthorized individuals had gained access to personal information through the misappropriation of user IDs and passwords from legitimate customers. These disclosures were required by state law, as previously discussed. In January 2006, ChoicePoint reached a settlement with the Federal Trade Commission<sup>44</sup> over charges that the company did not have reasonable procedures to verify the identity of prospective new users. The company agreed to implement new procedures to ensure that it provides consumer reports only to legitimate business for lawful purposes. In the mean time, both information 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 order for customers of this reseller to obtain products and services containing sensitive personal information, they must now undergo a credentialing process involving a site visit by the information reseller to verify the accuracy of information

---

<sup>44</sup>In its settlement with ChoicePoint, the Federal Trade Commission alleged violations of the Fair Credit Reporting Act and section 5 of the Federal Trade Commission Act. Section 5 of the act prohibits "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission can issue orders, obtain injunctions, impose civil penalties, and undertake civil actions to enforce the act. 5 U.S.C. § 45.

---

reported about the business. Applicants are then scored against a credentialing checklist to determine whether they will be granted access to sensitive information. In addition, both resellers reported efforts to strengthen user ID and password protections and restrict access to sensitive personal information (including full driver's license numbers and Social Security numbers) to a limited number of customers, such as law enforcement agencies (others would be able to view masked information). Although we did not test the effectiveness of these measures, if implemented correctly, they could help provide assurance that sensitive information is protected appropriately.

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. Officials at one reseller told us that security profiles were established for each employee that restrict access to various sections of the center based upon employee job functions. Computer rooms were further protected with a combined system of biometric hand readers and security codes. Security cameras were placed throughout the facility for continuous recording of activity and review by security staff. Information resellers also had contingency plans in place to continue or resume operations in the event of an emergency.

Information resellers reported that on an annual basis, or more frequently if needed, they conduct security risk assessments as well as internal and external security audits. These assessments address such topics as vulnerabilities to internal or external security threats, reporting and responding to security incidents, controls for network and physical facilities, and business continuity management. The assessments also addressed strategies for mitigating potential or identified risks.

If properly implemented, security measures such as those reported by information resellers could contribute to effective implementation of the *security safeguards* principle.

---

---

## Information Resellers Generally Informed the Public about Their Privacy Policies and Practices

According to the *openness* principle, the public should be informed about an organization's privacy policies and practices, and individuals should have ready means of learning about the organization's use of personal information.

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. Several Web sites also provided advice to consumers on protecting personal information and discussed what to do if individuals suspect they are victims of identity theft.

Providing public notice of privacy policies informs individuals of what steps an organization takes to protect the privacy of the personal information it collects and helps to ensure the organization's accountability for its stated policies.

---

## Information Reseller Policies Generally Allow Individuals Limited Ability to Access and Correct Their Personal Information

According to the *individual participation* principle, individuals should have the right to know about the collection of personal information, to access that information, to request correction, and to challenge the denial of those rights. Information resellers generally allow individuals access to their personal information. However, this access is limited, as is the opportunity to make corrections. 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. For example, one information reseller stated that it offers a free report, under certain circumstances, on an individual's claims history, employment history, or tenant history. Resellers may offer basic reports to individuals at no cost, but they generally charge for reports on additional information. A free consumer report, such as an employment history report, for example, typically excludes information such as driver's license data, family information, and credit header data that a reseller may possess in other databases.

---

Although individuals can access information about themselves, if they find inaccuracies, they generally cannot have these corrected by the resellers.<sup>45</sup> Information resellers direct individuals to take their cases to the original data sources—such as courthouses or other local government agencies—and attempt to have the inaccuracy corrected there. Several resellers stated that they would correct any identified errors introduced through their own processing and aggregation of data. As discussed above, resellers, as a matter of policy, do not make corrections to data obtained from other sources, even if the consumer provides evidence that the data are wrong.

According to resellers, making corrections to their own databases is extremely difficult, for several reasons. First, the services these resellers provide concentrate on providing references to a particular individual from many sources, rather than distilling only the most accurate or current reference. For example, a reseller might have many instances in its databases of a particular individual's current address. Although most might be the same, there could be errors as well. Resellers generally would report the information as they have it rather than attempting to determine which entry is correct. This information is important to customers such as law enforcement agencies. Further, resellers stated that making corrections to their databases could be ineffective because the data are continually refreshed with updated data from the source, and thus any correction is likely to be changed back to its original state the next time the data are updated. In addition, as discussed in the collection limitation section, resellers stated their belief that it would not be appropriate to allow the public to access and correct information held for certain purposes, such as fraud detection and locating criminals, since providing such rights could undermine the effectiveness of these uses (e.g., by allowing criminals to access and change their information). However, as a result of these practices, individuals cannot know the full extent of personal information maintained by resellers or ensure its accuracy.

---

<sup>45</sup>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.

---

---

## Information Resellers Report Measures to Ensure Accountability for the Collection and Use of Personal Information

According to the *accountability* principle, individuals controlling the collection or use of personal information should be accountable for taking steps to ensure the implementation of the Fair Information Practices. 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 (e.g., the Gramm-Leach-Bliley Act and the Driver's Privacy Protection Act). Information resellers reported that these officials had a range 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 (e.g., cell phone records).

Auditing of an organization's practices is one way of ensuring accountability for adhering to privacy policies and procedures. 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.

Establishing accountability is critical to the protection of privacy. Actions taken by data resellers should help ensure that their privacy policies are appropriately implemented.

---

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

Agency practices for handling personal information acquired from information resellers did not always fully reflect the Fair Information Practices. Further, agencies generally lacked policies that specifically address their use of personal information from commercial sources, although DHS Privacy Office officials reported that they were drafting such a policy. As shown in table 8, four of the Fair Information Practices—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 *data quality* principle that data should be accurate, current, and complete. Agency policies and practices with regard to the other four principles, however, 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 application of 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, which often are not conducted, are a valuable tool that could address important aspects of the Fair Information Practices. 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 8: 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
<i>Collection limitation.</i> 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.
<i>Data quality.</i> 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.
<i>Purpose specification.</i> 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.
<i>Use limitation.</i> 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).
<i>Security safeguards.</i> 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).

(Continued From Previous Page)

Principle	Agency application of principle	Agency practices
<i>Openness.</i> 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 <i>Purpose specification</i> above. Agencies did not have established policies specifically addressing the use of personal information obtained from resellers.
<i>Individual participation.</i> 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 <i>Purpose specification</i> above. Because agencies generally did not disclose their collections of personal information from resellers, individuals were often unable to exercise these rights.
<i>Accountability.</i> 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 (footnote 2 in app. I lists these components). We did not obtain information on smaller components of Justice and DHS.

### Agency Procedures Reflect the Collection Limitation, Data Quality, Use Limitation, and Security Safeguards Principles

The *collection limitation* principle establishes, among other things, that organizations should obtain only the minimum amount of personal data necessary to process a transaction. This principle also underlies the Privacy Act requirement that agencies maintain in their records “only such information about an individual as is relevant and necessary to accomplish a purpose of the agency.”<sup>46</sup> Regarding most law-enforcement and counterterrorism purposes, which accounted for 90 percent of usage in

<sup>46</sup> 5 U.S.C. § 552a (e)(1). The Privacy Act (at § 552a (j) & (k)) allows agencies to claim an exemption from this provision if the records are used for certain purposes. For example, records compiled for criminal law enforcement purposes or for a broader category of investigative records compiled for criminal or civil law enforcement purposes can be exempted from this requirement.



---

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.<sup>47</sup> Having initiated investigations on specific individuals, however, agencies generally reported that they obtained as much personal information as possible about the individuals being investigated, because law enforcement investigations require pursuing as many investigative leads as possible.

The *data quality* principle states that, among other things, personal information should be relevant to the purpose for which it is collected and be accurate. This principle is mirrored in the Privacy Act's requirement for agencies to maintain all records used to make determinations about an individual with sufficient accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness.<sup>48</sup>

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. Officials from several law enforcement component agencies, including ATF and DEA, said corroboration was necessary to build legally sound cases from investigations. For example, U.S. Secret Service officials reported that they instruct agents that the information obtained from resellers should be independently corroborated, and that none of it should be used as probable cause for obtaining warrants.

Further, FBI officials from FTTTF noted that obtaining data from information resellers helps to improve the overall quality and accuracy of the data in investigative files. Officials stated that the variety of private companies providing personal information enhances the value, quality, and diversity of the information used by the FBI, noting that a decision to put

---

<sup>47</sup>In two cases, agency components used reseller data to conduct broader searches for previously unidentified criminal behavior. These two cases were an application at DEA used to identify potential prescription drug fraud and efforts by Citizenship and Immigration Services to detect large patterns of potential fraud through address searches and other queries.

<sup>48</sup>5 U.S.C. § 552a(e)(5). The Privacy Act allows agencies to claim an exemption from this provision of the act for certain designated purposes. For example, records compiled for criminal law enforcement purposes can be exempt from this provision. A broader category of investigative records compiled for criminal or civil law enforcement purposes cannot be exempt from this provision.

---

an individual under arrest is based on “probable cause,” which is determined by a preponderance of evidence, rather than any single source of information, such as information in a reseller’s data base.

Likewise, for non law-enforcement use, such as debt collection and fraud detection and prevention, agency components reported procedures for mitigating potential problems with the accuracy of data provided by resellers by obtaining additional information from other sources when necessary. For example, the Executive Office for U.S. Attorneys uses information resellers to obtain information on assets possessed by an individual indebted to the United States. According to officials, should information contained in the information reseller databases conflict with information provided by an individual, further investigation takes place before any action to collect debts would be taken. Likewise, officials from the U.S. Citizenship and Immigration Services (USCIS) component of DHS and the Office of Consular Affairs within the Department of State reported similar practices. While these practices do not eliminate inaccuracies in data coming into the agency, they help ensure the quality of the information that is the basis for agency actions.

The *use limitation* principle provides that personal information should not be disclosed or used for other than a specified purpose without consent of the individual or legal authority. This principle underlies the Privacy Act requirement that prevents agencies from disclosing records on individuals except with consent of the individual, unless disclosure of the record would be, for example, to another agency for civil or criminal law enforcement activity or for a purpose that is compatible with the purpose for which the information was collected.<sup>49</sup>

Although agencies rely on resellers’ multipurpose collection of information as a source, agency officials said their use of reseller information was limited to distinct purposes, which were generally related to law enforcement or counterterrorism. For example, the Department of Justice reported uses specific to the conduct of criminal investigations on individuals, terrorism investigations, and the location of assets and witnesses. Other Justice and DHS components, such as the Federal Protective Service, U.S. Secret Service, FBI, and ATF, also reported that they used information reseller data for investigations. For uses not related

---

<sup>49</sup>Such uses are referred to as “routine uses” in the Privacy Act, 5 U.S.C. § 552a (a(7)) and (b).

---

to law enforcement, such as those reported by State and SSA, use of reseller information was also described as supporting a specific purpose (e.g., fraud detection or debt collection).

The use limitation principle also precludes agencies from sharing personal information they collect for purposes unrelated to the original intended use of the information. Officials of certain law enforcement components of these agencies reported that in certain cases they share information with other law enforcement agencies, a use consistent with the purposes originally specified by the agency. For example, the FBI's FTTTF supports ongoing investigations in other law enforcement agencies and the intelligence community by sharing information obtained from resellers (among other information) in response to requests about foreign terrorists from FBI agents or officials from partner agencies.<sup>50</sup>

The *security safeguards* principle requires that personal information be reasonably protected against unauthorized access, use, or disclosure. This principle also underlies the Privacy Act requirement that agencies establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records on individuals.<sup>51</sup> This principle is further mirrored in the FISMA requirement to protect information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction, including through controls for confidentiality.

While we did not assess the effectiveness of information security or the implementation of FISMA 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.<sup>52</sup> For example, all four agencies cited the use of passwords to prevent unauthorized access to information

---

<sup>50</sup>The task force's partner agencies include ICE, the Department of Defense Counterintelligence Field Activity Office, the Office of Personnel Management, and members of the intelligence community.

<sup>51</sup>5 U.S.C. § 552a(e)(10).

<sup>52</sup>Although we did not assess the effectiveness of information security or compliance with FISMA at any agency as part of this review, we have previously reported on weaknesses in almost all areas of information security controls at 24 major agencies, 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).

---

reseller databases. Further, agency components such as ATF, DEA, CBP, and USCIS, reported that they limit access to sensitive personal information (e.g., full Social Security number, driver's license number) to those with a specific need for this information. Several agency components also reported that resellers were promptly notified to deactivate accounts for employees separated from government service to protect against unauthorized use. As another security measure, several components, including DEA and the FBI, reported that resellers notified them when accounts were accessed from Internet addresses at unexpected locations, such as outside the United States.

Another measure to prevent unauthorized disclosure reported by law enforcement agencies, such as the FBI, ICE, and Secret Service, is the use of "cloaked logging," which prevents vendor personnel from monitoring the queries being made by law enforcement agents. Officials in FBI's FTTTF reported that, in order to maintain the integrity of investigations, resellers are contractually prohibited from tracking or monitoring the exact persons or other entities being searched by FTTTF personnel. Law enforcement officials stated that the ability to mask searches from vendors is important so that those outside law enforcement have no knowledge of who is being investigated and so that subjects of an investigation are not "tipped off."

Agency adherence to the *collection limitation, data quality, use limitation, and security safeguards* principles was based on general business procedures—including law-enforcement investigative practices—that reflect security and civil liberties protections, rather than written policies specifically regarding the collection, accuracy, use, and security of personal information obtained from resellers. Implementation of these practices provides individuals with assurances that only a limited amount of their personal information is being collected, that it is used only for specific purposes, and that measures are in place to corroborate the accuracy of the information and safeguard it from improper disclosure. These controls help prevent potential harm to individuals and invasion of their privacy by limiting the exposure of their information and reducing the likelihood of inaccurate data being used to make decisions that could affect their welfare.

---

---

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, among other things, that individuals should be made aware of the purpose and intended uses of the personal information being collected about them and have the ability to access and correct such information, if necessary. The Privacy Act reflects these principles in part by requiring 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.<sup>53</sup>

In a number of cases, agencies did not adhere to the *purpose specification* or *openness* principles in regard to their use of reseller information 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.<sup>54</sup> OMB guidance on implementing the Privacy Act does not 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

---

<sup>53</sup>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.

<sup>54</sup>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).

---

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.<sup>55</sup> Other programs that involve use of information reseller data include the fraud prevention and detection programs reported by SSA and State as well as law enforcement programs within ATF, the U.S. Marshals, and USCIS. For these programs, associated system of records notices identified by officials did not specify the use of information reseller data.

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.<sup>56</sup> In one case, a notice indicated incorrectly that personal information was collected only from the individuals concerned. Specifically, USCIS prepared a system of records notice covering the Computer Linked Application Information Management System, which did not identify information resellers as a source. Instead,

---

<sup>55</sup>As we previously reported, this notice did not fully disclose the scope of the use of reseller data during the test phase. See [GAO-05-864R](#).

<sup>56</sup>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. 5 U.S.C. § 552a (j) and (k). One system of records notice for the Treasury Enforcement Communications System (the system identified by ATF as covering their investigative case files) claimed such an exemption. The Department of State identifies categories of sources in the system of records notices it identified but does not specifically identify use of reseller data. The State system of records notices also claim an exemption from identifying categories of sources but invoke that exemption only under certain circumstances (e.g., to the extent that a specific investigation would be compromised).

---

the notice stated only that “information contained in the system of records is obtained from individuals covered by the system.”<sup>57</sup>

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

The *individual participation* principle gives individuals the right to access and correct information that is maintained about them. However, under the Privacy Act, agencies can claim exemptions from the requirement to provide individual access and the ability to make corrections if the systems are for law enforcement purposes.<sup>58</sup> In most cases where officials identified system-of-record notices associated with reseller data collection for law enforcement purposes, agencies claimed this exemption. Like the ability to mask database searches from vendors, this provision is important so that the subjects of law enforcement investigations are not tipped off.

Aside from the law enforcement exemptions 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

---

<sup>57</sup>The notice was last updated in October 2002, before the service and benefit functions of the U.S. Immigration and Naturalization Service transitioned into DHS as U.S. Citizenship and Immigration Services.

<sup>58</sup>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.

---

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 Are Often Not Conducted

The PIA is an important tool for agencies to address privacy early in the process of developing new information systems, and to the extent that PIAs are made publicly available,<sup>59</sup> 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. In doing so, they serve to address the *openness* and *purpose specification* principles.

However, only three agency components reported developing PIAs for their systems or programs that make use of information reseller data.<sup>60</sup> 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.”<sup>61</sup> 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

---

<sup>59</sup>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).

<sup>60</sup>The agency components that identified preparation of PIAs for systems or programs making use of information reseller data included USCIS for its Fraud Tracking System, TSA for its Secure Flight commercial data test, and FBI's FTTTF, which reported that it was in the process of finalizing a PIA. Only the PIA for TSA's test specifically identified the use of commercial data. We were unable to determine if FTTTF's PIA identified the use of commercial data since it was not yet final.

<sup>61</sup>OMB, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, Memorandum M-03-22 (Washington, D.C.: Sept. 26, 2003).



---

make their own judgments on whether retaining the results of searches of information reseller databases constituted a “systematic incorporation” of information.

DHS has recently developed guidance requiring PIAs to be conducted whenever reseller data are involved. The DHS Privacy Office<sup>62</sup> guidance on conducting PIAs points out, for example, that a program decision to obtain information from a reseller would constitute a new source of information, requiring that a PIA be conducted. 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.”<sup>63</sup> 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.”

In one case, a DHS component prepared a PIA for a system that collects reseller data but had not identified in the assessment that resellers were being used. DHS’s USCIS uses copies of court records obtained from an information reseller to support evidentiary requirements for official adjudication proceedings concerning fraud. Although this use was reported to be covered by the PIA for the office’s Fraud Tracking System, the PIA identifies only “public records” as the source of its information and does not mention that the public records are obtained from information resellers.<sup>64</sup> In contrast, the draft DHS guidance on PIAs instructs DHS component agencies to “list the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from another source such as a commercial data aggregator.” At the time of our review, this draft guidance had not yet been

---

<sup>62</sup>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.”

<sup>63</sup>Department of Homeland Security Privacy Office, *Privacy Impact Assessments: Official Guidance* (March 2006), p. 34.

<sup>64</sup>USCIS officials stated that the PIA for the Fraud Tracking System, now called the Fraud Detection and National Security System, would be updated on an incremental basis and that a future update would identify information resellers as a data source.

---

disseminated to DHS components. Lacking such guidance, DHS components did not have policies in place regarding the conduct of PIAs with respect to reseller data, nor did other agencies we reviewed.

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.

---

### 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 taking steps to ensure the implementation of the Fair Information Practices), agencies should take steps to ensure that employee uses of personal information from information resellers are appropriate. While agencies described activities to oversee the use of information resellers, such activities were largely based on trust of the user to use the information appropriately. For example, in describing controls placed on the use of commercial data, officials from component agencies identified measures such as instructing users that reseller data are for official use only and requiring users to sign statements of responsibility attesting to a need to access the information reseller databases and that their use will be limited to official business. Additionally, agency officials reported that in accessing reseller databases, users are required to select from a list of vendor-defined “permissible purposes” (e.g., law enforcement, transactions authorized by the consumer) before conducting a search. While these practices appear consistent with the accountability principle, they are focused on individual user responsibility rather than management oversight.

For example, 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. For example, one information reseller reported that it does not provide reports to agencies on the “permissible purpose” that a user selects before conducting a search.

Not all component agencies lacked robust user monitoring. Specifically, according to FBI officials from the FTTTF, their network records and monitors searches conducted by the user account, including who is

---

searched against what public source database. The system also tracks the date and time of the query as well as what the analyst does with the data. FBI officials stated that the vendor reports as well as the network monitoring provide FBI with the ability to detect unusual usage of the public source providers.

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.

---

## Conclusions

Services provided by information resellers serve as important tools that can enhance 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. 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. 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. To more fully embrace these principles could require resellers to change the way they conduct business, and currently resellers are not legally required to follow them. 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.

Agencies take steps to adhere to Fair Information Practices such as the *collection limitation*, *data quality*, *use limitation*, and *security safeguards* principles. However, 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. Specifically, agencies did not always have policies or practices in place to address the *purpose specification*, *individual participation*, *openness*, and *accountability* principles with respect to reseller data. An important

---

factor contributing to this is that OMB privacy guidance does not clearly address information reseller data, which has become such a valuable and useful tool for agencies. As a result, 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.

---

## Matter for Congressional Consideration

In considering legislation to address privacy concerns related to the information reseller industry, Congress should consider the extent to which the industry should adhere to the Fair Information Practices.

---

## Recommendations for Executive Action

To improve accountability, ensure adequate public notice of agencies' use of personal information from commercial sources, and allay potential privacy concerns arising from agency use of information from such sources, we are making three recommendations to the Director of OMB and the heads of the four agencies. Specifically, we recommend that:

- the Director of OMB revise guidance on system of records notices and privacy impact assessments to clarify the applicability of the governing laws (the Privacy Act and the E-Government Act) to the use of personal information from resellers. These clarifications should specify the circumstances under which agencies should make disclosures about their uses of reseller data so that agencies can properly notify the public (for example, what constitutes a "systematic" incorporation of reseller data into a federal system). The guidance should include practical scenarios based on uses agencies are making of personal information from information resellers (for example, visa, criminal, and fraud investigations).
- the Director of OMB direct agencies to review their uses of personal information from information resellers, as well as any associated system of records notices and privacy impact assessments, to ensure that such notices and assessments explicitly reference agency use of information resellers.

- 
- the Attorney General, the Secretary of Homeland Security, the Secretary of State, and the Commissioner of SSA develop specific policies for the collection, maintenance, and use of personal information obtained from resellers that reflect the Fair Information Practices, including oversight mechanisms such as the maintenance and review of audit logs detailing queries of information reseller databases—to improve accountability for agency use of such information.

---

## Agency Comments and Our Evaluation

We received written comments on a draft of this report from the Justice's Assistant Attorney General for Administration (reproduced in appendix III), from the Director of the DHS Departmental GAO/OIG Liaison Office (reproduced in appendix IV), from the Commissioner of SSA (reproduced in appendix V), and from State's Assistant Secretary and Chief Financial Officer (reproduced in appendix VI). We also received comments via E-mail from staff of OMB's Office of Information and Regulatory Affairs. Justice, DHS, SSA, and OMB all generally agreed with the report and described actions initiated to address our recommendations. Justice and SSA also provided technical comments, which has been incorporated in the final report as appropriate.

In its comments, Justice agreed that revised or additional guidance and policy could be created to address unique issues presented by use of personal information obtained from resellers. However, noting that the Privacy Act allows law enforcement agencies to exempt certain records from provisions of the law that reflect aspects of the Fair Information Practices, Justice recommended that prior to issuance of any new or revised policy, careful consideration be given to the balance struck in the Privacy Act on applying the Fair Information Practices to law enforcement data. We recognize that law enforcement purposes are afforded the opportunity for exemptions from some of the provisions of the Privacy Act. The report acknowledges this fact. We also agree and acknowledge in the report that the Fair Information Practices serve as a framework of principles for balancing the need for privacy with other public policy interests, such as national security and law enforcement.

DHS also agreed on the importance of guidance to federal agencies on the use of reseller information and stated that it is working diligently on finalizing a DHS policy for such use. The agency commented that its Privacy Office has been reviewing the use and appropriate privacy protections for reseller data, including conducting a 2-day public workshop on the subject in September 2005. DHS also noted that it had just issued

---

departmentwide guidance on the conduct of privacy impact assessments in March 2006, which include directions relevant to the collection and use of commercial data. We have made changes to the final report to reflect the recent issuance of the DHS guidance.

SSA noted in its comments that it had established internal controls, including audit trails of systems usage, to ensure that information is not improperly disclosed. SSA also stated that it would amend relevant system-of-record notices to reflect use of information resellers and would explore options for enhancing its policies and internal controls over information obtained from resellers.

State interpreted our draft report to “rest on the premise that records from ‘information resellers’ should be accorded special treatment when compared with sensitive information from other sources.” State indicated that it does not distinguish between types of information or sources of information in complying with privacy laws. However, our report does not suggest that data from resellers should receive special treatment. Instead, our report takes the widely accepted Fair Information Practices as a universal benchmark of privacy protections and assesses agency practices in comparison with them. State also interpreted our draft report to state that fraud detection, as a purpose for collecting personal information, is not related to law enforcement. However, the draft does not make such a claim. We have categorized agency uses of personal information based on descriptions provided by agencies and have categorized fraud detection uses separately from law enforcement to provide insight into different types of uses. We do not claim the two uses are unrelated. Finally, the department stated that in its view, it would be bad policy to require specification of sources such as data resellers in agency system of records notices. In contrast, we believe that adding clarity and specificity about sources is in the spirit of the purpose specification practice and note that DHS has recently issued guidance on privacy impact assessments that is consistent with this view.

OMB stated that, based on a staff-level meeting of agency privacy experts, it believes agencies recognize that when personal data are brought into their systems, this fact must be reflected in their privacy impact assessments and system-of-record notices. We do not find this observation inconsistent with our findings. We found, however, that inconsistencies occurred in agencies’ determinations of when or whether reseller information was actually brought into their systems, as opposed to being merely “accessed” on an ad-hoc basis. We believe clarification of this issue

---

is important. OMB further stated that agencies have procedures in place to verify commercial data before they are used in decisions involving the granting or recoupment of benefits or entitlements. Again, this is not inconsistent with the results of our review. Finally OMB stated that it would discuss its guidance with agency senior officials for privacy to determine whether additional guidance concerning reseller data is needed.

---

## Comments from Information Resellers

We also obtained comments on excerpts of our draft report from the five information resellers we reviewed. General comments made by resellers and our evaluation are summarized below:

- Several resellers raised concerns about our reliance on the OECD version of the Fair Information Practices as a framework for assessing their privacy policies and business practices. They suggested that it would be unreasonable to require them to comply with aspects of the Fair Information Practices that they believe were intended for other types of users of personal information, such as organizations that collect information directly from consumers. Further, they commented that our draft summary appeared to treat strict adherence to all of the Fair Information Practices as if it were a legally binding requirement. In several cases, they suggested that it would be more appropriate for us to use the privacy framework developed by the Asia-Pacific Economic Cooperation (APEC) organization in 2004, because the APEC framework is more recent and because it explicitly states that it has limited applicability to publicly available information.
- As discussed in our report, the OECD version of the Fair Information Practices is widely used and cited within the federal government as well as internationally. In addition, the APEC privacy framework, which was developed as a tool for encouraging the development of privacy protection in the Asia Pacific region, acknowledges that the OECD guidelines are still relevant and “in many ways represent the international consensus on what constitutes honest and trustworthy treatment of personal information.”<sup>65</sup> Further, our use of the OECD guidelines is as an analytical framework for identifying potential privacy issues for further consideration by Congress—not as legalistic compliance criteria. The report states that the Fair Information

---

<sup>65</sup>Asia-Pacific Economic Cooperation, *APEC Privacy Framework*, Version 4 (Santiago, Chile: Nov. 17-18, 2004), p. 4.

---

Practices are not precise legal requirements; rather they provide a framework of principles for balancing the needs for privacy against other public policy interests, such as national security, law enforcement, and administrative efficiency. In conducting our analysis, we noted that the nature of the reseller business is largely at odds with the principles of *collection limitation*, *data quality*, *purpose specification*, and *use limitation*. We also noted that resellers are not currently required to follow the Fair Information Practices and that for resellers to more fully embrace them could require that they change the way they do business. We recognize that it is important to achieve an appropriate balance between the benefits of resellers' services and the public's right to privacy and point out that, as Congress weighs various legislative options, it will be critical to determine an appropriate balance. We have made changes in this report to clarify that we did not attempt to make determinations of whether or how information reseller practices should change and that such determinations are a matter of policy based on balancing the public's right to privacy with the value of reseller services.

- Several information resellers stated that the draft did not take into account that public record information is freely available. For example, one reseller stated that public records should be understood by consumers to be open to all for any use not prohibited by state or federal law. Another stated that information resellers merely effectuate the determination made by governmental entities that public records should be open to all.

However, the views expressed by the resellers do not take into account several important factors. First, resellers collect information for their products from a variety of sources, including information provided by consumers to businesses. Resellers products are not based exclusively on public records. Thus a consideration of protections for public record information does not take the place of a full assessment of the information reseller business. Second, resellers do not merely pass on public record information as they find it; they aggregate information from many different sources to create new information products, and they make the information much more readily available than it would be if it remained only in paper records on deposit in government facilities. The aggregation and increased accessibility provided by resellers raises privacy concerns that may not apply to the original paper-based public records. Finally, it is not clear that individuals give up all privacy rights to personal information contained in public records. The Supreme Court has expressed the opinion in the past that



---

individuals retain a privacy interest in publicly released personal information. We therefore 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 may be made about the appropriate balance between resellers' services and the public's right to privacy.

- Several resellers also noted that the draft report did not address the complexity of the reseller business—the extent to which resellers' businesses vary among themselves and overlap with consumer reporting agencies. We have added text addressing this in the final report.

The resellers also provided technical comments, which were incorporated in the final report as appropriate.

---

We are sending copies of this report to the Attorney General, the Secretary of Homeland Security, the Secretary of State, the Commissioner of the Social Security Administration, the Director of the Office of Management and Budget, and other interested congressional committees. Copies will be made available to others on request. In addition, this report will be available at no charge on our Web site at [www.gao.gov](http://www.gao.gov).

If you have any questions concerning this report, please call me at (202) 512-6240 or send E-mail to [koontzl@gao.gov](mailto:koontzl@gao.gov). Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Major contributors to this report are John de Ferrari, Assistant Director; Mathew Bader; Barbara Collier; Pamlutricia Greenleaf; David Plocher; and Jamie Pressman.



Linda D. Koontz  
Director, Information Management Issues

---

*List of Requesters*

The Honorable F. James Sensenbrenner, Jr.  
Chairman

The Honorable John Conyers, Jr.  
Ranking Minority Member  
Committee on the Judiciary  
House of Representatives

The Honorable Steve Chabot  
Chairman

The Honorable Jerrold Nadler  
Ranking Minority Member  
Subcommittee on the Constitution  
Committee on the Judiciary  
House of Representatives

The Honorable Bill Nelson  
Ranking Minority Member  
Subcommittee on International Operations and Terrorism,  
Committee on Foreign Relations  
United States Senate

The Honorable Bennie G. Thompson  
Ranking Minority Member  
Committee on Homeland Security  
House of Representatives

The Honorable Zoe Lofgren  
Ranking Minority Member  
Subcommittee on Intelligence, Information Sharing, and Terrorism  
Risk Assessment  
Committee on Homeland Security  
House of Representatives

The Honorable Loretta Sanchez  
Ranking Minority Member  
Subcommittee on Economic Security, Infrastructure Protection, and  
Cybersecurity  
Committee on Homeland Security  
House of Representatives

---

# Objectives, Scope, and Methodology

---

Our objectives were to determine the following:

- how the Departments of Justice, Homeland Security, and State and the Social Security Administration are making use of personal information obtained through contracts with information resellers;
- the extent to which the information resellers providing personal information to these agencies have policies and practices in place that reflect widely accepted principles for protecting the privacy and security of personal information; and
- the extent to which these agencies have policies and practices in place for handling information reseller data that reflect widely accepted principles for protecting the privacy and security of personal information.

To address our objectives, we identified and reviewed applicable laws such as the Privacy Act of 1974 and the E-Government Act, agency policies and practices, and the widely accepted privacy principles embodied in the Organization for Economic Cooperation and Development (OECD) version of the Fair Information Practices. Working with liaisons at the four federal agencies we were requested to review, we identified officials responsible for the acquisition and use of personal information from information resellers. Through these officials, we obtained applicable contractual documentation such as statements of work, task orders, blanket purchase agreements, purchase orders, interagency agreements, and contract terms and conditions.

To address our first objective, we obtained and reviewed contract vehicles covering federal agency use of information reseller services for fiscal year 2005. We also reviewed applicable General Services Administration (GSA) schedule and Library of Congress FEDLINK contracts with information resellers that agencies made use of by various means, including through issuance of blanket purchase agreements, task orders, purchase orders, or interagency agreements. We analyzed the contractual documentation provided to determine the nature, scope, and dollar amounts associated with these uses, as well as mechanisms for acquiring personal information. In an effort to identify all relevant instances of agency use of information resellers and related contractual documents, we developed a list of structured questions to address available contract documents, uses of personal information, and applicable agency guidance. We provided these questions to agency officials and held discussions with them to help ensure

that they provided all relevant information on uses of personal information from information resellers. To further ensure that relevant contract vehicles were identified, we asked major information resellers about their business with the four agencies. We also interviewed officials from GSA and the Library of Congress to discuss the mechanisms available to federal agencies for acquiring personal information and to identify any additional uses of these mechanisms by the four agencies.

To further address our first objective, we categorized agency use of information resellers into five categories: counterterrorism, debt collection, fraud detection/prevention, law enforcement, and other. These categorizations were based on the component and applicable program's mission, as well as the specific reported use of the contract. In identifying relevant uses of information resellers, we were unable to identify small purchases (e.g., purchases below \$2,500), as agencies do not track this information centrally. In addition, to the extent practicable, we excluded uses that generally did not involve the use of personal information. For example, officials from several component agencies reported that their use of the LexisNexis and West services was primarily for legal research rather than for public records information. In other cases, reported amounts may reflect uses that do not involve personal information because agencies were unable to separate such uses from uses involving personal information.

To address our second objective, we obtained and reviewed relevant private sector laws and guidance, such as the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, and the Fair Information Practices. We also identified major information resellers in agency contractual agreements for personal information and held interviews with officials from these companies, including Acxiom, ChoicePoint, Dun & Bradstreet,<sup>1</sup> LexisNexis, and West, to discuss security, quality controls, and privacy policies. In addition, we conducted site visits at Acxiom, ChoicePoint, and LexisNexis, and obtained written responses to related questions from West. These five resellers accounted for approximately 95 percent of the dollar value of all reported contracts with resellers. To determine the extent that they reflect widely accepted Fair Information Practices, we reviewed and compared information reseller's privacy policies and procedures with these principles. In conducting our analysis, we identified the extent to which

---

<sup>1</sup>Dun & Bradstreet specializes in business information, which may contain personal information on business owners.

reseller practices were consistent with the key privacy principles of the Fair Information Practices. We also assessed the effect of any inconsistencies; however, we did not attempt to make determinations of 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.

To address our third objective, we identified applicable guidelines and management controls regarding the acquisition, maintenance, and use of personal information from information resellers at each of the four agencies. We also interviewed agency officials, including acquisition and program staff, to further identify relevant policies and procedures. Our assessment of overall agency application of the Fair Information Practices was based on the policies and procedures of major components at each of the four agencies.<sup>2</sup> We also conducted interviews at the four agencies with senior agency officials designated for privacy as well as officials of the Office of Management and Budget (OMB) to obtain their views on the applicability of federal privacy laws (including the Privacy Act of 1974 and the E-Government Act of 2002) and related guidance on agency use of information resellers. In addition, we compared relevant policies and management practices with the Fair Information Practices.

We assessed the overall application of the principles of the Fair Information Practices by agencies according to the following categories:

1. *General.* We assessed the application as general if the agency had policies or procedures to address all major aspects of a particular principle.
2. *Uneven.* We assessed the application as uneven if the agency had policies or procedures that addressed some but not all aspects of a

---

<sup>2</sup>We obtained information on policies and practices from the following major components of Justice and DHS. For Justice: Bureau of Alcohol Tobacco, Firearms, and Explosives, Drug Enforcement Administration, Executive Office for U.S. Attorneys, Executive Office of the U.S. Trustees, Federal Bureau of Investigation, and the U.S. Marshals Service. For DHS: U.S. Citizenship and Immigration Services, U.S. Immigration and Customs Enforcement, Transportation Security Administration, U.S. Secret Service, U.S. Customs and Border Protection, and the Federal Emergency Management Agency. We did not obtain information on policies and management practices for smaller components.

---

particular principle or if some but not all components and agencies had policies or practices in place addressing the principle.

We performed our work at the Departments of Homeland Security, Justice, and State in Washington, D.C.; at the Social Security Administration in Baltimore, Maryland; Acxiom Corporation in Little Rock, Arkansas; ChoicePoint in Alpharetta, Georgia; Dun & Bradstreet in Washington, D.C.; and LexisNexis in Washington, D.C., and Miamisburg, Ohio. Our work was conducted from May 2005 to March 2006 in accordance with generally accepted government auditing standards.

---

# Federal Laws Affecting Information Resellers

---

Major laws that affect information resellers include the Gramm-Leach-Bliley Act, the Drivers Privacy Protection Act, the Health Insurance Portability and Accountability Act, the Fair Credit Reporting Act, and the Fair and Accurate Credit Transactions Act. Their major privacy related provisions are briefly summarized below.

---

## Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act requires financial institutions (e.g., banks, insurance, and investment companies) to give consumers privacy notices that explain the institutions' information-sharing practices (P.L. 106-102 (1999), Title V, 15 U.S.C. 6801). In turn, consumers have the right to limit some, but not all, sharing of their nonpublic personal information. Financial institutions are permitted to disclose consumers' nonpublic personal information without offering them an opt-out right in a number of circumstances including the following:

- to effect a transaction requested by the consumer in connection with a financial product or service requested by the consumer; maintaining or servicing the consumer's account with the financial institution or another entity as part of a private label credit card program or other extension of credit; or a securitization, secondary market sale, or similar transaction;
- with the consent or at the direction of the consumer;
- to protect the confidentiality or security of the consumer's records; to prevent fraud; for required institutional risk control or for resolving customer disputes or inquiries; to persons holding a legal or beneficial interest relating to the consumer; or to the consumer's fiduciary;
- to provide information to insurance rate advisory organizations, guaranty funds or agencies, rating agencies, industry standards agencies, and the institution's attorneys, accountants, and auditors;
- to the extent specifically permitted or required under other provisions of law and in accordance with the Right to Financial Privacy Act of 1978, to law enforcement agencies, self-regulatory organizations, or for an investigation on a matter related to public safety;
- to a consumer reporting agency in accordance with the Fair Credit Reporting Act or from a consumer report reported by a consumer reporting agency;

- in connection with a proposed or actual sale, merger, transfer, or exchange of all or a portion of a business if the disclosure concerns solely consumers of such business; and
- to comply with federal, state, or local laws; an investigation or subpoena; or to respond to judicial process or government regulatory authorities.

---

## Driver's Privacy Protection Act

The Driver's Privacy Protection Act generally prohibits the disclosure of personal information by state departments of motor vehicles. (P.L. 103-322 (1994), 18 U.S.C. § 2721-2725). It also specifies a list of exceptions when personal information contained in a state motor vehicle record may be disclosed. These permissible uses include the following:

- for use by any government agency in carrying out its functions;
- for use in connection with matters of motor vehicle or driver safety and theft; motor vehicle emissions; motor vehicle product alterations, recalls, or advisories; motor vehicle market research activities;
- for use in the normal course of business by a legitimate business, but only to verify the accuracy of personal information submitted by the individual to the business and, if such information is not correct, to obtain the correct information but only for purposes of preventing fraud by pursuing legal remedies against, or recovering on a debt or security interest against, the individual;
- for use in connection with any civil, criminal, administrative, or arbitral proceeding in any federal, state, or local court or agency;
- for use in research activities;
- for use by any insurer or insurance support organization in connection with claims investigation activities;
- for use in providing notice to the owners of towed or impounded vehicles;
- for use by a licensed private investigative agency for any purpose permitted under the act;



- for use by an employer or its agent or insurer to obtain information relating to the holder of a commercial driver's license;
- for use in connection with the operation of private toll transportation facilities;
- for any other use, if the state has obtained the express consent of the person to whom a request for personal information pertains;
- for bulk distribution of surveys, marketing, or solicitations, if the state has obtained the express consent of the person to whom such personal information pertains;
- for use by any requester, if the requester demonstrates that it has obtained the written consent of the individual to whom the information pertains; and
- for any other use specifically authorized under a state law, if such use is related to the operation of a motor vehicle or public safety.

---

## Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191) made a number of changes to laws relating to health insurance. It also directed the Department of Health and Human Services to issue regulations to protect the privacy and security of personally identifiable health information. The resulting privacy rule (45 C.F.R. Part 164) defines certain rights and obligations for covered entities (e.g., health plans and health care providers) and individuals, including the following:

- giving individuals the right to be notified of privacy practices and to inspect, copy, request correction, and have an accounting of disclosures of health records, except for specified exceptions;
- setting limits on the use of health information apart from treatment, payment, and health care operations (e.g., for marketing) without the individual's authorization;
- permitting disclosure of health information without the individual's authorization for purposes of public health protection; health oversight; law enforcement; judicial and administrative proceedings; approved research activities; coroners, medical examiners, and funeral directors; workers' compensation programs, government abuse, neglect, and

domestic violence authorities; organ transplant organizations; government agencies with specified functions, e.g., national security activities; and as required by law;

- requiring that authorization forms contain specific types of information, such as a description of the health information to be used or disclosed, the purpose of the use or disclosure, and the identity of the recipient of the information; and
- requiring covered entities to take steps to limit the use or disclosure of health information to the minimum necessary to accomplish the intended purpose, unless authorized or under certain circumstances.

---

## Fair Credit Reporting Act

The Fair Credit Reporting Act (P.L. 91-508, 1970, 15 U.S.C. § 1681) governs the use of personal information by consumer reporting agencies, which are individuals or entities that regularly assemble or evaluate information about individuals for the purpose of furnishing consumer reports to third parties. The act defines a consumer report as any communication by a consumer reporting agency about an individual's credit worthiness, character, reputation, characteristics, or mode of living and permits its use only in the following situations:

- as ordered by a court or federal grand jury subpoena;
- as instructed by the consumer in writing;
- for the extension of credit as a result of an application from a consumer or the review or collection of a consumer's account;
- for employment purposes, including hiring and promotion decisions, where the consumer has given written permission;
- for the underwriting of insurance as a result of an application from a consumer;
- when there is a legitimate business need, in connection with a business transaction that is initiated by the consumer;
- to review a consumer's account to determine whether the consumer continues to meet the terms of the account;

- to determine a consumer's eligibility for a license or other benefit granted by a governmental instrumentality required by law to consider an applicant's financial responsibility or status;
- for use by a potential investor or servicer or current insurer in a valuation or assessment of the credit or prepayment risks associated with an existing credit obligation; and
- for use by state and local officials in connection with the determination of child support payments, or modifications of enforcement thereof.

The act generally limits the amount of time negative information can be included in a consumer report to no more than 7 years, or 10 years in the case of bankruptcies. Under the act, individuals have a right to access all information in their consumer reports; a right to know who obtained their report during the previous year or two, depending on the circumstances; and a right to dispute the accuracy of any information about them.

---

## Fair and Accurate Credit Transactions Act

The Fair and Accurate Credit Transactions Act (P.L. 108-159, 2003) amended the Fair Credit Reporting Act, extending provisions to improve the accuracy of personal information assembled by consumer reporting agencies and better provide for the fair use of and consumer access to personal information. The act's provisions include the following:

- consumers may request a free annual credit report from nationwide consumer reporting agencies, to be made available no later than 15 days after the date on which the request is received;
- persons furnishing information about individuals to consumer reporting agencies, and resellers of consumer reports, must have policies and procedures for investigating and correcting inaccurate information,
- consumers are given the right to prohibit business affiliates of consumer reporting agencies from using information about them for certain marketing purposes; and
- consumer reporting agencies cannot include medical information in reports that will be used for employment, credit transactions, or insurance transactions unless the consumer consents to such disclosures.

# Comments from the Department of Justice



U.S. Department of Justice

MAR 17 2006

Washington, D.C. 20530

Linda Koontz  
Director, Information Management Issues  
U.S. Government Accountability Office  
441 G Street, NW  
Washington, DC 20548

Dear Ms. Koontz:

Thank you for the opportunity to review the final draft of the Government Accountability Office (GAO) report entitled *Privacy: Opportunities Exist for Agencies and Information Resellers to More Fully Adhere to Key Principles* (GAO-06-421/310228). The draft was reviewed by 16 components of the Department of Justice (DOJ) who had participated in this review. Earlier today, the DOJ provided you technical comments to be incorporated in the report as appropriate. This letter constitutes the formal comments of the DOJ, and I request that it be included in the final report.

The DOJ is committed to protecting the privacy rights of individuals in the course of its counterterrorism and law enforcement mission. To spearhead this effort, the DOJ has recently appointed a Chief Privacy and Civil Liberties Officer (CPCLO) to oversee and administer the DOJ's privacy functions. The DOJ is also establishing a departmental Privacy and Civil Liberties Board to assist the CPCLO in ensuring that the DOJ's activities are carried out in a way that continues to fully protect the privacy and civil liberties of all Americans.

As the GAO report points out, the recent security breaches involving information resellers have highlighted the public's concerns regarding personal data maintained by such resellers and led to the GAO's review of the use of personal information from information resellers by the DOJ, as well as the DOJ's policies and practices for handling such information. The DOJ recognizes the unique issues presented by reseller information and agrees that additional measures could be taken regarding its use, in the form of revised or additional guidance and policy. At the same time, the DOJ also recognizes the need to consider agency resources, competing mission priorities, and the privacy protections that are already in place as a result of the DOJ's compliance with the Privacy Act of 1974, 5 U.S.C. §552a.

Ms. Linda Koontz

2

In recognition of the variety of government operations (such as law enforcement and intelligence), the Privacy Act incorporated some, but not all, of the Fair Information Practices.<sup>1</sup> Law enforcement may use the regulatory process to exempt certain records from some of the requirements of the Privacy Act. For example, pursuant to regulations, criminal law enforcement records may be exempted from the Privacy Act's requirement that an agency make reasonable efforts to assure that a record is accurate, complete, timely, and relevant for agency purposes, prior to disseminating that record to someone other than an agency or pursuant to FOIA. Instead of focusing on satisfying the Fair Information Practices, the more appropriate metric should be whether an agency has met the requirements of the Privacy Act.

Thus, the DOJ recommends that prior to the issuance of any new guidance or policy, a careful analysis and assessment of the degree of need for any new guidance should be conducted. That assessment should be used to ensure that the guidance is tailored in such a way as to avoid any negative impact on the DOJ's resources and competing mission priorities. Further, any new guidance or policy should be crafted in such a way as to avoid any increase in litigation risk, and to fully recognize and take into account the balance that Congress has already struck in the Privacy Act in applying Fair Information Practices to law enforcement data.

The DOJ stands willing to assist in the development of any new guidance or policy considered as a result of this effort. We look forward to working with OMB and other agencies toward a solution that strikes the proper balance between the furtherance of the DOJ's mission and the protection of individuals' privacy.

Again, we appreciate the opportunity to comment on this report. If you have any questions regarding our comments, please contact Richard Theis, Assistant Director, Audit Liaison Group, Management and Planning Staff. If you would like to discuss or receive a briefing, please contact me at (202) 514-3101.

Sincerely,



Paul R. Corts  
Assistant Attorney General  
for Administration

---

<sup>1</sup>First proposed in 1973 by a U.S. governmental advisory committee and widely accepted as including: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability.

# Comments from the Department of Homeland Security

U.S. Department of Homeland Security  
Washington, DC 20528



**Homeland  
Security**

March 17, 2006

Ms. Linda Koontz  
Director, Information Management  
Government Accountability Office  
Washington, DC 20548

Dear Ms. Koontz:

Re: Draft Report GAO-06-421, Privacy: Opportunities Exist for Agencies and Information Resellers to More Fully Adhere to Key Principles.

Thank you for the opportunity to review the draft report. The Department of Homeland Security (DHS) and the Privacy Office commend the GAO for undertaking this important and informative review. Certainly guidance on the collection and use of commercial data is important for federal agencies, such as DHS. Early on in the establishment of the DHS Privacy Office, the Department determined that one of the top three issues that needed to be addressed was the use of private sector information for homeland security purposes. It is an increasingly important issue, as the report notes.

To that end, the Privacy Office at DHS began its review of commercial data use and appropriate privacy safeguards through internal DHS study and by doing outreach publicly and in cooperation with DHS offices and other federal and private sector partners. The Privacy Office hosted a two-day public workshop, September 8-9, 2005, on Privacy and Technology: Government Use of Commercial Data for Homeland Security. The agenda and full transcripts of the conference, including a review of the application of the Privacy Act and Fair Information Practice Principles, is posted at our website at [www.dhs.gov/privacy](http://www.dhs.gov/privacy) and is available to the public and government agencies for review. Mention of this in the final GAO report could assist the dialogue and enable decision makers to review information and suggestions raised for appropriate use of commercial data and challenges experienced by federal agencies.

The Department appreciates the thoughtful work of GAO in addressing current use and practices at DHS. We would like to report that in early March 2006, and since the last contact with GAO, updated Privacy Impact Assessment Guidance, which includes directions relevant to the collection and use of commercial data, has been published by the Privacy Office and distributed throughout the Department. It also is posted on both the Department's internal and external websites. Please see *Privacy Impact Assessments, Official Guidance 2006, Privacy Office, U.S. Department of Homeland Security*. We respectfully suggest the GAO report could be updated to reflect this. Prior to this, the

[www.dhs.gov](http://www.dhs.gov)

---

**Appendix IV**  
**Comments from the Department of Homeland**  
**Security**

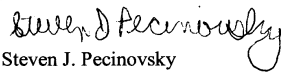
---

Department did have guidance on Privacy Impact Assessments that had been distributed in draft form in July 2005, both internally in DHS and externally with all of our federal partners. The Department of Justice advised DHS of their intention to adopt the DHS published guidance of March 2006.

The Department believes that our guidance, which includes questions that address the use of commercial data, is unique in the government in this regard. As a result, we believe the DHS Privacy Office should be given recognition in the GAO report for its efforts to encourage transparency regarding the use of commercial data. The Department continues to work diligently on finalizing a policy for DHS use of commercial data and expects to have that policy in circulation shortly. The Department will continue to address the need for transparency about the use of commercial data as part of the overall effort to reorganize and review legacy Privacy Act systems.

We thank you again for the opportunity to review this most important report and provide comments.

Sincerely,



Steven J. Pecinovsky  
Director  
Departmental GAO/OIG Liaison Office

# Comments from the Social Security Administration



**SOCIAL SECURITY**

The Commissioner

March 17, 2006

Ms. Linda Koontz  
Director, Information Management Issues  
U.S. Government Accountability Office  
Room 4-T-21  
441 G Street, NW  
Washington, D.C. 20548

Dear Ms. Koontz:

Thank you for the opportunity to review the draft report, "Privacy: Opportunities Exist For Agencies and Information Resellers to More Fully Adhere to Key Principles" (GAO-06-421). Our comments are enclosed.

If you have any questions, please have your staff contact Candace Skurnik, Director, Audit Management and Liaison Staff, at (410) 965-0374.

Sincerely,

A handwritten signature in black ink that reads "Anne B. Barnhart".  
Anne B. Barnhart

Enclosure

SOCIAL SECURITY ADMINISTRATION BALTIMORE MD 21235-0001



COMMENTS OF THE SOCIAL SECURITY ADMINISTRATION (SSA) ON THE  
GOVERNMENT ACCOUNTABILITY OFFICE'S (GAO) DRAFT REPORT,  
"PRIVACY: OPPORTUNITIES EXIST FOR AGENCIES AND INFORMATION  
RESELLERS TO MORE FULLY ADHERE TO KEY PRINCIPLES" (GAO-06-421)

General Comments

Thank you for the opportunity to review and provide comments on this GAO draft report. We share GAO's concerns about the potential for security breaches involving information resellers and support GAO's suggestion for congressional consideration and recommendations for Executive Branch action in support of ensuring adherence to applicable laws and the Fair Information Practices relating to privacy protection.

SSA is committed to protecting privacy with regard to information the Agency maintains, including information obtained from information resellers. We have established internal controls, including audit trails of any systems usage, to ensure that any information disclosed is for proper use. In order to identify any internal control weaknesses and potential problems that could result in waste, fraud and abuse, and to ensure compliance with the Federal Managers Financial Integrity Act of 1982, SSA components regularly perform Management Control Systems Reviews mandated by SSA and the Office of Management and Budget.

GAO Recommendation

We recommend that the Attorney General, the Secretary of Homeland Security, the Secretary of State, and the Commissioner of SSA develop specific policies for the collection, maintenance, and use of personal information obtained from resellers that reflect the Fair Information Practices, including oversight mechanisms such as the maintenance and review of audit logs detailing queries of information reseller databases, to improve accountability for agency use of such information.

SSA Comment

We agree. To better address the Fair Information Practices concerning information SSA obtains from information resellers, we will amend our relevant Privacy Act systems of records notices to reflect the use of information resellers/commercial data sources.

We will also explore options for enhancing our policies and internal controls over information SSA obtains from information resellers, including options for improved audit trail maintenance and review.

# Comments from the Department of State



United States Department of State

*Assistant Secretary and Chief Financial Officer*

*Washington, D.C. 20520*

MAR 20 2006

Ms. Jacquelyn Williams-Bridgers  
Managing Director  
International Affairs and Trade  
Government Accountability Office  
441 G Street, N.W.  
Washington, D.C. 20548-0001

Dear Ms. Williams-Bridgers:

We appreciate the opportunity to review your draft report, "PRIVACY: Opportunities Exist For Agencies and Information Resellers to More Fully Adhere to Key Principles," GAO Job Code 310732.

The enclosed Department of State comments are provided for incorporation with this letter as an appendix to the final report.

If you have any questions concerning this response, please contact Brian Egan, Legal Adviser, Bureau of Legal Affairs, at (202) 647-2227.

Sincerely,

A handwritten signature in black ink, appearing to read "Bradford R. Higgins".

Bradford R. Higgins

cc: GAO – Jamie Pressman  
CA & DS  
State/OIG – Mark Duda

Department of State Comments on GAO Draft Report  
**PRIVACY: Opportunities Exist For Agencies and Information  
Resellers to More Fully Adhere to Key Principles**  
(GAO-06-421 GAO Code 310732)

Thank you for giving us the opportunity to comment on GAO's draft report "Privacy: Opportunities Exist For Agencies and Information Resellers to More Fully Adhere to Key Principles."

In general, GAO's report seems to rest on the premise that records from "information resellers" should be accorded special treatment when compared with sensitive information from other sources. We do not believe that this premise is inherently sound. The Department receives sensitive information from a variety of sources in order to ensure that visas and passports are issued only to those who are entitled to them, to conduct investigations as part of its diplomatic security mission, and in other contexts. The Department does not distinguish between types of information or sources of information in deciding whether to comply with privacy laws. All Department information is treated in accordance with applicable privacy laws, regardless of the source or type of information at issue.

We also have a few specific technical comments. We request that GAO revise those sections of the report (e.g., at 58 and 62) which suggest that "fraud protection" in the passport and visa context is "not related to law enforcement." The Department is charged with investigating, making arrests, and working with other appropriate law enforcement agencies to detect and prosecute potential cases of visa and passport fraud. In the passport context, GAO recently stated that "[m]aintaining the integrity of the U.S. passport is essential to the State Department's effort to protect U.S. citizens from terrorists, criminals, and others," and that "Passport fraud is often intended to facilitate such crimes as illegal immigration, drug trafficking, and alien smuggling." See GAO, Improvements Needed to Strengthen U.S. Passport Fraud Detection Efforts (June 29, 2005) at 2. Fraud detection in the passport and visa context is clearly related to law enforcement, as well as to the vital task of providing homeland security.

On a related note, we disagree with GAO's criticism (at 62-63) of the use of terms such as "public source material" to identify categories of

---

sources of records in Privacy Act systems of records notices. To the extent that an agency's system of record notices properly identify "categories" of records, the notices are in compliance with the Privacy Act. See 5 U.S.C. § 552a(e)(4)(I). In our view, it would be bad policy to require separate and specific mention of information from individual sources such as data resellers, as this would imply that such information could not be considered when it was **not** specifically mentioned. Such a policy could result in critical information not being considered in a given case (in the case of the Department, for example, in adjudicating a visa or passport application), with consequent harmful effects on the United States national interest. The proliferation of such requirements for "specific mention" in systems of records notices would likely compound this problem, with the result that USG judgments would be less, not more, well-founded.

---

## 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](http://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](http://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](http://www.gao.gov/fraudnet/fraudnet.htm)

E-mail: [fraudnet@gao.gov](mailto:fraudnet@gao.gov)

Automated answering system: (800) 424-5454 or (202) 512-7470

---

## Congressional Relations

Gloria Jarmon, Managing Director, [JarmonG@gao.gov](mailto: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](mailto:AndersonP1@gao.gov) (202) 512-4800  
U.S. Government Accountability Office, 441 G Street NW, Room 7149  
Washington, D.C. 20548