AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

PERSONAL INFORMATION ACQUIRED BY THE GOVERNMENT FROM INFORMATION RESELLERS: IS THERE NEED FOR IMPROVEMENT?

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON
COMMERCIAL AND ADMINISTRATIVE LAW

AND THE

SUBCOMMITTEE ON THE CONSTITUTION

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

APRIL 4, 2006

Serial No. 109–98

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://judiciary.house.gov

U.S. GOVERNMENT PRINTING OFFICE

26–912 PDF WASHINGTON : 2006

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

F. JAMES SENSENBRENNER, JR., Wisconsin, *Chairman*

HENRY J. HYDE, Illinois
HOWARD COBLE, North Carolina
LAMAR SMITH, Texas
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
STEVE CHABOT, Ohio
DANIEL E. LUNGREN, California
WILLIAM L. JENKINS, Tennessee
CHRIS CANNON, Utah
SPENCER BACHUS, Alabama
BOB INGLIS, South Carolina
JOHN N. HOSTETTLER, Indiana
MARK GREEN, Wisconsin
RIC KELLER, Florida
DARRELL ISSA, California
JEFF FLAKE, Arizona
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TOM FEENEY, Florida
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas

JOHN CONYERS, JR., Michigan
HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
MARTIN T. MEEHAN, Massachusetts
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
ANTHONY D. WEINER, New York
ADAM B. SCHIFF, California
LINDA T. SÁNCHEZ, California
CHRIS VAN HOLLEN, Maryland
DEBBIE WASSERMAN SCHULTZ, Florida

PHILIP G. KIKO, *Chief of Staff-General Counsel*
PERRY H. APELBAUM, *Minority Chief Counsel*

SUBCOMMITTEE ON COMMERCIAL AND ADMINISTRATIVE LAW

CHRIS CANNON, Utah *Chairman*

HOWARD COBLE, North Carolina
TRENT FRANKS, Arizona
STEVE CHABOT, Ohio
MARK GREEN, Wisconsin
RANDY J. FORBES, Virginia
LOUIE GOHMERT, Texas

MELVIN L. WATT, North Carolina
WILLIAM D. DELAHUNT, Massachusetts
CHRIS VAN HOLLEN, Maryland
JERROLD NADLER, New York
DEBBIE WASSERMAN SCHULTZ, Florida

RAYMOND V. SMIETANKA, *Chief Counsel*
SUSAN A. JENSEN, *Counsel*
BRENDA HANKINS, *Counsel*
MIKE LENN, *Full Committee Counsel*
STEPHANIE MOORE, *Minority Counsel*

SUBCOMMITTEE ON THE CONSTITUTION

STEVE CHABOT, Ohio, *Chairman*

TRENT FRANKS, Arizona
WILLIAM L. JENKINS, Tennessee
SPENCER BACHUS, Alabama
JOHN N. HOSTETTLER, Indiana
MARK GREEN, Wisconsin
STEVE KING, Iowa
TOM FEENEY, Florida

JERROLD NADLER, New York
JOHN CONYERS, JR., Michigan
ROBERT C. SCOTT, Virginia
MELVIN L. WATT, North Carolina
CHRIS VAN HOLLEN, Maryland

PAUL B. TAYLOR, *Chief Counsel*
E. STEWART JEFFRIES, *Counsel*
HILARY FUNK, *Counsel*
KIMBERLY BETZ, FULL COMMITTEE COUNSEL
DAVID LACHMANN, *Minority Professional Staff Member*

CONTENTS

APRIL 4, 2006

OPENING STATEMENT

	Page
The Honorable Chris Cannon, a Representative in Congress from the State of Utah, and Chairman, Subcommittee on Commercial and Administrative Law	1
The Honorable Melvin L. Watt, a Representative in Congress from the State of North Carolina, and Ranking Member, Subcommittee on Commercial and Administrative Law	2
The Honorable Steve Chabot, a Representative in Congress from the State of Ohio, and Chairman, Subcommittee on the Constitution	3
The Honorable Jerrold Nadler, a Representative in Congress from the State of New York, and Ranking Member, Subcommittee on the Constitution	4

WITNESSES

Ms. Linda D. Koontz, Director, Information Management Issues, U.S. Government Accountability Office	
Oral Testimony	7
Prepared Statement	10
Ms. Maureen Cooney, Acting Chief Privacy Officer, U.S. Department of Homeland Security	
Oral Testimony	44
Prepared Statement	45
Mr. Peter Swire, William O'Neill Professor of Law, Moritz College of Law of the Ohio State University, Visiting Senior Fellow, Center for American Progress	
Oral Testimony	48
Prepared Statement	51
Mr. Stuart K. Pratt, President and Chief Executive Officer, Consumer Data Industry Association	
Oral Testimony	61
Prepared Statement	63

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Additional Material for the Record submitted by Linda D. Koontz, Director, Information Management Issues, U.S. Government Accountability Office	86

PERSONAL INFORMATION ACQUIRED BY THE GOVERNMENT FROM INFORMATION RESELLERS: IS THERE NEED FOR IMPROVEMENT?

TUESDAY, APRIL 4, 2006

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COMMERCIAL
AND ADMINISTRATIVE LAW,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittees met, pursuant to call, at 12:03 p.m., in Room 2138 Rayburn House Office Building, the Honorable Chris Cannon (Chairman of the Subcommittee on Commercial and Administrative Law) presiding.

Mr. CANNON. I think we will get started here. The hearing will be called to order.

As many of you know, the protection of personal information in the hands of the Federal Government has long been a top priority for my Subcommittee, the Subcommittee on Commercial and Administrative Law, and Chairman Chabot's Subcommittee, the Constitution Subcommittee. Both of our Subcommittees have played a major role in respect to protecting personal privacy and civil liberties under the leadership and guidance of Jim Sensenbrenner, Chairman of the Judiciary Committee.

In this post-September 11th world, however, it is no easy task to balance the competing goals of keeping our Nation secure while at the same time protecting the privacy of our Nation's citizens. Nevertheless, I believe that our respective Subcommittees and the Judiciary Committee are uniquely and best suited to study and resolve these issues.

Our accomplishments to date include the establishment of the first statutorily-created Privacy Office in a Federal agency, namely the Department of Homeland Security. That office has since earned plaudits from both the public and private sectors. Based on the successes of that office, we also spearheaded the creation of a similar function in the Justice Department, which was signed into law in January of this year.

In addition, both my Subcommittee and the Constitution Subcommittee have considered the support of legislation requiring a Federal agency to prepare a privacy impact analysis for proposed and final rules and to include this analysis in the Notice for Public Comment issued in conjunction with the publication of such rules.

Today's hearing focuses on the respective roles that the Federal Government and information resellers have with respect to personal information collected in commercial databases. As the hearing title denotes, we approach this subject with an open mind and willingness to understand the factors and nuances concerning how Federal agencies and those in the private sector safeguard personal information that they obtain from us.

As technological developments increasingly facilitate the collection, use, and dissemination of personally identifiable information, the potential for misuse of such information escalates. Five years ago, the GAO warned: "our Nation has an increasing ability to accumulate, store, retrieve, cross-reference, analyze, and link vast numbers of electronic records in an ever-faster and more cost-efficient manner. These advances bring substantial Federal information benefits as well as increasing responsibilities and concerns." Given the largely unfettered use of Social Security numbers and the availability of other personally identifiable information, identity theft has swiftly evolved into one of the most prolific crimes in the United States. According to the Federal Trade Commission, identity theft topped the list of consumer complaints filed with the Agency in 2005. The FTC estimates that 10 million consumers were victims of some form of identity theft in 2003.

As a result of this crime, American businesses suffered an estimated $48 billion in losses, while consumers incurred an additional $5 billion in out-of-pocket losses. Just this week, the Justice Department announced that nearly 4 million households, about 3 percent of all households in the Nation, learned that they had been identity theft victims. Just last week, I got a credit card in the mail with a little note saying that my account had been viewed as one that might be subject to identity theft, and so I have a new card with a new number. I hadn't memorized the old one, so it was not much of an inconvenience. But it is a broad problem.

Unfortunately, we continue to receive reports from GAO finding shortcomings in how Federal agencies safeguard personal information, and the private sector's vulnerability was highlighted by the many high-profile databases that have occurred in recent years. Questions have also been posed about the accuracy of some of the data maintained in these commercial databases. It is against this complex but exceedingly interesting backdrop that we are holding this hearing today.

I would now like to turn to my colleague Mr. Watt, the distinguished Ranking Member of my Subcommittee, and ask him if he has any opening remarks.

Mr. WATT. Thank you, Mr. Chairman. I will be brief.

Let me commend Chairman Sensenbrenner and Ranking Member Conyers and Mr. Chabot and Mr. Nadler for taking steps to get the GAO to conduct this investigation and produce this report. It is clear that privacy issues that confront our country as a result of extraordinary technological advances are significant and that the ramifications of how we treat the privacy of personally identifiable information is heightened in the post-9/11 world. I say this as a member of both the Financial Services and Judiciary Committees, and have heard testimony from numerous witnesses on the enhanced concerns about the Government's acquisition, maintenance,

and dissemination of personal information and the opportunity for identity theft created by the massive data mining of this information.

One of the main recommendations of the 9/11 Commission was the establishment of a Governmentwide watchdog to safeguard civil liberties. The Commission found that currently, "there is no office within the Government whose job it is to look across the Government at the actions we are taking to protect ourselves and to ensure that liberty concerns are appropriately considered."

We have tried to get that recommendation passed, without any success up to this point, and I think the need for that kind of oversight body is continuing to grow and we need to do that.

I am looking forward to the testimony of the witnesses. And with that, Mr. Chairman, I will yield back the balance of my time.

Mr. CANNON. The gentleman yields back. Thank you.

Now I would like to turn to my colleague Mr. Chabot, the distinguished chair of the Constitution Subcommittee, and ask him if he has any opening remarks.

Mr. CHABOT. Yes, I do. Thank you, Mr. Chairman.

Mr. CANNON. The gentleman is recognized for 5 minutes.

Mr. CHABOT. First I would like to thank you for holding this hearing and thank all our witnesses for assisting us in our examination of issues related to the security and privacy of our personal information.

Security breaches reported in the media last year involving the unauthorized access to and theft of personal information highlighted an emerging area of concern to all of us, that being the treatment of our personal information as just another commodity. Our concerns are well-founded, as recent statistics released by the Department of Justice reveal that identity theft affected 3.6 million households across the Nation and cost our economy $3.2 billion during the first half of 2004 alone.

The security breaches also raise questions with regard to the Federal Government's reliance on and contributions to the use of personal information. Questions raised include: Are Federal agencies collecting information on us? What information is being collected? Where is the information going and where will it eventually end up? What Federal laws guide collection activities? And most importantly, how, as individuals affected by these collection activities, can we best monitor and ensure that such information is being used as was intended?

Last spring, I, along with the Chairman and Ranking Member of the full Committee, Mr. Conyers, charged GAO with finding answers to these questions. In particular, we sought to gain a better understanding of the Federal Government's involvement and reliance on data as it relates to fulfilling our Federal Government's top priorities, such as our Nation's law enforcement and antiterrorism efforts, and performing other critical domestic functions such as effectively distributing benefits.

Our inquiry was also prompted by the information age in which we live, where technology has allowed personal information to be universally available to anyone at any time, including to the Federal Government. The information provided by the commercial data suppliers has served an important role in supporting our Nation's

law enforcement and antiterrorism efforts. It has also played an important role in assisting the Federal Government to perform other administrative responsibilities. For example, last fall, commercial data companies provided critical assistance to FEMA to assist the victims of Hurricane Katrina.

However, with the widespread availability of information comes increased risks of privacy and security breaches, unauthorized uses, and other negative effects, to which the Federal Government is not immune.

I hope through today's hearing we can gain a better understanding of the existing Federal laws and policies in place guiding commercial data suppliers and the Federal Government in handling personal information. Moreover, I look forward to discussing whether Federal laws such as the Privacy Act of 1974 and E-Government Act of 2002, which guide the Federal Government, and the Fair Credit Reporting Act and the Gramm-Leach-Bliley Act, which guide the commercial data industry, have been affected in addressing concerns raised by the emerging industry.

With a better understanding of the existing framework, we can ensure that the Federal Government continues to have access to the types of information that will enable it to fulfill its responsibilities. At the same time, we can ensure that citizens know when and how their information is being collected and used by the Federal Government.

I look forward to discussing these issues and learning whether new legislation, such as the Federal Agency Privacy Protection Act which I have introduced in the previous Congresses, would be an appropriate remedy to ensure citizens' privacy concerns over the use of their personal information by the Federal Government. The Federal Agency Privacy Protection Act would require that all Federal agencies conduct privacy impact assessments when issuing a notice regarding a new or interpretive rule relating to the collection of personally identifiable information on citizens, as well as when final rules are promulgated.

Again, I welcome the witnesses here with us today and look forward to their testimony.

I yield back the balance of my time.

Mr. CANNON. Thank you, Mr. Chabot.

Mr. Nadler, do you have an opening statement?

Mr. NADLER. Yes. Thank you, Mr. Chairman. I will be brief because I want to get to our witnesses.

Modern technology and security concerns have greatly threatened the privacy of the most personal information about every American. The nexus between private information resellers and Government action are especially troubling.

How we handle these complicated issues—and they are complicated—will affect the lives of every one of our constituents. It is not simply a matter of identity theft but of the basic right to be secure in our persons, our papers, and our homes. People need to know that when they visit a doctor, go to the store, read a book, engage in the practice of their religion, they will not be subject to unwanted and uninvited prying eyes.

The secret NSA wiretaps, some of the abuses of power by the Justice Department, some of the more extravagant claims by this

Administration are warning signs. I hope this Congress looks more carefully at the question of privacy from both a technical and legal perspective. This study and this hearing are important steps in this direction.

Of course, in one sense, this study, this hearing, everything we are doing, in one sense is irrelevant, because the Administration claimed in the NSA wiretap situation that the President has inherent power to disobey the FISA law because of inherent power under article II and under the authorization for the use of military force. And in fact, it claims inherent power to go beyond that, and we have no way of knowing what the NSA or some other agency may in fact be doing that might invade privacy. The Administration won't tell us. They won't testify to us. It is all secret. And in fact, the Administration is conducting an investigation into who revealed what we do know about the NSA wiretaps, because they think that ought to have remained secret. I disagree, obviously, but that is their position.

And they have made it quite clear that, in fact, various Government agencies may be going far beyond what we know in wiretapping or otherwise invading the privacy of American citizens regardless of what the law says and regardless of any law we may pass, because the President has inherent power to disregard that during a war, and we are in a war on terrorism.

So everything we say, everything we investigate, everything we hear, everything we do may in fact be irrelevant because the President claims the power to ignore it and may or may not be exercising that power in ways that are unknown to us. That is a far greater threat to our liberty than probably anything else we are talking about.

So I thank you, Mr. Chairman, for scheduling this hearing. But I hope we realize that the ability of this Congress to deal with this is very much circumscribed by the unprecedented and tyrannical claim of power that the Administration is making.

I thank you. I yield back.

Mr. CANNON. Far be it from me to disagree with the gentleman, but I think it is the role of Congress to oversee any president of either party.

Mr. NADLER. Well, I certainly agree with that.

Mr. CANNON. That is not the focus of this hearing, but we certainly need to be doing that.

Mr. NADLER. Mr. Chairman, if I could just say.

Mr. CANNON. Certainly.

Mr. NADLER. You are not disagreeing with me. I certainly agree that we ought to be overseeing the Administration. My point is that the Administration claims under the wartime power that we have no power to do that.

Mr. CANNON. I understand that you are being very harsh about the Administration. I think our objective is to transcend the current status of affairs with the war on terror.

Without objection, the gentleman's entire statement will be placed in the record. Hearing no objection, so ordered.

Without objection, all Members may place their statements in the record at this point. Hearing no objection, so ordered.

Without objection, the Chair will be authorized to declare recesses of this hearing at any point. Hearing no objection, so ordered.

I ask unanimous consent that Members have 5 legislative days to submit written statements for inclusion in today's hearing record. Hearing no objection, so ordered.

I am now pleased to introduce the witnesses for today's hearing. Our first witness is Linda Koontz, who is the Director of GAO's Information and Management Issues Division. In that capacity, she is responsible for issues regarding the collection, use, and dissemination of Government information. Mrs. Koontz has led GAO's investigations into the Government's data mining activities as well as E-Government initiatives. In addition to obtaining her bachelor's degree from Michigan State University, Ms. Koontz received certification as a Government financial manager. She is also a member of the Association for Information and Image Management Standards Board.

Maureen Cooney, our next witness, is the Acting Chief Privacy Officer for the Department of Homeland Security. Ms. Cooney, we always appreciated working with your predecessor, Nuala O'Connor Kelly, and we look forward to working with you as well. As I previously noted in my opening remarks, my Subcommittee, with the support of Chairman Jim Sensenbrenner, played a major role in establishing Ms. Cooney's office at the Department of Homeland Security. The legislation creating her office not only mandated the appointment of a privacy officer, but specified the officer's responsibilities. One of the principal responsibilities of the DHS Privacy Officer, as set out by statute, is the duty to assure that the use of technologies sustain and do not erode privacy protections relating to the use, collection, and disclosure of personal information. In addition, the Privacy Officer must assure that personal information is handled in full compliance with the Privacy Act and assess privacy impact of the Department's proposed rules.

Before joining the DHS Privacy Office, Ms. Cooney worked on international privacy and security issues at the U.S. Federal Trade Commission, where she served as the principal liaison for the FTC to the European Commission and article 29 Working Party on Privacy Issues. She also played a major role on the rewrite of the Organization for Economic Cooperation and Development Security Guidelines for Information Systems and Networks. Prior to that assignment, Ms. Cooney worked on privacy and security issues with the Treasury Department in the Office of the Comptroller of the Currency. We are really pleased that there are people that know as much about this as you do, who are here to help guide us.

Ms. Cooney received her bachelor's degree in American studies from Georgetown University and her law degree from Georgetown University Law Center.

Our third witness is Peter Swire, the C. William O'Neill Professor in Law and Judicial Administration at the Moritz College of Law of Ohio State University. In addition to his academic endeavors, Professor Swire is a consultant with the law firm Morrison & Foerster, where he provides advice on privacy, cyberspace, and related matters. He is also currently a visiting senior fellow at the Center for American Progress, a nonpartisan research and edu-

cational institute. Under the Clinton administration, Professor Swire was OMB's Chief Counselor for Privacy.

Professor Swire received his undergraduate degree from Princeton University and his law degree from Yale Law School. He is a prolific writer, with numerous law review articles and other writings to his credit.

Our final witness is Stuart Pratt. Mr. Pratt is the president and CEO of the Consumer Data Industry Association, an international trade association representing more than 250 consumer information companies. Prior to his current position, Mr. Pratt served as the association's vice president of government relations. He is a well-known expert on the Fair Credit Reporting Act, identity fraud, and the issues of consumer data and public record data issues. Mr. Pratt received his undergraduate degree from Furman University in Greenville, South Carolina.

I extend to each of you my warm regards and appreciation for your willingness to participate in today's hearing. In light of the fact that your written statements will be included in the hearing record, I request that you limit your oral remarks to 5 minutes. Accordingly, please feel free to summarize or highlight the salient points of your testimony.

You will note that we have a lighting system, which is not yet on but they are the two little gizmos in front of you. It starts with a green light and you have 4 minutes before it turns yellow, and then at the 5-minute mark it turns red. It is my habit to tap the gavel at 5 minutes. We will appreciate it if you would finish up your thoughts within that time frame. We don't want to cut people off in the middle of your thinking, but I find it works better if everybody realizes we have a 5-minute limit. I am probably going to be a little more aggressive with questions so that we can give everybody an opportunity to ask questions.

After you have presented your remarks, the Subcommittee Members, in the order they arrived, will be permitted to ask questions of the witness. They will also be limited to 5 minutes.

Pursuant to the direction of the Chairman of the Judiciary Committee, I ask the witnesses to please stand and raise your right hand to take the oath.

[Witnesses sworn.]

Mr. CANNON. Thank you. You may be seated.

The record should reflect that each of the witnesses answered in the affirmative.

Ms. Koontz, would you please proceed with your testimony.

TESTIMONY OF LINDA D. KOONTZ, DIRECTOR, INFORMATION MANAGEMENT ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Ms. KOONTZ. Mr. Chairman and Members of the Subcommittees, I appreciate the opportunity to discuss the results of GAO's work on the Federal Government's purchase of personal information from businesses known as information resellers. My testimony summarizes the results of the report we did at the Committee's request and that we are issuing today. For that report we reviewed four agencies: Justice, Homeland Security, State, and Social Security.

Information is an extremely valuable resource and information resellers provide services that are important to a variety of Federal agency functions. Specifically, for fiscal year 2005, the four agencies we reviewed reported a combined total of approximately $30 million in obligations for the purchase of personal information from resellers.

The vast majority of this spending, about 91 percent, was for law enforcement or counterterrorism. For example, the Department of Justice, the largest user among the four, used the information for criminal investigations, locating witnesses and fugitives, and researching assets held by individuals of interest. Reseller information was also used by others to detect and investigate fraud, verify identities, and determine eligibility for benefits.

As agreed, we also evaluated agency and reseller privacy policies and practices against the Fair Information Practices, a set of widely accepted principles for protecting the privacy and security of personal information. These principles, with variations, are the basis of privacy laws in many countries and are the foundation of the Privacy Act. They are not legally binding either on Federal agencies or resellers, but we believe they do provide a useful framework for analyzing agency and reseller practices and serve as an appropriate basis for further discussion and debate.

Applying this framework to Federal agencies, we found some inconsistencies. Agencies did take steps to address the privacy and security of the information acquired from resellers, but their handling of this information did not always fully reflect the Fair Information Practices. For example, although agencies issued privacy notices on information collections, these did not always specifically state that information resellers were among the sources used. This is not consistent with the principle that the public should be informed about privacy policies and have a ready means of learning about the use of personal information. One reason for this kind of inconsistency is ambiguity in OMB's guidance regarding how privacy requirements apply to Federal agency use of reseller information.

To address these inconsistencies, we made recommendations to OMB and to the agencies we reviewed. These agencies generally agreed with our report and reported actions they are taking. In particular, the Privacy Office within Homeland Security has conducted a public workshop on the Government's use of commercial data for homeland security and recently finalized guidance on conducting privacy impact assessments, which includes very useful direction on the collection and use of commercial data.

Regarding resellers, they also took steps to protect privacy, but these measures were not fully consistent with the Fair Information Practices. For example, resellers generally informed the public about key privacy practices and principles and they have recently taken steps to improve security safeguards. However, 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 reseller business, which is based on providing information to multiple customers for multiple purposes.

Further, resellers generally limit the extent to which individuals can gain access to personal information held about themselves, as

well as the extent to which they can correct or delete inaccurate information contained in reseller databases.

In response, information resellers raised concerns about our reliance on the Fair Information Practices and suggested it would be unreasonable for them to comply with some aspects of the principles that, they believe, were intended for organizations that collect information directly from consumers. Nonetheless, we believe that analysis against a framework of the Fair Information Practices is important as a starting point to frame potential issues and facilitate informed discussion, and we suggest that Congress consider these issues in its deliberations.

In conclusion, privacy is ultimately about striking a balance between competing interests. In this case, it is about balancing the value of reseller information as to important Government functions against the privacy rights of individuals. I look forward to participating in the discussion on how best to strike that balance.

This concludes my statement. Thank you.

[The prepared statement of Ms. Koontz follows:]

United States Government Accountability Office

GAO

Testimony

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

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

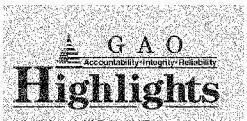
PERSONAL INFORMATION

Agencies and Resellers Vary in Providing Privacy Protections

Statement of Linda D. Koontz
Director, Information Management Issues

GAO-06-609T

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.



Highlights

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

Why GAO Did This Study

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

What GAO Recommends

In its report, GAO suggests that the Congress consider the extent to which resellers should adhere to the Fair Information Practices. In addition, GAO is making recommendations to the Office of Management and Budget and the four agencies to establish policy to address agency use of personal information from commercial sources.

Agency officials generally agreed with the content of the report. Resellers questioned the applicability of the Fair Information Practices, especially with regard to public records.

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

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

April 2006

PERSONAL INFORMATION

Agencies and Resellers Vary in Providing Privacy Protections

What GAO Found

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

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

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

Mr. Chairmen and Members of the Subcommittees:

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

Federal agency use of such information is governed primarily by the Privacy Act of 1974,[2] which requires that the use of personal information be limited to predefined purposes and involve only information germane to those purposes. The provisions of the Privacy Act, in turn, are largely based on a set of principles for protecting the privacy and security of personal information, known as the Fair Information Practices, which were first proposed in 1973 by a U.S. government advisory committee.[3] These principles, now widely accepted, include

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

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

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

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

These principles, with some variation, are used by organizations to address privacy considerations in their business practices and are also the basis of privacy laws and related policies in many countries, including the United States, Germany, Sweden, Australia, New Zealand, and the European Union.

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

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

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

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

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

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

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

Results in Brief

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

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

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

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

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

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

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

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

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

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

Background

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

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

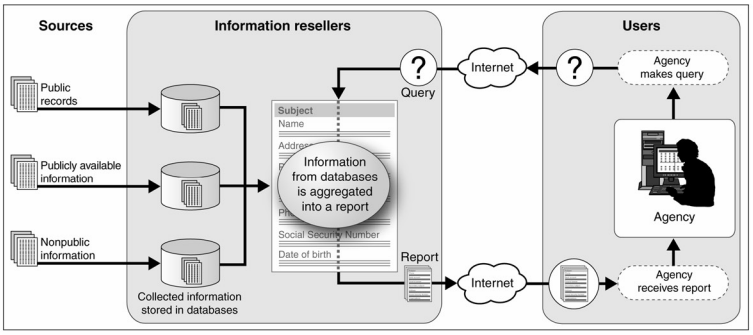
Information resellers have now amassed extensive amounts of personal information about large numbers of Americans. They supply it to customers in both government and the private sector, typically via a centralized online resource. Generally, three types of information are collected:

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

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

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

Figure 1: Typical Information Flow through Resellers to Government Customers



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Table 1: The OECD Fair Information Practices

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

Source: OECD.

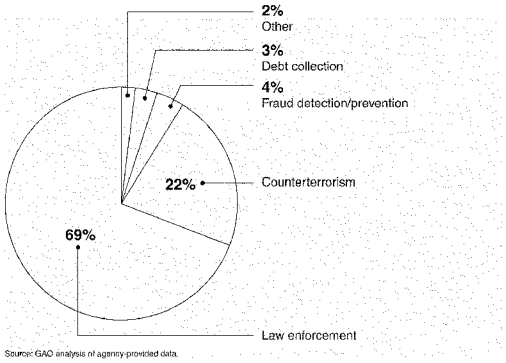
The Fair Information Practices are not precise legal requirements. Rather, they provide a framework of principles for balancing the need for privacy with other public policy interests, such as national security, law enforcement, and administrative efficiency. Ways to strike that balance vary among countries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

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

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

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

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



Source: GAO analysis of agency-provided data.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Principle	Agency application of principle	Agency practices
Collection limitation. The collection of personal information should be limited, should be obtained by lawful and fair means, and, where appropriate, with the knowledge or consent of the individual.	General	Agencies limited personal data collection to individuals under investigation or their associates.
Data quality. Personal information should be relevant to the purpose for which it is collected, and should be accurate, complete, and current as needed for that purpose.	General	Agencies corroborated information from resellers and did not take actions based exclusively on such information.
Purpose specification. The purpose for the collection of personal information should be disclosed before collection and upon any change to that purpose, and its use should be limited to that purpose and compatible purposes.	Uneven	Agency system of records notices did not generally reveal that agency systems could incorporate information from data resellers. Agencies also generally did not conduct privacy impact assessments for their systems or programs that involve use of reseller data.
Use limitation. Personal information should not be disclosed or otherwise used for other than a specified purpose without consent of the individual or legal authority.	General	Agencies generally limited their use of personal information to specific investigations (including law enforcement, counterterrorism, fraud detection, and debt collection).
Security safeguards. Personal information should be protected with reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification, or disclosure.	General	Agencies had security safeguards such as requiring passwords to access databases, basing access rights on need to know, and logging search activities (including "cloaked logging," which prevents the vendor from monitoring search content).
Openness. The public should be informed about privacy policies and practices, and individuals should have ready means of learning about the use of personal information.	Uneven	See *Purpose specification* above. Agencies did not have established policies specifically addressing the use of personal information obtained from resellers.
Individual participation. Individuals should have the following rights: to know about the collection of personal information, to access that information, to request correction, and to challenge the denial of those rights.	Uneven	See *Purpose specification* above. Because agencies generally did not disclose their collections of personal information from resellers, individuals were often unable to exercise these rights.
Accountability. Individuals controlling the collection or use of personal information should be accountable for taking steps to ensure the implementation of these principles.	Uneven	Agencies do not generally monitor usage of personal information from information resellers to hold users accountable for appropriate use; instead, they rely on users to be responsible for their behavior. For example, agencies may instruct users in their responsibilities to use personal information appropriately, have them sign statements of responsibility, and have them indicate what permissible purpose a given search fulfills.

Legend:

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

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

Source: GAO analysis of agency-supplied data.

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

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

[22] Although we did not assess the effectiveness of information security at any agency as part of this review, we have previously reported on weaknesses in almost all areas of information security controls at 24 major agencies, including Justice, DHS, State, and SSA. For additional information see GAO, *Information Security: Weaknesses Persist at Federal Agencies Despite Progress Made in Implementing Related Statutory Requirements*, GAO-05-552 (Washington, D.C.: July 15, 2005) and *Information Security: Department of Homeland Security Needs to Fully Implement Its Security Program*, GAO-05-700 (Washington, D.C.: June 17, 2005).

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

The *purpose specification, openness*, and *individual participation* principles stipulate that individuals should be made aware of the purpose and intended uses of the personal information being collected about them, and, if necessary, have the ability to access and correct their information. These principles are reflected in the Privacy Act requirement for agencies to publish in the *Federal Register*, "upon establishment or revision, a notice of the existence and character of a system of records." This notice is to include, among other things, the categories of records in the system as well as the categories of sources of records.[23]

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

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

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

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

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

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

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

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

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

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

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

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

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

[27] The Privacy Act allows agencies to claim exemptions if the records are used for certain purposes. 5 U.S.C. § 552a (j) and (k). For example, records compiled for criminal law enforcement purposes can be exempt from the access and correction provisions. In general, the exemptions for law enforcement purposes are intended to prevent the disclosure of information collected as part of an ongoing investigation that could impair the investigation or allow those under investigation to change their behavior or take other actions to escape prosecution. In most cases where officials identified system-of-record notices associated with reseller data collection for law enforcement purposes, agencies claimed this exemption.

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

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

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

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

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

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

requiring PIAs to be conducted whenever reseller data are involved. However, although the DHS guidance clearly states that PIAs are required when personally identifiable information is obtained from a commercial source, it also states that "merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement."[81] Like OMB's guidance, the DHS guidance is not clear, because agency personnel are left to make individual determinations as to whether queries are "on an ad hoc basis."

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

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

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

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

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

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

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

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

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

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

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

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

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

Contacts and Acknowledgements

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

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Mail or Phone

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

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

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Congressional Relations

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

Public Affairs

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

PRINTED ON RECYCLED PAPER

Mr. CANNON. Thank you, Ms. Koontz.
Ms. Cooney?

TESTIMONY OF MAUREEN COONEY, ACTING CHIEF PRIVACY OFFICER, U.S. DEPARTMENT OF HOMELAND SECURITY

Ms. COONEY. Thank you. Chairmen Cannon and Chabot, Ranking Members Watt and Nadler, and Members of the Subcommittees on Commercial and Administrative Law and the Constitution, it is an honor to testify before you today. Because this marks my very first appearance before the Subcommittee, I would like to offer a few biographical background notes.

It is my honor to currently serve as the Acting Chief Privacy Officer for the Department of Homeland Security. I come to this position with 20 years of Federal service experience in risk management and compliance and enforcement activities as well as in consumer protection on global information privacy and security issues post-9/11. I was recruited from the Federal Trade Commission to join the Department of Homeland Security more than 2 years ago as Chief of Staff of the Privacy Office and Senior Adviser for International Privacy Policy.

Since that time, it has been my privilege to help build the DHS Privacy Office with my colleagues and under the leadership of former Chief Privacy Officer Nuala O'Connor Kelly and Secretaries Chertoff and Ridge.

I appreciate this opportunity to address the subject of personal information acquired by the Government from information resellers. The use of commercial data for homeland security involves complex issues that touch on privacy, program effectiveness, and operational efficiency. I commend the Government Accountability Office for undertaking their analysis, which will positively assist in informing privacy policy development.

As my written statement points out, internally the primary oversight mechanism used by the Privacy Office for ensuring appropriate use of personal information regardless of its source is the privacy impact assessment, which is required to be used by section 208 of the E-Government Act of 2002 and section 222 of the Homeland Security Act.

Privacy impact assessments, or PIAs as we call them, can be one of the most important instruments in establishing trust between the Department's operations and the public simply because they are generally very transparent. In fact, PIAs are fundamental at our Department in making privacy an operational element within the DHS family. Privacy impact assessments allow for the examination of privacy questions concerning a program or an information system's collection and use of information, including commercial reseller data.

As mentioned in my colleague Ms. Koontz's testimony, the DHS Privacy Office has issued official guidance on the conduct of privacy impact assessments. Various sections of that guidance are particularly relevant to the subject matter of this hearing. I refer you to my written testimony on the details of that.

I am a little concerned that we may run out of time, so one of the points that I would like to make is that in addition to privacy requirements under the Privacy Act of 1974, the privacy impact as-

sessment process really augments the system of record notice provisions in the Privacy Act that provide for notice to the public about the types of information collected by the Government and the treatment of that information. The DHS Privacy Office reviews new systems of record notices to make sure that the presence of commercial data is made transparent if data is collected as a source of information in a system, and we are seeking to apply this to existing sources as well.

The Privacy Office also has been part of a broad-based dialogue on the use of commercial data both within and outside of the Department. In September of 2005, we hosted a public workshop addressing privacy and technology, exploring the use of commercial data for homeland security. The workshop examined the policy, legal, and technology issues associated with the Government's use of commercial personally identifiable data for homeland security purposes.

With input from the public workshop, the DHS Privacy Office is now in the process of drafting specific guidance for our Department on the use of commercial data. The guidance will address three broad categories of use: comparing data in commercial and Government databases, obtaining data from commercial sources for use in Government systems, and use of Government analytic tools on commercial databases.

We will be hosting a meeting with our internal Privacy and Data Integrity Board made up of senior Department managers on April 11th to collaborate on this policy through a full and meaningful discussion of an appropriate framework for using commercial data.

The Privacy Office also has been discussing commercial data issues with the DHS Data Privacy and Integrity Advisory Committee, our Federal advisory committee made up of U.S. citizens with expertise in privacy information technology, information security, and public policy.

In October of 2005 the DHS Privacy Advisory Committee published a report on the use of commercial data to reduce false positives in screening programs, and the Committee's recommendations will be incorporated in our policy development.

Thank you for inviting me, and thank you for your support of the DHS Privacy Office.

[The prepared statement of Ms. Cooney follows:]

PREPARED STATEMENT OF MAUREEN COONEY

Chairmen Cannon and Chabot, Ranking Members Watt and Nadler, and Members of the Subcommittees on Commercial and Administrative Law and the Constitution, it is an honor to testify before you today on the activities of the United States Department of Homeland Security, for which I am privileged to served as the Acting Chief Privacy Officer.

Thank you for inviting me to speak with you on the subject of personal information acquired by the government from information resellers.

As you know, the DHS Chief Privacy Officer is the first statutorily required privacy officer in the Federal government. The responsibilities of the DHS Chief Privacy Officer are set forth in Section 222 of the Homeland Security Act of 2002. They include:

(a) assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection and disclosure of personal information;

(b)

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;

(c) evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government;

(d) conducting a privacy impact assessment of proposed rules of the Department on the privacy of personal information, including the type of personal information collected and the number of people affected; and

(e) preparing a report to Congress on an annual basis on activities of the Department that affect privacy, including complaints of privacy violations, implementation of the Privacy Act of 1974, internal controls and other matters.[1]

It is upon this statutory authority that the Chief Privacy Officer and the DHS Privacy Office review and approach the use of personal information by the Department, including the use of data from information resellers.

The use of data from information resellers for homeland security involves complex issues that touch on privacy, program effectiveness and operational efficiency. There are many benefits to the government when commercial data is used responsibly. It can save time, it is often more precise, and is updated more quickly and, therefore, in certain circumstances, it could be more accurate and therefore have greater data integrity than other sources. At the same time, the government's use of commercial data must be transparent and appropriate. The DHS Privacy Office has been part of a broad based dialogue both within and outside of the Department on the use of commercial data.

As noted by the Government Accountability Office (GAO), unless an information reseller is operating a System of Records specifically on behalf of a Federal agency, it is not subject to the provisions of the Privacy Act of 1974. However, the Privacy Act applies to Federal agencies that bring data from information resellers into a Federal System of Records. The Privacy Office exercises oversight over the way Departmental components access, use and maintain data obtained from information resellers as part of our responsibility to assure that Departmental systems operate in accordance with Section 222(b) of our authorizing statute—that information in DHS Systems of Records is handled in a manner consistent with the fair information practices principles set out in the Privacy Act.

The main oversight mechanism used by the Privacy Office for information systems is the Privacy Impact Assessment (PIA). PIAs are fundamental in making privacy an operational element within the Department. Conducting PIAs demonstrates the Department's efforts to assess the privacy impact of utilizing new or changing information systems, including attention to mitigating privacy risks. Touching on the breadth of privacy issues, PIAs allow the examination of the privacy questions that may surround a program or system's collection of information, including commercial reseller data, as well as the system's overall development and deployment. When worked on early in the development process, PIAs provide an opportunity for program managers and system owners to build privacy protections into a program or system in the beginning. This avoids forcing the protections in at the end of the developmental cycle when remedies can be more difficult and costly to implement.

With respect to the data types that are collected and their handling, the PIA process augments the Systems of Record Notice provisions in the Privacy Act that provide notice to the public about the types of information collected and its treatment. The PIA can be one of the most important instruments in establishing trust between the Department's operations and the public.

In accordance with Section 208 of the E-Government Act of 2002 and OMB's implementing guidance, the Department of Homeland Security is required to perform PIAs whenever it procures new information technology systems or substantially modifies existing systems that contain personal information. Although the E-Government Act allows exceptions from the PIA requirement for national security systems, DHS is implementing Section 222 of the Homeland Security Act to require that all DHS systems, including national security systems, must undergo a PIA if they contain personal information. The Privacy Office has staff with security clearances that allow them to work with programs to assess the privacy impact of classified systems or systems that contain classified information. In cases where the publication of the PIA would be detrimental to national security, the PIA document may not be published or may be published in redacted form.

Every PIA must address at least two issues:

[1] The Homeland Security Act of 2002, Pub. L. No. 107–296, Title II, § 116 Stat. 2155.

1. It must address the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and

2. It must evaluate the protections and alternative processes for handling information to mitigate potential privacy risks.

The Privacy Office has issued official guidance on the conduct of Privacy Impact Assessments. The most up-to-date version of the guidance is available at the DHS Privacy Office Web site at *http://www.dhs.gov/dhspublic/interapp/editorial/editorial—0511.xml.* However, earlier versions of the guidance have been available internally to DHS for about two years, with initial guidance issued in February 2004.

Various sections of the PIA guidance are particularly relevant to the subject matter of this hearing. First, the guidance states that the PIA requirement applies broadly to personally identifiable information rather than to a much narrower category of "private" information. If information can be connected with an individual, it is personally identifiable information, whether or not the information is private or secret. This is important because much of the information purchased from information resellers is either publicly available, e.g., addresses and telephone numbers, or is derived from public records.

In addition, Section 1.2.2 of the guidance directs programs that use data from commercial data aggregators to state this fact and then to explain in Section 1.3 why data from this source is being used. Section 2.3.4 requires a statement about whether data obtained from commercial data aggregators is assessed for quality, and if so, what quality measures are used.

Some products offered by information resellers permit users to "ping" resellers' databases either to obtain new information or to verify information in government databases. This ability to access information without bringing it into Federal systems raises the question about when information is actually "collected" by a government agency. It is DHS policy that any time information from an information reseller is used in a decision-making process, whether the decision involves correcting existing government information or obtaining new information, a PIA is required.

In order to clarify specific issues related to the use of data from information resellers, the DHS Privacy Office is in the process of drafting specific guidance on the use of commercial data to complement the general PIA guidance. The guidance on the use of commercial data will apply specifically to the use of data from information resellers and will address three broad categories of use: comparing data in commercial and government databases, obtaining data from commercial sources for use in government systems; and use of government analytic tools on commercial databases. The guidance will specify when PIAs must be performed and what additional requirements might apply to programs that use data from commercial sources. We expect this guidance to be released as soon as it completes Departmental clearance, and would be happy to discuss it with you at that time.

The DHS Privacy Office has been part of a broad-based national dialog on these issues. In September of 2005, the Privacy Office held a public workshop on the use of commercial data for homeland security. The objective of the workshop was to look at the policy, legal, and technology issues associated with the government's use of commercial personally identifiable data in homeland security. A broad range of experts, including representatives from government, academia, and business participated in the panel discussions. The panels addressed how government agencies are using commercial data to aid in homeland security; the legal issues raised by the government's use of commercial data, particularly the applicability of the Privacy Act; current and developing technologies that can aid the government in data analysis; ways in which technology can help protect individual privacy while enabling government agencies to analyze data; and ways to build privacy protections into the government's use of commercial data. At the end of each panel, the audience was given an opportunity to address questions to the panelists. The full transcript of the Workshop is available at www.dhs.gov/privacy. A report summarizing the workshop is attached.

The Privacy Office has also been working with the DHS Data Privacy and Integrity Advisory Committee (DPIAC) on issues related to the use of commercial data. In October 2005, the DPIAC published a report on the use of commercial data to reduce false positives in screening programs. The report is available on the DHS Privacy Office Web site at http://www.dhs.gov/interweb/assetlibrary/privacy—advcom—rpt—1streport.pdf. The Committee recommends that commercial data be used for screening programs only when:

- It is necessary to satisfy a defined purpose
- The minimization principle is used
- Data quality issues are analyzed and satisfactorily resolved
- Access to the data is tightly controlled

- The potential harm to the individual from a false positive misidentification is substantial
- Use for secondary purposes is tightly controlled
- Transfer to third parties is carefully managed
- Robust security measures are employed
- The data are retained only for the minimum necessary period of time
- Transparency and oversight are provided
- The restrictions of the Privacy Act are applied, regardless of whether an exemption may apply
- Simple and effective redress is provided
- Less invasive alternatives are exhausted

The Committee is now working on a broader report that addresses the use of commercial data in applications beyond screening. We are using the work of the DPIAC to help inform our work on guidance for the Department.

We are living through a time of tremendous change as more and more personal information becomes electronic. In electronic form such information is more easily collected, analyzed and used for various purposes and serves as a basis for decision-making in personal, social, political and economic spheres. It is the goal of the DHS Privacy Office to ensure that commercial information used by the Department in the performance of its mission is used responsibly and with respect for individuals' legitimate expectations of privacy. We look forward to working with the Committee and everyone involved on these important issues.

Thank you.

Mr. CANNON. We are thrilled how well you all have done in that office.

Ms. COONEY. Thank you.

Mr. CANNON. It has been a great model for what we have done otherwise, what we hope to do still.

Professor Swire, you are recognized for 5 minutes.

TESTIMONY OF PETER SWIRE, WILLIAM O'NEILL PROFESSOR OF LAW, MORITZ COLLEGE OF LAW OF THE OHIO STATE UNIVERSITY, VISITING SENIOR FELLOW, CENTER FOR AMERICAN PROGRESS

Mr. SWIRE. Thank you, Mr. Chairman, and thank you to the Committee for the invitation to participate today. And I express my appreciation for the leadership this Committee has shown, including in creating the Chief Privacy Officer office that we have just heard the impressive discussion from Ms. Cooney.

In my written testimony, I give a little bit of the history of this topic. In 1974, when the Privacy Act was passed, the most important databases were primarily Government databases, like IRS or Social Security. Today, by contrast, the databases are dominated by private-sector databases. That is where the records are. So the big question is how do we update our laws and practices to this new reality.

The overall theme of my testimony is that we are still early on the learning curve about how to incorporate private databases into public agency activities. My written testimony gives some comments on the GAO report and the Fair Information Practices, but I highlight four recommendations.

First, because Federal agencies make such important decisions based on the data, we must have accurate data and we have to have effective ways to get redress when mistakes inevitably do occur.

Second, new mechanisms of accountability are likely needed as agencies rely more and more on these private-sector records. There should be expanded use of privacy impact assessments, perhaps along the line of Chairman Chabot's bill, and there are other steps that I will go into.

Third, greater expertise and leadership is needed in the executive branch at the highest levels on privacy issues, including policy leadership from the Executive Office of the President. The lack of such leadership on privacy, I believe, has led to significant and avoidable problems.

Fourth, as we continue along the learning curve, it is important to merge today's discussion about privacy with the discussions about information sharing in the war on terror, and I suggest a National Academy of Sciences study on privacy and information sharing might be useful.

Let me turn to a couple of things in more detail.

In order to think about accuracy of data over time, I think it makes sense for the Government to test and audit the accuracy of data, at least selectively, at the time that we purchase the data. S. 1789, the data breach bill that has been passed by the Senate Judiciary Committee, calls for audits like this as new Government contracts are formed. I think that might help us get a sense of where the accuracy is and isn't.

However accurate data is on the front end, though, we are going to have issues on the back end. We are going to have mistakes that get made. Many people on the Committee likely know about the troubles that Senator Kennedy or Congressman Lewis have had getting off watch lists. Last month, Senator Ted Stevens of Alaska told the story about his wife, which I hadn't heard about until I was researching this. Apparently, she was having great trouble getting on airplanes. Her first name is Catherine, the nickname for that is "Cat," and they had her down as Cat Stevens and she was having trouble getting on airplanes.

Now, if it is tough for Senators, including quite powerful Senators, to get their family members off of watch lists, it suggests there are issues for all 300 million Americans. So how we do redress is something to really think about going forward.

In the testimony I discuss some of the other accountability mechanisms—privacy impact assessments and the rest—that I think can be considered and cites to legislation that does some of this.

I would like to turn to the question of the structure of privacy protection in the executive branch. Step one has been creation by your Committee of the Chief Privacy Officer in Homeland Security and now elsewhere, and I was pleased to get to testify on that in 2002 before your Committee when that was set up. In 2004, Congress created the Privacy and Civil Liberties Board for intelligence activities only. But the gap is for the rest, which is where a lot of commercial data is used. There is no White House leadership, there is no policy official who is on the job there. One recent example, I think, illustrates the need to have a policy official looking at these issues up front and correcting problems.

You might have seen press reports about 2 weeks ago that the IRS has a proposed rule now to allow tax preparation companies, for the first time, to sell people's tax records or even to give them

away to people with no limits on how they then get resold or redisclosed. It would be legal under this, if I sign my name for my company, to put my tax records up on the Internet. It is supposed to be done with consent, but, you know, when you sign your tax forms, you sign in about 27 places and maybe you missed this one. And suddenly you have consented to sale of your tax records.

Now, when I worked at OMB, my office reviewed proposals such as this. We got it before it became policy. I think we would have noticed the lack of limits on redisclosure and resale. And I don't think the rule would have gone forward the way it did. If such a mistake had happened, I think we would have moved to correct it. But now this rule may be going final, and without a White House ability currently to spot and correct such mistakes, privacy problems, I think, turn out to be worse than they ought to be. So I think continued steps toward leadership on privacy in the executive branch are called for.

The last point I want to make in my testimony is we have hearings on information sharing, how we have to use the data to fight terrorism, and we have hearings on privacy, how we have to stop uses of data that might lead to identity theft and the rest. I think we probably need to bring those two things together. One way to do that might be a National Academy of Sciences study on the two that would involve commercial databases but also how to do privacy and information sharing. I have been working on this in my own research. I think it is a big issue that a lot of people should come together to examine. So I suggest that as one possible thing for your Committee to consider.

Thank you, and I look forward to questions.

[The prepared statement of Mr. Swire follows:]

PREPARED STATEMENT OF PETER SWIRE

Testimony of Professor Peter P. Swire

C. William O'Neill Professor of Law
The Ohio State University

Visiting Senior Fellow
Center for American Progress

Before the
Subcommittee on Commercial and Administrative Law
and the
Subcommittee on the Constitution
of the
Judiciary Committee of the U.S. House of Representatives

Oversight Hearing on "Personal Information Acquired by the Government From Information Resellers: Is There Need for Improvement"

April 4, 2006

I thank the Committee for the invitation to testify before you today on the draft GAO Report "Privacy: Opportunities Exist for Agencies and Information Resellers to More Fully Adhere to Key Principles."

The testimony briefly describes my background and the history of today's topic. In 1974, when the Privacy Act was passed, the most important databases used by the government were developed by the government. Today, by contrast, the private sector assembles a far greater portion of the databases that are useful and relied on by government agencies. The big question is how we update our laws and practices to this new reality.

The overall theme of my testimony is that we are still early on the learning curve about how to incorporate private databases into public-sector actions. My testimony first gives some comments on the way the Report interprets the Fair Information Practices. It then makes the following principle recommendations:

1. Because agencies make such important decisions based on the data, it is essential to have accurate data and effective ways to get redress for the mistakes that inevitably occur.

2. New mechanisms of accountability are likely needed as agencies rely more heavily on non-government suppliers of data. There should be expanded use of privacy impact assessments. The government contractor provisions in S. 1789, a data-breach bill, also illustrate additional steps that may be useful.

3. Greater expertise and leadership is needed in the executive branch on privacy issues, notably including policy leadership within the Executive Office of the President. The lack of such leadership on privacy has led to significant, avoidable problems.

4. As we continue along the learning curve, it is important to merge today's discussion about privacy protection with the ongoing debates about the need for information sharing within the government. The Committee may wish to support creating a National Academy of Sciences study on privacy and information sharing, including the use of commercial data by the federal government.

Background of the Witness

I am the C. William O'Neill Professor of Law at the Moritz College of Law of the Ohio State University. I am also a Visiting Senior Fellow at the Center for American Progress, a think tank based here in Washington, D.C.[1]

I have written extensively on a wide range of information privacy and security issues, including as lead author of a book on U.S. and E.U. privacy law, published by the Brookings Institution in 1998. From 1999 until early 2001, I served in the U.S. Office of

Management and Budget, as the Chief Counselor for Privacy. My writings appear at www.peterswire.net.[2]

Introduction: Moving up the Learning Curve about Government Use of Commercial Databases

My overall theme today is that the GAO Report is a step along our learning curve about the government's use of commercial databases that contain personal information. This hearing continues the process of clarifying the topic, so that we can better use commercial information when that is appropriate but also avoid the risks that arise from incorrect use of personal information.

A brief look at the history helps us understand why the present use of commercial databases is so different from the past. The Privacy Act was passed in 1974 due to the new accumulations of government information about individuals. This was the mainframe era, when government agencies such as the Social Security Administration and the Internal Revenue Service had the most computerized and detailed records that existed about most Americans. The Privacy Act put limits on how information could be shared among agencies, and essentially prevented one massive database of government records from being created.

Today, by contrast, the private sector holds enormously more and more detailed computerized records than does the government about individuals in our country. Today, an ordinary laptop has more computing power than the mainframe of the 1970s. Today, our personal computers can share data at a volume unimaginable not long ago. In the private sector, many records, and especially those in the public domain, are gathered by companies that specialize in the business of re-selling that information. The private sector relies on these information resellers for many purposes, including fraud prevention, target marketing, and finding people for reasons that range from newspaper interviews to witnesses for litigation.

Because the private sector finds it useful and cost-effective to rely on information resellers, it is not surprising that government agencies would also wish to use these services in analogous settings. The GAO Report that is the subject of today's hearing demonstrates these analogous uses, such as fraud prevention and location of witnesses for litigation. The GAO Report also shows that information from resellers is used for additional purposes that are specific to the public sector, notably and apparently most often for law enforcement investigations.

To summarize the history, government agencies held the largest databases of personal information in the 1970s. Today, the largest volume of data is held in the private sector, and this hearing concerns the rules of the road for government access to those private-sector databases.

Comments on the Fair Information Practices

As the GAO Report correctly states, Fair Information Practices ("FIPs") have been used as a key basis for privacy laws and practices, both in the United States and around the world. Most prominently, the Organization for Economic Cooperation and Development in 1980 promulgated the "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data." During the past quarter-century, the Guidelines have remained influential in forming privacy law and policy. The precise implementation of the OECD principles has also varied considerably as privacy laws have been created for different countries, different sectors, and at different stages of technological development.

The GAO Report uses the OECD Guidelines to test current practices in federal agencies and by information resellers. In doing so, the Report differs from my understanding of the FIPs with respect to the public domain and public records.

The Report briefly mentions but then does not rely on the concept of "publicly available information." (P. 11) Information that has been published in a newspaper, put on a Web site, or otherwise made public is treated differently than information that is kept confidential in the files of a government agency or doctor's office. The idea of "minimization of use" does not apply to information that is publicly available. Instead, this is the realm of the public domain, protected by the First Amendment and the analogous free press provisions in Europe and elsewhere, where we expect and encourage intensive scrutiny and use of facts and ideas. In my reading, the Report appears to criticize agencies and resellers for failure to minimize use of data in the public domain. That criticism is not consistent with how we have written privacy laws in the United States. The Gramm-Leach-Bliley Act, for instance, only applies to "nonpublic personal information." Public personal information is generally outside the scope of privacy laws, and such public information is one significant portion of the reselling industry.

This lack of attention to the public domain undermines a key finding of the Report, that "the nature of the information reseller business is fundamentally at odds with the principles of collection limitation, data quality, purpose specification, and use limitation. These principles center on strictly limiting the collection and use of personal information." (p. 9)[3] To the extent that resellers are collecting public domain information and presenting it in more usable form, then I do not agree with the Report's conclusion that resellers are "fundamentally at odds" with the Guidelines.

What should be in public records? With that said, the important debate then shifts to what information is properly in the public domain. In particular, there is a major and complicated debate about what personal information should be included in "public records" that are released by government.

During my time at OMB, we examined exactly that question in a report about privacy and the use of personal information in bankruptcy records.[4] The key question was whether any changes should be made to the definition of "public record" as traditional paper records shifted online. The clear answer was that some changes were needed. In particular, we recommended that Social Security Numbers and bank account

numbers not be placed in online records, because of the high risk of identity theft. It didn't make sense, in our view, to have people's bank account numbers be available for easy browsing. Since that time, the Courtroom 21 Project and many state-level projects have been working on the right way to have records go online while still protecting privacy. There should be ongoing legislative attention to this definition of public records, and I am concerned that there has been little or no focus on the issue at the federal level since the bankruptcy report in January, 2001.

Beyond public records – toward framework legislation for privacy protection. Information resellers also provide personal data beyond that contained in public records or other parts of the public domain. For instance, resellers may provide so-called "credit header" information to identify individuals, and may draw on an array of private-sector sources of information to create lists for marketing, antifraud, and other purposes. There are longstanding debates about the private-sector uses of credit header and other information. I will not try to sort through those debates today.

The simple point for this discussion is that some government uses of commercial databases are quite analogous to private-sector uses. The benefits of using the data are often similar, such as to locate individuals or prevent fraud. The risks of using the data are also often similar, such as facilitating identity theft or giving individuals the feeling that they have lost control over their personal information and thus their identity.

Where public agencies are using data for the same tasks as private entities, then similar sorts of safeguards are generally appropriate in both the public and private sectors. To address these similar risks, I have begun working with a number of companies and public interest groups to see if the time has come in this country for framework legislation to protect privacy. In short, similar risks of commercial databases should be treated similarly, whether the users are in the public or private sector.

Where government is unique. On the other hand, as discussed below in connection with redress, some government uses of data are different. The government makes uniquely important decisions based on personal information, including decisions to investigate and detain people in connection with criminal activity or to prevent terrorism. Where the government is making these sorts of unique decisions, then unique measures on data accuracy and redress are likely appropriate.

The Need for Data Accuracy and Effective Redress.

Because of the unique importance to individuals of governmental decisions, it is especially important to have accurate data on the front end, as agencies receive personal information. It is also especially important to have an effective means of redress on the back end, to correct the mistakes that inevitably occur.

In order to assure accuracy, it likely makes sense over time for the government to test and audit the accuracy of data received from commercial resellers. Better

governmental decisions will result from improved understanding about the accuracy (or inaccuracy) of types of data.

The need for data accuracy is a crucial basis for the fair information of practice of access, as discussed in the GAO Report. The idea, familiar from the Fair Credit Reporting Act, is that individuals should have access to their records and thus be able to correct mistakes. My experience, such as in the negotiation of the Safe Harbor with Europe in 2000, is that access has also been an especially controversial component of privacy debates in the U.S. Just last week, the House Energy and Commerce Committee included a provision for consumer access to information reseller databases as part of the data breach bill, H.R. 4127. By contrast, the version of the bill passed by the House Financial Services Committee, H.R. 3997, does not contain a consumer access provision.

This hearing today cannot resolve the general issue of access. I support effective access where that is feasible, but my experience is that there should be important exceptions, such as for law enforcement investigations and some anti-fraud efforts. In those settings, the benefits of access, such as improving data accuracy, are weighed against the risks of access, which notably include tipping off criminals about the investigation or giving fraudsters access to sensitive information.

However accurate data becomes as the input for government decisions, there will inevitably be some mistakes. For programs where the government is making decisions about individuals based on commercial databases, it thus is necessary to have an *effective means of redress* for those mistakes.

Special redress measures are required in government programs because of the serious and special nature of many of the decisions made by the government. Consider the consequences in the private sector if the wrong person ends up on a target marketing list provided by a reseller. The consequence for the company is the waste of a postage stamp, and the consequence for the individual is one more advertising leaflet that gets placed in the circular file.

By contrast, a mistake by the government can be far more serious. The wrong person may be detained as part of a law enforcement or immigration proceeding. The wrong person may be singled out for secondary screening or placed onto a watch list. The Committee likely knows about the troubles that Senator Edward Kennedy and Representative John Lewis have had getting off of watch lists. Last month, Senator Ted Stevens of Alaska publicly discussed the problems confronting his wife, Catherine. A short form of Catherine, you see, gives her the same name as someone now barred from entering the country, the singer Cat Stevens.

To the extent the government increasingly relies on commercial databases to make these government decisions, there must be an opportunity for redress that matches the importance of the government actions. When the system is so hard to manage even for Senators and Congressmen, then that is a sign that something better needs to be done for all 300 million Americans.

To summarize on accuracy and redress, the importance of government decisions means that, for the purchase of information from commercial resellers, special measures are likely needed for the government sector. Accuracy that is good enough for marketing is not necessarily good enough to detain a suspect. Redress measures that get someone off that marketing list are likely not sufficient for terrorist watch lists or other government programs. Recent reports give some good guidance for how those redress mechanisms should look.[5]

Mechanisms for Accountability and the Need for White House Leadership

As the history shows, the Privacy Act was designed for a world where the largest stores of data came from government databases. Today, privacy issues in government increasingly come from databases created in the private sector. To address this new reality, the government should continue to develop mechanisms for accountability. These mechanisms include: assurance of data quality; effective means of redress; privacy impact assessments; other measures in the procurement process; and greater Executive Branch leadership on privacy.

One step that has already been taken is in the OMB guidance under the E-Government Act of 2002. This guidance recognized for the first time that Privacy Impact Assessments (PIAs) should be performed for commercial sources: "when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources." By including this assessment of commercial sources of information, the guidance did a good update of protections. The guidance then went on to state: "Merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement." I think that use of a PIA may also be appropriate in the latter setting, especially where a commercial product is regularly used by the government and a large number of queries are made by the government.

The Senate Judiciary Committee has included a number of relevant provisions in its version of the proposed data breach legislation, S. 1789. Section 401 of that bill would require the General Services Administration to evaluate privacy and security issues on contracts for information of over $500,000. Section 402 would create procedures for evaluating and auditing of private-sector entities that support an agency's use of personal information. Section 403 requires a PIA before a contract is entered into for government contracting for access to private-sector databases. These provisions are quite detailed, and I have not studied them closely enough to have a view on each aspect. Taken together, however, the provisions show possible mechanisms for assessing the risks and benefits of new contracts for government purchase of personal information from the private sector.

Another component of assuring accountability is to have expertise and leadership on privacy issues within the federal government. This Committee took an important step in that direction in 2002, when it crafted the language that created the Chief Privacy

Officer for the Department of Homeland Security. This was the first time that such a privacy official had been specifically created by an Act of Congress. Having testified on the subject in that hearing in 2002, it is a particular pleasure for me to participate today with the current occupant of that position, Ms. Maureen Cooney, and to hear of the many actions the office is taking to protect privacy while also protecting our nation.

The Congress took another important step to institutionalize privacy protections when it created the Privacy and Civil Liberties Board as part of the intelligence reform law in 2004. After a lamentable delay, which lasted until this February, the members of the Board have now been nominated and confirmed. I have had the pleasure to meet with the Board's leadership, and I hope and believe the Board will play an important role in addressing privacy and civil liberties issues within the scope of its jurisdiction.

That jurisdiction is limited, however, to the intelligence community. As the GAO Report indicates, much of the current agency use of commercial databases occurs for other purposes. There is thus a notable gap of White House or inter-agency leadership on how to address the subject of today's hearing. When it comes to overall government policies for how to use commercial databases consistent with privacy, there is no policy official in the White House who has privacy as a principal concern.

I believe there should be. From my own experience in such a role, there are numerous and difficult issues that face agencies in the handling of personal information. Agencies benefit from an inter-agency structure that allows government-wide issues to be addressed in a coordinated fashion. These issues are sometimes technical and can be handled as such. These issues, however, often have a large policy component that benefits from policy leadership.

One recent example shows the need for leadership and privacy expertise from the Executive Branch. You may have seen press reports in the past two weeks that the IRS is proposing to change its rules to allow tax preparers for the first time to sell tax returns to outside parties, or even to have the outside parties release tax returns publicly. The release of tax returns would happen only with signed consent, but this consent can easily happen when a tax preparer tells the busy customer just to "sign here and here and here."

When I worked at OMB, my office reviewed proposals such as this. We would have noticed the total absence of limits on redisclosure and resale. The proposed rule would not have gone forward the way it did here. If such a mistake had happened, we would have moved quickly to correct it. Without a White House ability to spot and correct such mistakes, privacy problems will continue to be much worse than they ought to be.

Information Sharing as One Area for Further Study

Up to this point, I have focused on topics covered by the GAO report. I am concerned, however, that the report has been done in isolation from the way that many issues of government data use are being considered today. I refer to the view, voiced by

the 9/11 Commission and elsewhere, that the government must do much more "information sharing" in the wake of the September 11 attacks.

Everyone in this town knows the importance of how you frame an issue. If you have a hearing one day about "the need for information sharing," then most people will cheer and we will want to open up the spigots to those flows. If you hold another hearing the next day about "invasion of privacy and identity theft," then some of those same people might cheer and say we should stop this over-use of data.

To achieve national security and privacy, we need to bring these two discussions together. I am currently doing research on this topic. The DHS Advisory Committee on Privacy and Security recently released a document that addresses some of the same issues.[6]

My own research in this area has convinced me both of its importance and complexity. I therefore offer a suggestion to the Committee about one step to consider – a National Academy of Science study on privacy and information sharing, including the use of commercial data by the federal government. The National Academy of Sciences has done other excellent work on mixed topics of science and policy. Assembling a group of experts to do such a study may be the most promising route to moving us up the learning curve. We know that the sources of data are very different today than when the Privacy Act was drafted in 1974. The proper use and dissemination within the government of today's data is thus a timely and important topic for study, and then for action.

---

[1] Today's testimony draws in part on "*Protecting Privacy in the Digital Age*: American Progress Recommendations on Government's Use of Commercial Databases," (May 4, 2005), available at http://www.americanprogress.org/site/pp.asp?c=biJRJ8OVF&b=651807.

[2] In 2004-05 I was a member of the Information Policy Forum, an unpaid group of persons from the non-profit sector that Lexis/Nexis asked for advice on information policy issues. I am no longer on that group, and am not affiliated with any information resellers.

[3] Later, the Report says that the purposes for collecting data must be those stated in advance or those "compatible" with the original purposes. By paraphrasing the OECD Guidelines, the Report misses one of the topics that was most debated in 1980, that uses are permitted where they are "not incompatible" with the original purposes. That is, use of personal data is in fact permitted, so long as the use is "not incompatible" with the original uses. In my experience, this shift in terminology has often been used as a basis for explaining why the Guidelines permit greater use of personal information, and more exceptions to privacy laws, than might otherwise be understood.

[4] U.S. Office of Management and Budget, Department of Justice, and Treasury Department, "Study of Financial Privacy and Bankruptcy," January 2001, available at http://www.privacy2000.org/presidential/OMB_1-01_Study_of_Financial_Privacy.htm.

[5] My Ohio State colleague Peter Shane has written "The Bureaucratic Due Process of Government Watch Lists," Mar. 6, 2006, available at http://law.bepress.com/expresso/eps/1084. Technologist Jeff Jonas and Paul Rosenzweig, now an official in the Department of Homeland Security, have written "Correcting False

Positives: Redress and the Watch List Conundrum," June 17, 2005, available at http://www.heritage.org/Research/HomelandDefense/lm17.cfm.

[6] Report of the Department of Homeland Security Data Privacy and Integrity Advisory Committee, "Framework for Privacy Analysis of Programs, Technologies, and Applications," Rep. No. 2006-1, adopted Mar. 7, 2006, available at http://www.privacilla.org/releases/DHS_Privacy_Framework.pdf.

Mr. CANNON. Thank you, Professor.
Mr. Pratt?

TESTIMONY OF STUART PRATT, PRESIDENT AND CHIEF EXECUTIVE OFFICER, CONSUMER DATA INDUSTRY ASSOCIATION

Mr. PRATT. Chairmen Cannon and Chabot, Ranking Members Watt and Nadler, Members of the Committees, thank you for this opportunity to appear before you today.

We are here to discuss the GAO's report regarding Government uses of data and some concerns that we do have with regard to that report, that we hope will inform your thinking here as the Committee.

First, while the report does survey governmental uses of our members' systems, it does not discuss the value and effectiveness of them. Government agencies are faced with extraordinary challenges in accomplishing their missions. Consider just a few examples of those: preventing money laundering and terrorist financing, enforcing child support orders, locating missing and exploited children, researching fugitives, researching assets held by individuals of interest, witness location, entitlement fraud, background screening for national security investigations, and disaster assistance, as was mentioned.

A real-world example of how these systems work, a public record provider can provide for as little as $25 a search of 100 million criminal records in order for that to be done. Otherwise, you would have to spend approximately $48,000 and it would take days, if not weeks, to accomplish the same search.

These are just one of a number of examples we include in our written testimony of the direct value of data products that our members produce.

We do have other concerns with the report beyond its lack of an adequate description of the value of our members' services. First, the report does not help the reader understand the breadth of the application of Federal laws to data products used by Government agencies today. The report lists laws, but it relegates an incomplete discussion of their requirements to an appendix. Chairman Chabot mentioned several of these laws. There is one that is not acknowledged directly in the report, and that is that the FTC Act, section 5, also applies to data practices and it does include enforcement actions relative to privacy notices as well as to the security of sensitive personal information.

One such law, the Fair Credit Reporting Act, applies to the public sector equally as it does to the private sector, and thus all decisions where there is a determination of a consumer's eligibility such as approval or denial are made, extensive rights are accorded to that consumer under this statute. This is just one of many Federal statutes that need to be considered in the context of this discussion today.

The GAO report does commingle a variety of different business models under a single uniform "information reseller" term and then attempts to monolithically apply the OECD privacy guidelines across every business model and every product. In doing so, we think they make a mistake in thinking that Fair Information Practices frameworks can operate as a one-size-fits-all yardstick. We

disagree, and the guidelines themselves caution against such an approach. In fact, they state that the application of the guidelines should be considered in the context of different categories of personal information, different protective measures to be applied, depending on their nature and the context in which they are collected, stored, processed, and disseminated. We don't think that the GAO fully adhered to this OECD guidance itself, and there are certainly other privacy guidelines that are more contemporary than those of the OECD that were produced back in 1980.

Again, the implication of the GAO's report is that congressional oversight was also incomplete and that its review of the industry sector's uses of personal information was insufficient. We disagree. The GAO does not properly account for the system, for example, of public records in this country and the inapplicability of many of the privacy principles to such public records.

Just a couple of examples of how the actual privacy principles would or wouldn't apply.

Consumer consent. If consumers had the ability to consent or to control data that would go into a fraud prevention tool, criminals could simply prohibit the kind of information we use to stop identity theft.

Data quality. If a consumer could—if we applied data quality to the principle of public records in the way that we would under the way that we would under the Fair Credit Reporting Act, we probably couldn't aggregate a system of criminal histories in this country the way that we do today.

Use limitations. How would you apply a use limitation concept to criminal histories or other types of public records—records of eviction, professional licensing—used for background screening in the way that we do today?

Access and correction. If we allow all types of databases to be tied to an access and correction standard, then we are allowing a fraudster to have access to a fraud prevention system, and not only to do so but then to correct the information that is used to prevent the very fraud which they are going to attempt to commit.

The GAO report states in its conclusion that, Given that reseller data may be used for many purposes that could affect an individual's livelihood and rights, ensuring that individuals have appropriate degrees of control or influence over the way in which their personal information is obtained and used—as envisioned in the Fair Information Practices—is critical.

I don't know that we disagree with that, but we disagree with the application of the principles, as we have discussed in our testimony. A one-size-fits-all approach simply can't work for all types of data systems that we have discussed. We also don't think that the OECD guidelines should be used as an overlay for all of the Federal laws that do today regulate various aspects of personal information that are used in our society today.

With that, we thank you for this opportunity to testify and we welcome your questions.

[The prepared statement of Mr. Pratt follows:]

PREPARED STATEMENT OF STUART K. PRATT

Chairmen Cannon and Chabot, Ranking members Watt and Nadler, and members of the committees, thank you for this opportunity to appear before you today. For the record, my name is Stuart Pratt and I am president and CEO of the Consumer Data Industry Association.[1] Our members appreciate this opportunity to discuss our serious concerns with basic premises which underlie and methodologies employed in drafting the report written by the General Accountability Office (GAO) regarding the government's use of data provided by consumer data companies.[2]

THE RECOGNIZED VALUE OF CDIA MEMBERS' SYSTEMS

CDIA's members are the leading companies producing consumer data products and services for both the private and public sector markets. The GAO report surveys governmental uses of our members' systems, but leaves the reader with a less than complete perspective on the value and effectiveness of such services. Consider the following examples of governmental uses of our members products and services:

- Preventing money laundering and terrorist financing through investigative tools.
- Enforcing child support orders through the use of sophisticated location tools.[3]
- Assisting law enforcement and private agencies which locate missing and exploited children through location tools.
- Researching fugitives, assets held by individuals of interest through the use of investigative tools which allow law enforcement agencies tie together disparate data on given individuals and thus to effectively target manpower resources.
- Witness location through use of location tools.
- Entitlement fraud prevention, eligibility determinations, and identity verification through fraud prevention data matching and analytical products.
- Background screening for employment and security clearances.
- Disaster assistance.

Homeland security, law enforcement and entitlement program management are all faced with extraordinary challenges in accomplishing their missions. The GAO's report does not properly set the stage for understanding how difficult it is to accomplish their missions. Consider the facts regarding simply identity verification:

Personal identifiers change:

While it probably doesn't occur to most of us, the identifiers we use in everyday life do change and more often than most might think. For example, data from the U.S. Postal Service and the U.S. Census confirm that over 40 million addresses change every year. More than three million last names change due to marriage and divorce. While trends in naming conventions are changing, this fact is still far more often true for women than men.

We use our identifiers inconsistently:

It is a fact that we use our identifiers inconsistently for a wide variety of reasons. First, many citizens choose to use nicknames rather than a given name. However, there are times where, in official transactions, a full name is required, Some consumers, when hurried, use an initial coupled with a last name, rather than their full name or nickname. Consumers are also inconsistent in the use of generational designations (e.g., III, or Sr.). Finally, there are times where consumers themselves do make mistakes when completing applications, such as transposing a digit in an SSN. Thus, a consumer's identifiers may be presented in different ways in different databases and, in some cases, the data may be partially incorrect.

---

[1] CDIA, as we are commonly known, is the international trade association representing over 300 consumer data companies that provide fraud prevention and risk management products, credit and mortgage reports, tenant and employment screening services, check fraud and verification services, systems for insurance underwriting and also collection services.

[2] The GAO employs the term information reseller and we have concerns with the use of the term which will be discussed later in this testimony. For example we do not believe that the term "consumer reporting agency" as defined by the Fair Credit Reporting Act should be commingled with other data products due to the specificity of law which regulates this product. The GAO fails to draw this distinction in its draft report.

[3] In 2004 there were 5.5 million location searches conducted by child support enforcement agencies to enforce court orders.

Personal identifiers are not always unique:

We think of our names as a very personal part of who we are. However, our names are less uncommon and unique than we might think. For example, families carry forward family naming conventions leading to some consumers sharing entirely the same name. Further, U.S. Census data shows that both first and last names are, in some cases amazingly common. Fully 2.5 million consumers share the last name Smith. Another 3 million share the name Jones and more than thirteen million consumers have one of ten common last names. First names are also used very commonly leading to common naming combinations. Eight million males have either the name James or John and a total of 57 million males have one of ten common first names. An additional 26 million females have one of ten common first names. Common naming conventions make it more difficult and in some cases impossible to depend on name alone to properly match consumer data.

Identifiers are shared:

Our birthday is a unique day in our lives, but it is, nonetheless, a date shared with hundreds of thousands of others. Date of birth alone is not an effective identifier. Family members who live together end up sharing addresses and per our discussion above, where consumers share the same name due to family traditions and the address at which they live, distinguishing one consumer from another is complex.

Data entry errors do happen:

Hundreds of millions of applications for credit, insurance, cellular phone services, and more are processed every year. There is no doubt that in the process of entering a consumer's identifying information errors can be made which carry forward into databases and into the reporting of data to consumer reporting agencies.

We do not always update our records:

Consumers don't always remember to update records when they move or when portions of their personal identifying information change. For example, consumers are permitted to change their social security number under certain circumstances in addition to officially changing their names and while the percentages of consumers who take these steps is small relative to the U.S. population, such changes do affect data matching systems. It is important to know that some consumers try to separate themselves from their records on purpose and apply with the SSA for employer ID numbers (EINs) to use in lieu of their SSNs.[4] A non-custodial parent who does not want to pay child support might employ such tactics in order to avoid being located and forced to fulfill a court order. A consumer who does not want to take responsibility for their mismanagement of credit and hopes that by using new identifying to separate himself/herself from a credit report is another example. Clearly fugitives are another example of a type of person who will employ tactics to try and separate themselves from their histories.

These facts about our identifying information demonstrate how challenging it is to match records with individuals and why the products, tools and services of our members are in such high demand.

Let's now consider what government representatives themselves have said about the value they derive from the use of consumer reporting agencies and other consumer data companies. On September 8, 2005, the Department of Homeland Security held a workshop which explored its use of commercial data. This public meeting brought forward important input which informs the record of this hearing.

Regarding identity verification, Grace Mastalli, Principle Deputy Director for the Information Sharing and Collaboration Program in DHS stated the following regarding the value of CDIA member services: "There are people without prescriptions, without driver's licenses, and it the commercial data sources, in many instances right now, that are facilitating not just placing people, but verifying their identities to the claims . . .we get to make sure that entitlements go to individuals who deserve them."

Regarding how our members' systems contribute to the accuracy of governmental systems, Mastalli indicated that "we have sometimes used commercial data, not just to support identity authentication, but to assure the integrity of government data, and the accuracy of government data. Unfortunately, in many respects, the commer-

[4] The FTC investigates "file segregation" schemes. Here's what they say on their website about this activity: "You're promised a chance to hide unfavorable credit information by establishing a new credit identity. The problem: File segregation is illegal. If you use it, you could face fines or even a prison sentence."

cial enterprises have done better jobs of organizing and, what I call 'cleaning' data to eliminate errors in data."

Mr. Jeff Ross, senior advisor in the area of money laundering and terrorist financing, in the Office of Terrorist Financing and Financial Crime at the Department of Treasury, also participated in this DHS workshop. He pointed out that many crimes have a financial aspect to them including narcotics trafficking, public corruption, terrorist financing, and organized crime in general. His comments help explain the investigative research value of CDIA member tools where he states "so commercial data bases are very important to us in law enforcement area to be used proactively . . . we have targets and need information, where you are trying, also, to find a specific individual or entity that should be involved . . . who could also be potential witnesses in a case."

Mastalli provided a very concrete example of how the sophistication of private-sector data matching tools contributes to efficient use of governmental law enforcement agents. She noted that ". . . commercial database providers provide accurate data—often more accurate than some that we have, because they spend the time cleaning it and verifying it and have matching capabilities that we in government have not yet invested in to eliminate the 17 instances of an individual who has a phonetically spelled name being recorded as 17 people instead of one."

She goes on to explain that government cannot always anticipate what data might be of value to a particular investigation. Mastalli provided the following scenario: "One extremely well-known law enforcement intelligence example from immediately post 9/11 was when there was a now well-publicized threat . . . that there might be cells of terrorists training for scuba diving underwater bombing, similar to those that trained for 9/11 to fly—but not land—planes. How does the government best acquire that? The FBI applied the standard shoe-leather approach—spent millions of dollars sending out every agent in every office in the country to identify certified scuba training schools. The alternative could and should have been for the Federal government to be able to buy that data for a couple of hundred dollars from a commercial provider, and to use that baseline and law enforcement resources, starting with the commercial baseline. One of the issues here is that, other than the name of the owner or manager of scuba diving schools, there was no personally identifiable data."

To further the point regarding the value of commercial data our members supply, consider the following two examples:

Example 1:

In this example we learn how the aggregation of public records creates low-cost research efficiencies that ensure that "shoe leather" investigations conducted by highly trained personnel are truly are targeted and results-focused. One commercial database provider charges just $25 for an instant comprehensive search of multiple criminal record sources, including fugitive files, state and county criminal record repositories, proprietary criminal record information, and prison, parole and release files, representing more than 100 million criminal records across the United States.[5] In contrast, an in-person, local search of one local courthouse for felony and misdemeanor records takes 3 business days and costs $16 plus courthouse fees.[6] An in-person search of every county courthouse would cost $48,544 (3,034 county governments times $16). Similarly, a state sexual offender search costs just $9 and includes states that do not provide online registries of sexual offenders. An in-person search of sexual offender records in all 50 states would cost $800.[7]

Example 2:

While this next example is drawn from the private sector, it helps illustrate how fraud prevention and identity verification services reduce fraud and is analogous to the value of such systems when used by the government, as well. A national credit card issuer reports that they approve more than 19 million applications for credit every year. In fact they process more than 90,000 applications every day, with an approval rate of approximately sixty percent. This creditor reports that they identify one fraudulent account for every 1,613 applications approved. This means that the

---

[5] *http://www.choicetrust.com/servlet/com.kx.cs.servlets.CsServlet?channel=home&product=bgcheck&subproduct=default&anchor=#.* All RVI providers recommend that employers should supplement 'no criminal record found' results with a local county records search before making a hiring decision as any national criminal database will not contain all current criminal records since courthouses add new records daily.

[6] Id.

[7] Assuming each in-person search costs $16, the same as an in-person county courthouse search.

tools our members provided were preventing fraud in more than 99.9 percent of the transactions processed.

The GAO paper should have done more to speak to the value of the commercially available data and analytical tools our members provide and not merely to provide an accounting of governmental uses. We hope that the above discussion will inform the this hearing record and set a more complete context for these committees' future deliberations.

CONCERNS WITH GAO'S REPORT

Now having an appropriate context for truly understanding the value that our members' services bring to both the public and private sectors, I would like to discuss serious concerns we have with the GAO's presentation of current Federal laws and how they regulate our members' practices as well as their attempt to apply the 1980 Organization for Economic Development (OECD) privacy guidelines to the practices of "information resellers." We believe that a thorough understanding of the decades of congressional oversight and action is essential to today's hearing.

The State of Current Federal Laws

The United States is on the forefront of establishing sector-specific and enforceable laws regulating uses of personal information of many types. The GAO does provide an accounting of some of these Acts on page 18 of their draft report. Their accounting includes the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.),[8] The Gramm-Leach-Bliley Act (Pub. L. 106–102, Title V),the Health Insurance Portability and Accountability Act (Pub. L. 104–191), and the Drivers Privacy Protection Act (18 U.S.C. 2721 et seq.).

While the GAO relegates their discussion of statutory requirements to Appendix II of the draft report, we believe that such a discussion is essential and that it should have been included in the body of the report. In doing so, the GAO would have provided readers with a better one-to-one understanding of the operation of current laws in contrast with their views of the application of OECD guidelines US information practices.[9] For example, it is important to note that, predating the Privacy Act of 1974 (and OMB implementing guidelines therein), the OECD Guidelines of 1980 and the Gramm-Leach-Bliley Act of 1999 (and implementing regulations therein), the E-Government Act of 2002 and the Federal Information Security Management Act of 2002, was enactment of the Fair Credit Reporting Act in 1970. Equally important is understanding the breadth of the application of this law in particular and thus why a discussion of consumer data companies in general should not be commingled with a discussion of the practices of consumer reporting agencies.

The FCRA applies to both the private and public sectors and thus is extremely relevant to today's discussion. It has been the focus of careful oversight by the Congress resulting in significant changes in both 1996[10] and again in 2003.[11] There is no other law that is so current in ensuring consumer rights and protections are adequate.[12]

Key to understanding the role of the FCRA is the fact that it regulates any use of personal information (whether obtained from a public or private source) defined as a consumer report. A consumer report is defined as data which is gathered and shared with a third party for a determination of a consumer's eligibility for enumerated permissible purposes.

This concept of an eligibility test is a key to understanding how Federal laws regulate personal information. The United States has a law which makes clear that any third-party supplied data that is used to accept or deny, for example, my application for a government entitlement, employment,[13] credit (e.g., student loans), insurance, and any other transaction initiated by the consumer where there is a legitimate business need. The breadth of the application of the FCRA to how data is used

[8] The GAO also lists the Fair and Accurate Credit Transactions Act of 2003 (Pub. L. cite), however this act is in fact a series of amendments to the FCRA.

[9] CDIA has serious concerns about the attempt by the GAO to measure the acceptability of the practices of US consumer data companies, which are in fact regulated by US laws today. This concern will be discussed more fully later in this testimony.

[10] See Pub. L. 104–208, Title II, Subtitle D, Chapter 1).

[11] See FACT Act Amendments (Pub. L. 108–159).

[12] It is also true that the Gramm-Leach-Bliley Act, Title V provisions regulating the use of nonpublic personal information is current due to the extensive role that federal banking regulators and the Federal Trade Commission play in drafting regulations, issuing guidance and enforcing the law.

[13] This includes national security investigations, background checks for security clearances, basic employment screening processes for new hires, review processes for promotions, and more.

to include or exclude a consumer is enormous. Again, this law applies equally to governmental uses and not merely to the private sector.

Because personal information about consumers is used for decisions to accept or deny access to a consumer, they have fundamental rights which the GAO report does not discuss in any depth and which demonstrate why it is inappropriate to attempt to overlay a discussion of OECD privacy guidelines with this statute. Consider the following:

- The right of access—consumers may request at any time a disclosure of all information in their file at the time of the request. This right is enhanced by requirements that the cost of such disclosure must be free under a variety of circumstances including where there is suspected fraud, where a consumer is unemployed and seeking employment, or where a consumer is receiving public assistance and thus would not have the means to pay. Note that the right of access is absolute since the term file is defined in the FCRA and it includes the base information from which a consumer report is produced.
- The right of correction—a consumer may dispute any information in the file. The right of dispute is absolute and no fee may be charged.
- The right to know who has seen or reviewed information in the consumer's file—as part of the right of access, a consumer must see all "inquiries" made to the file and these inquiries include the trade name of the consumer and upon request, a disclosure of contact information, if available, for any inquirer to the consumer's file.
- The right to deny use of the file except for transactions initiated by the consumer—consumers have the right to opt out of non-initiated transactions, such as a mailed offer for a new credit card.
- The right to be notified when a consumer report has been used to take an adverse action—This right, ensures that I can act on all of the other rights enumerated above.
- Beyond the rights discussed above, with every disclosure of a file, consumers receive a notice providing a complete listing all consumer rights. A separate GAO report produced as a result of the FACT Act indicated that in a single year, perhaps 50 million consumers see their files and receive these notices.
- Finally, all such products are regulated for accuracy with a "reasonable procedures to ensure maximum possible accuracy" standard. Further all sources which provide data to consumer reporting agencies must also adhere to a standard of accuracy which, as a result of the FACT Act, now includes new rulemaking powers for the FTC and functional bank regulators.

The GAO report does not attempt to describe the delivery of products regulated under the FCRA and thus fails to properly inform the reader of the concomitant rights accorded in all of these cases. Every CDIA member mentioned in this report is operating, in part and sometimes solely as a consumer reporting agency. Therefore, in every case where products sold to governmental agencies were used for a determination of a consumer's eligibility, they were regulated by the FCRA with all of the rights discussed above. The GAO's report should have acknowledged this fact and discussed uses of consumer reports separately from other data products.

Not all consumer data products are used for eligibility determinations regulated by the FCRA. Congress has applied different standards of protection that are appropriate to the use, the sensitivity of the data, etc. Our members produce and sell a range of fraud prevention and location products which are governed by other laws such as GLB.

Fraud prevention systems deploy a diversity of strategies. In 2004 alone, businesses conducted more than 2.6 billion searches to check for fraudulent transactions. As the fraud problem has grown, industry has been forced to increase the complexity and sophistication of the fraud detection tools they use.

Fraud detection tools are also known as Reference, Verification and Information services or RVI services. RVI services are used not only to identify fraud, but also to locate and verify information for public and private sector uses. While fraud detection tools may differ, there are four key models used.

- **Fraud databases**—check for possible suspicious elements of customer information. These databases include past identities and records that have been used in known frauds or are on terrorist watch lists, suspect phone numbers or addresses, and records of inconsistent issue dates of SSNs and the given birth years.
- **Identity verification products**—crosscheck for consistency in identifying information supplied by the consumer by utilizing other sources of known

data about the consumer. Identity thieves must change pieces of information in their victim's files to avoid alerting others of their presence. Inconsistencies in name, address, or SSN associated with a name raise suspicions of possible fraud.

- **Quantitative fraud prediction models**—calculate fraud scores that predict the likelihood an application or proposed transaction is fraudulent. The power of these models is their ability to assess the cumulative significance of small inconsistencies or problems that may appear insignificant in isolation.
- **Identity element approaches**—use the analysis of pooled applications and other data to detect anomalies in typical business activity to identify potential fraudulent activity. These tools generally use anonymous consumer information to create macro-models of applications or credit card usage that deviates from normal information or spending patterns, as well as a series of applications with a common work number or address but under different names, or even the identification and further attention to geographical areas where there are spikes in what may be fraudulent activity.

Who uses Fraud Detection Tools?

The largest users of fraud detection tools are financial businesses, accounting for approximately 78 percent of all users. However, there are many non-financial business uses for fraud detection tools. Users include:

- **Governmental agencies**—Fraud detection tools are used by the IRS to locate assets of tax evaders, state agencies to find individuals who owe child support, law enforcement to assist in investigations, and by various federal and state agencies for employment background checks.
- **Private use**—Journalists use fraud detection services to locate sources, attorneys to find witnesses, and individuals use them to do background checks on childcare providers.

Location services and products

CDIA's members are also the leading location services providers in the United States. These services, which help locate individuals, are a key business-to-business tool that creates great value for consumers and business alike. Locator services depend on a variety of matching elements, but again, a key is the SSN. Consider the following examples of location service uses:

- There were 5.5 million location searches conducted by child support enforcement agencies to enforce court orders. Access to SSNs dramatically increases the ability of child support enforcement agencies to locate non-custodial, delinquent parents (often reported in the news with the moniker "deadbeat dads"). For example, the Financial Institution Data Match program required by the Personal Responsibility and Work Opportunity Reconciliation Act of 1996 (PL 104–193) led to the location of 700,000 delinquent individuals being linked to accounts worth nearly $2.5 billion.
- There were 378 million location searches used to enforce contractual obligations to pay debts.
- Tens of millions of searches were conducted by pension funds (location of beneficiaries), lawyers (witness location), blood donors organizations, as well as by organizations focused on missing and exploited children.

Clearly location services bring great benefit to consumers, governmental agencies and to businesses of all sizes.

CDIA CONCERNS WITH THE GAO'S USE OF TERM INFORMATION RESELLER

As discussed above, part our concern with the GAO's report is that it commingles a variety of different business models under a single term "information reseller" and in doing so the report also commingles data products which are regulated under different Federal laws. For example, CDIA's members which are operating as consumer reporting agencies should not be discussed in the report as though they are not in fact highly regulated businesses. Similarly, CDIA's members which are defined as "financial institutions" under GLB are also highly regulated with regard to how information is to be used (see Section 502(e)) as well as though extensive federal agency rules prescribing how such information should be secured.

By employing the term "information reseller" readers are left with the wrong impression that such a term may exist in law or that it is possible to consider the multiplicity of different business models (and products produced therein) that make up the consumer data industry as a single type of entity and one that, in the eyes of

the GAO, is not highly regulated. It is exceedingly difficult, if not impossible, to make meaningful statements which have the breadth of those often made in the draft report regarding the practices of many different types of business models delivering different products and services. Finally, we also strongly disagree with paper's attempt to simplify a discussion of our members' businesses which are in fact highly regulated under a variety of sector-specific laws by attempting to apply a set of OECD guidelines as though there are not laws which were thoroughly debated by the congress over the years and which are mature and protective of consumer's today.

CDIA CONCERNS WITH GAO OECD GUIDELINE APPLICATION

Let me amplify on our concerns regarding how the GAO has attempted to apply the 1980 OECD privacy guidelines as a scorecard against which to evaluate the practices of CDIA members. Due to the GAO's mistaken assumptions about the breadth of the application of current laws, the GAO also makes the mistake of thinking that a fair information practices framework can operate as a one-size-fits-all yardstick. We disagree for a variety of reasons.

First, we are concerned about how the GAO attempted to make use of the guidelines. Let us consider what the OECD said about their own guidelines:

> *These Guidelines should not be interpreted as preventing:*
>
> *a) the application, to different categories of personal data, of different protective measures depending upon their nature and the context in which they are collected, stored, processed or disseminated;*

Further to the question of how privacy guidelines are to be used, in the 1977 Report of the U.S. Privacy Protection Commission it was noted that "[P]rivacy, both as a societal value and as an individual interest, does not and cannot exist in a vacuum. . . . [T]he privacy protections afforded [to societal relationships] must be balanced against other significant values and interests. It is very common to find such statements associated with guidelines because they are not considered to be definitive rules with equal applicability to all data flows. We do not believe that the GAO's report adheres to this guidance provided by the authors of the OECD guidelines themselves or fully accounts for the U.S. Privacy Commission's admonition regarding how to apply guidelines.

Second, the GAO suggests, not purposefully, of course, but by omission that there is a single global opinion regarding which set of guiding principals is preeminent. To the contrary, consider the following:

- The 1973 HEW Report contains 5 principles.
- The 1980 OECD Guidelines contain 8 principles.
- The 1995 EU Data Protection Directive contains 11 principles.
- The 2000 FTC Report on Online Privacy contains 4 principles; and
- The 2004 APEC Privacy Framework contains 9 principles.

Each framework has to be applied with care and not monolithically across all data uses however different they may be in terms of risk, use, content and so on. The GAO does not explain why a particular set of principles was chose and as previously stated, we believe that the GAO's methodology by which the OECD principles was applied is flawed.

Third, as discussed above, there is an extraordinarily thorough record of congressional oversight of various industry sectors' uses of personal information. The U.S. has chosen a sector-specific structure to consumer data laws which ensures regulatory structures which are both appropriate to the data and which can be effectively enforced. Sector-specific laws and regulations exist today because of such oversight and due to the expertise of different committees overseeing different aspects of American business. The GAO, by implication and likely unintentionally, implies to the reader that all such oversight was incomplete and that a single evaluative standard is the right approach to analyzing our members business models and products. This, however, is a very fundamental flaw in the GAO's approach. Sector specific laws ensure that they are tailored to the industries, to the uses of data and to the risks involved. How healthcare data (i.e., HIPAA) is regulated is inevitably different than how one might regulate a telephone number (i.e., Do Not Call). Ultimately, tailored laws and regulations ensure that consumers are protected, but also are empowered by the data about them.

Fourth, the GAO's one-size-fits-all approach to applying the OECD guidelines ignores a fundamental bifurcation that exists with regard to information use and that is the difference between consumer data products used for eligibility determinations

and those which are not. A fraud prevention product, for example does not end a transaction, but provides a user with a "caution flag" which encourages the user to take additional steps to further authenticate a person's identity. As discussed above, where data is provided by our members for eligibility determinations such as employment or credit, the FCRA already provides a robust set of rights and protections for consumers. Regulation of consumer data where it is used for eligibility determinations is different than regulating consumer data used for fraud prevention or investigative location tool used by law enforcement. By not accounting for this essential bifurcation in uses, application of the OECD guidelines leaves readers with the wrong impression about how good data protection laws should operate.

Fifth, the GAO does not properly account for the system of public records which exists in our country and which has been considered a key pillar in the success of our democracy. Unlike other nations, our government cannot withhold information about us from us. Governmental transparency is achieved through open records and freedom of information acts at the state and federal levels. The application of many aspects of any one of a number of principles works against a system that has been in place since the early days of our country's existence. The GAO's report does readers a disservice by not discussing the unique nature of public records and by attempting to apply the OECD guidelines to this system of records.

To amplify on our general concern about the GAO's approach to applying OECD guidelines, let's now consider some specific illustrative examples.

Consumer Consent

The report states that "[r]esellers generally do not adhere to the principle that, where appropriate, information should be collected with the knowledge and consent of the individual."[14] The reader is left with the wrong impression regarding the practices of our members, the laws which currently regulate them and the appropriate application of a consent standard. For example, the GAO does not attempt to apply a consent-based standard on a product specific basis or even a business-model-specific basis, which is an inherent flaw in their methodology. If one were to apply such a standard to, for example, consumer credit reports, then the result would be to give consumers the ability to pick and choose which creditors' data would be reported to a credit bureau. Consumers could allow creditors they intend to pay on time to report and could prohibit from reporting those that they don't intend to pay on time or at all. The result would be to turn the nation's credit reporting system on its head and to affect the fundamental safety and soundness principle upon which our banking system has operated since the days of the great depression. In 1970, Congress recognized the inapplicability of this fair information practices concept since it would essentially work against the fundamental premise of data acting as an independent affirmation of a consumer's own willingness to pay, or otherwise qualify for a benefit. In a second example, of what value would an identity verification tool be if consumers who intend to commit fraud can decide which data will or won't be used? A third example involves public records. How does one apply a consent standard to records which are in the public domain? Through these examples, it is clear that consent is not a universal concept which can be applied to all data flows.

Data Quality

The title of the data quality discussion is "Information Resellers Do Not Ensure the Accuracy of Personal Information They Provide." This is misleading. As discussed above, CDIA's members are committed to the quality of information they collect. Further, in all cases where the data is used to produce a consumer report used for an eligibility decision, the standard for accuracy is found in the FCRA.[15] It is a standard that has been in place since 1970 (and amended extensively in both 1996 and again in 2003) and which applies to eligibility decisions such as applications for insurance, employment, government entitlements or credit. The GAO report does not properly acknowledge this fact or the breadth of the application of FCRA to consumer data transactions involving consumer reporting agencies. However, applying an accuracy standard to an investigative product used to locate individuals makes little sense. These location services are predicated on possible connections between addresses, names, etc., which are then followed up with direct contacts by law enforcement agents or collection agencies, for example. Location services are certainly high quality services and often are very precise, but since these products are not

[14] Page 44, Draft Report.

[15] The standard of accuracy in FCRA can be found at Sec. 607(a). A consumer reporting agency must use reasonable procedures to assure the maximum possible accuracy of the information in the report.

used to make an eligibility determination (e.g., job, credit) they are not regulated in the same way. This said, the quotes drawn included in this testimony regarding the high quality of consumer data products purchased by law enforcement or counterterrorism agencies (81% of users according to the GAO) speak for themselves. Like consumer consent, the concept of data quality cannot be applied in the same manner to each consumer data product as is implied by the GAO's methodology.

Use Limitations

The GAO report states that "[r]esellers do not generally limit the use of information beyond those limitations required by law." It is not clear what the GAO intends by this, but in fact both Title V of GLB and Section 604 of the FCRA do, for example, impose significant limitations on the use of nonpublic personal information and consumer reports respectively. The GAO's report does not acknowledge these use limitations in the context of their discussion. Further the GAO does not state that use limitations cannot apply to public records which are not gathered for purposes under the FCRA since such records are generally available to the general public directly from Federal, state and local agencies and courts. This said, the Drivers Privacy Protection Act does impose use limitations on records coming from state motor vehicle agencies. The draft report also states that "[w]ithout limiting use to predefined purposes, resellers cannot provide individuals with assurance that their information will only be accessed and used for identified purposes." This criticism of the system of laws and contract is without basis. We have discussed the extent of the laws which impose a variety of use limitations and as evidenced by the GLB's service provider requirements (in effect since 2001), HIPAA's business associate requirements (in effect since 2003), and the concept of using contracts to limit use is an entirely appropriate system for consumer data companies. In fact many laws which restrict uses of information, also require that certifications through contracts be obtained.

Access and Correction

CDIA's members when operating as consumer reporting agencies provide full access and a right of correction for all consumer reports. Consumer reports are used for eligibility determinations and thus our members fully agree with the application of this principle. However the application of an access and correction principle applied to a fraud prevention and location data base would result in empowering criminals to delete information that is used for pattern analysis and other analytics which help in linking suspects or key pieces of information necessary to stop fraud or to solve a case. The GAO's report does not properly describe the harmful application of an access and correction regime to location, investigative and fraud prevention systems which are not used to stop a transaction or prevent a consumer's access to a service or benefit (eligibility). In fact FTC Chairman Majoras stated in a letter responding to questions about the imposition of an access and correction obligation on information resellers:

> *"Before extending this approach to additional databases [beyond FCRA], however, it is necessary to consider carefully the impact of such extension. For example, requiring data merchants to provide consumers with access to sensitive information may itself present a significant security issue—in some cases it may be difficult for the data merchant to verify the identity of someone who claims to be a particular consumer demanding to see his or her file. Similarly, for databases that are used to prevent fraud or other criminal activities, providing correction rights could pose serious problems; those trying to perpetrate the fraud may take advantage of the right to 'correct' data to hide it from those they are trying to defraud."*

The GAO report states in its conclusion that "[g]iven that reseller data may be used for many purposes that could affect an individuals livelihood and rights, ensuring that individuals have an appropriate degree of control or influence over the way in which their personal information is obtained and used—as envisioned by the Fair Information Principles—is critical." For all of the reasons discussed above, the GAO has failed to support this claim because:

- Their analysis does not properly account for the severe regulation of consumer reporting agencies, and the breadth of the FCRA's application to all eligibility transactions which apply to all governmental transactions and uses.
- In taking a one-size-fits-all approach, the analysis does not properly account for the destructive consequences of applying various principles in the same way to all business models and product which make up the consumer data industry.

- In making this claim, the GAO often ignores or undercuts decades of congressional oversight, legislative enactments (FCRA, GLB, HIPAA, DPPA, etc.), federal regulatory activities and law enforcement actions.

CONCLUSION

In conclusion, the members of the CDIA believe that the GAO's report is methodologically flawed and often misleads readers through the attempt to apply a once-size-fits-all analysis of a set of privacy guidelines. The consumer data industry does not consist of a single entity called an "information reseller." It is an industry with a diversity of business models focused on the production of consumer reports, fraud prevention tools, location and investigative products, analytics services and more. CDIA's members create incredible value for the government agencies which use their services. The consumer data industry is a significantly regulated industry through sector-specific laws which tailor the component information use principles to the types of data, risks and uses involved. Our nation remains at the forefront of enacting enforceable laws and regulations with which our members commit themselves to complying each and every day.

We appreciate this opportunity to testify and we welcome your questions.

Mr. CANNON. Thank you, Mr. Pratt. We appreciate your testimony.

Now the gentleman from Ohio is recognized for 5 minutes.

Mr. CHABOT. Thank you very much, Mr. Chairman.

Ms. Cooney, I will begin with you, if I can. Would you elaborate on why privacy impact assessments are important, what they are good for, and how you have seen them work in action?

Ms. COONEY. Certainly, I would be happy to. At the Department of Homeland Security it has been a very important tool, on the front end of any mission program that uses an information system to collect personal information, to really determine on the front end why are we collecting the information, what information do we really need, how long will we keep it, how accurate is the information from the sources that we are taking it in from, how will we handle it, how do we plan to share it internally or with other Federal agencies or even State and local first responders, and what are the possible redress mechanisms?

So with a mission as critical as ours is to protect the homeland and security of the American people, we believe that it is also very critical that at each step, from the very beginning of a program through the entire lifecycle development of the technologies that we use to collect and store information, that we look critically at what we are doing and use some basic planning as we do those programs. To us, like in the private sector, it is important information management and it is good ethical Government behavior.

We have met with cooperation, really, throughout the Department in making that operationalized across business lines and it has been a very satisfactory experience.

Mr. CHABOT. Thank you very much.

Ms. Koontz, let me turn to you, if I can. What did the GAO find in terms of the security of personnel information in the GAO report? I know that you have already talked about it to some degree, but could you elaborate a little on that?

Ms. KOONTZ. Sure. We found that the four Federal agencies that we reviewed had put security protections in place to deal with reseller information. For example, all four of them told us that they had instituted passwords and other access controls to make sure that there wasn't unauthorized access to reseller information. Some of the agencies also had restricted access to very sensitive reseller

information only to those personnel who have a need to use that kind of thing.

Some of the law enforcement agencies as well use something known as cloaked logging. That is a procedure that actually masks the searches that law enforcement personnel do against reseller data so that even the vendor doesn't know what kind of searchers are being done. And this is a way of protecting the integrity of the investigations and making sure that subjects of investigations cannot be tipped off as to the existence of them.

That being said, I think Federal agencies realize that the security is an important component. We did not do a test of security controls at the four agencies we reviewed so we can't make an assessment of the efficacy of the controls that they have in place. And work that we have done Government-wide on security indicates that we found security weaknesses in almost every area in the 24 major agencies, including the four agencies that we reviewed.

Mr. CHABOT. Thank you very much.

Mr. Swire, do the same security concerns exist with Federal Government's maintenance of personal information as exist among commercial data companies?

Mr. SWIRE. Well, many of the challenges are the same. The Government uses overwhelmingly commercial software now, and they are using platforms and vendors that are very, very similar.

The Federal Government has some special challenges, though. There are classified systems for some systems, and that is a much harder standard to live up to. And also the Government probably has lagged, despite FISMA and GISRA and these security statutes, it has probably lagged the private-sector best practices. It has been hard sometimes to get the personnel in place, it has been hard to get the resources. So it has been a very big challenge and the scorecards haven't always been satisfactory.

Mr. CHABOT. Thank you.

And finally, Mr. Pratt, I would like to turn to you. What security policies are in place to ensure that citizens' information is not easily accessible by identity thieves or computer hackers?

Mr. PRATT. Well, I think the best baseline that we can see in guidance and law and regulation would be those that we find in the safeguards rules under Gramm-Leach-Bliley Act, which apply not—really are applied across the board in many of our member companies today. So that includes technical safeguards, strategies that you would use simplistically—firewalls, if you have online or offline systems. It includes employee training, it includes employee background screening, it includes the types of strategies discussed by the GAO in terms of, you know, password access, how quickly passwords are changed and cycled through, for example.

It includes even physical safeguards—who has access to a data center, who can in fact get in and potentially walk out with a hard drive that might contain sensitive personal information.

So when you have the technical, the physical, as well as the employee-based safeguards, you have, really, three legs of a key stool which we need to ensure is applied to really all kinds of sensitive personal information.

Mr. CHABOT. Thank you very much. My time has expired, Mr. Chairman.

Mr. CANNON. The gentleman yields back.

Mr. Nadler. The gentleman from New York, the Ranking Member of the Constitution Subcommittee, is recognized for 5 minutes.

Mr. NADLER. Thank you, Mr. Chairman.

I would like to ask all the panelists, given the importance of privacy impact assessments, as Ms. Cooney stated, do you support a broader requirement that agencies prepare privacy impact assessments for rules involving the collection of personally identifiable information in all Government agencies?

Start with Ms. Cooney, then everybody else.

Ms. COONEY. Thank you. I would say that certainly under Security 222 of the Homeland Security Act we read the requirement by Congress to really require DHS to undertake those types of privacy——

Mr. NADLER. No, no, clearly my question is do you think that Congress should extend that to other agencies?

Ms. COONEY. We found it helpful at DHS. I am not sure what the Administration view is, but I can tell you from our experience it has been a very helpful process.

Mr. NADLER. So you would think it a good idea to extend it to other agencies?

Ms. COONEY. It may be.

Mr. NADLER. Okay. Ms. Koontz?

Ms. KOONTZ. What we found in our work is that the privacy impact assessments were not being done consistently from agency to agency. And that was something that concerned us very much. And as Ms. Cooney said very articulately, the privacy impact assessments are a very powerful tool before you start building an information system, before you start collecting information, in order to assess what the privacy implications are and then to put the controls in place up front. And to the extent that they are made publicly available, I think they contributed to——

Mr. NADLER. Are you suggesting—this is for new rules. Is it your suggestion that we need better enforcement of them?

Ms. KOONTZ. I think we need better implementation of the existing requirements and I think that we saw that what Homeland Security put in their guidance to be a model that could be expanded to other agencies.

Mr. NADLER. Thank you.

Professor Swire?

Mr. SWIRE. I do support broadening the PIA's application to rules. I think we have used that they are a useful tool. There is an issue about scope. You don't want to have it for things that only have a tangential relationship to a couple of people's data. But in terms of enforcement, I think that goes back to having OMB or the White House have a privacy office to make sure agencies aren't falling down on the job. So you spread it to the rules and then you have some coordination across agencies.

Mr. NADLER. Thank you.

Mr. Pratt?

Mr. PRATT. I think from our perspective, really, you have at DHS a good model for how an agency should oversee the uses of private-sector information as well as data that would be gathered under the aegis of the public agency. So to the extent that you are sug-

gesting other agencies that may use sensitive personal information might need a similar infrastructure of knowledgeable and highly trained individuals, that makes sense to us. Certainly in the private sector we have chief information privacy officers, we have the same types of reviews in the financial services industry that go on with regard to how information is used and protected and so on. So I don't think that we ever have a problem with agencies understanding how to protect and secure and use responsibly information they obtain.

Mr. NADLER. I thank you.

Professor, do you think we could benefit from agency privacy ombudsmen in other parts of the Government?

Mr. SWIRE. Well, there have been efforts to spread it. I think there may be up to three or four different executive orders or executive statements that say agencies are supposed to have privacy offices, but implementation has really been uneven over time.

So there are a number of agencies that haven't been nearly as institutionalized as Homeland Security and haven't been as systematic in——

Mr. NADLER. See, so again, as in your answer to the previous question, if we had an office in the White House or somewhere to make sure that all the agencies were complying with privacy impact statements or with having the ombudsman function properly, or the agency offices, whatever we want to call them, function properly.

Mr. SWIRE. I can offer some perspective from having been in that seat. It gives you one person to criticize by name. And that has a very powerful effect, seeing your name in the newspaper as a bad guy, and it leads you to try to get other people to cooperate and make it all work a little bit better.

Mr. NADLER. It gives you a motive.

Mr. SWIRE. Yeah.

Mr. NADLER. Thank you.

Again, Professor Swire, to the extent that data processing operations might move overseas, what protections do we have or ought we have that we don't have to extend our protections for that eventuality?

Mr. SWIRE. Well, this issue of overseas has been a powerful issue that people are looking at. I must say, I have a slightly different perspective because the United States complained very much when Europe tried to do that to us. And Europe had in a privacy directive rules that they wouldn't let data go to the United States, and we wanted to make sure that American companies could use that data responsibly.

I am a step more cautious. I think it is always good to have the contractors under very good controls and make sure those controls work. I am not personally as sure that we should make a big line about overseas or not.

Mr. NADLER. Could I just ask if anybody else would want to comment on that question? Ms. Cooney?

Ms. COONEY. Thank you, Mr. Nadler. I would like to tell you that there is work presently going on that the Federal Government is very involved in, and we are included in that work in the DHS Privacy Office, both in the Organization for Economic Cooperation and

Development and in the APEC forum in working on cross-border enforcement on privacy issues. There has been some work already accomplished in certain areas, such as combatting spam, and that has been fairly effective.

What we have found so far is that it is not done solely by privacy practitioners or privacy enforcement officers, but it might be done by consumer protection folks in certain areas, criminal law enforcement in others, privacy professionals working together.

So I would want you to know that that is an active part of the agenda that we are working on as Federal partners in that.

Mr. NADLER. Thank you. Anybody else?

Thank you, Mr. Chairman.

Mr. CANNON. The gentleman yields back.

Mr. Franks, the gentleman from Arizona, is recognized for 5 minutes.

Mr. FRANKS. Well, Thank you, Mr. Chairman.

I want to direct this to anyone at the—in fact, I would like, maybe, for everyone to take a shot at it. I am wondering, in terms of what really are the challenges that we face to keep people's data secret and accurate, is it more of a policy issue that needs to be changed here from Congress, or is it more of a mechanical issue of just the reality that, with the expansion of computer technology and all of the different things that happen today, is it more of a technology challenge or is it more of a policy challenge?

Mr. PRATT. I will take a first stab at this. First of all, I do think that in this country we need to protect, under the rule of law, sensitive personal information no matter who gathers it. Some of the different laws that we have discussed in our testimony, which are also accounted for in the GAO report, do deal with sectors of business in this country where we have to secure and protect that information. The Gramm-Leach-Bliley Act information safeguards rules are a good example.

Certainly our membership has testified before several different Committees saying that information safeguards standards should apply to anybody who is going to gather sensitive personal information such as my name and my address and my Social Security number in that combination.

I think there are several effects to that, by the way. First of all, fewer folks will gather that information. They will think about it first. And that is good, because they should. And if they are going to gather it, they should protect it under that three-legged stool we have discussed. And I think in doing so, it does create an enforcement mechanism also, where there is failure in the marketplace. We think those are all good outcomes that could result from the enactment of law that would do that. There are several Committees that are focused on that now that I think would move forward with an effective program for protecting sensitive personal information.

It is also education, though. And I would say within the last 5 years, certainly the last decade, what we know and think about as information security is very different than it was 10 years ago. And certainly the velocity of change with technology makes it very challenging.

Mr. SWIRE. I think it is very much a policy issue where the hard things come in. There is a lot of consensus on data security. You

can get pretty much everyone to agree on the list. But which data is the right data to use? And this IRS example from my testimony is one example. Should your tax preparation agency be able to resell your data or not? They can have perfect security, it is just a question of whether that company should be reselling it or not. That is a policy decision. That is where I think a lot of the work has to happen.

Mr. FRANKS. Ms. Cooney?

Ms. COONEY. Thank you. I think the point that I would like to make is that the process of data security and information security practices is not one-size-fits-all and it is not a one-step process. It is an iterative process. I think Mr. Pratt's reference to the GLBA safeguards rule is very important and that those general guidelines can be used across Government systems as well as in the private sector, keeping in mind, as they require it, that it is an iterative process and you need to keep looking at your process both from a technology standpoint, from a personnel standpoint, and from a policy standpoint in terms of why do you need to keep this data and is it the right data to keep.

On the accuracy issues, and it somewhat answers your question, in terms of the application of the Fair Information Practices principles to data accuracy in the private sector for commercial resellers, whether all those principles should apply or would easily apply is something that could be discussed. But certainly a focus on allowing individuals some access to their information to correct the information really should be looked at, because originally that information would have been collected for very different purposes. Many citizens may not even know that a data aggregator has their information. And it is a matter of fairness as well as carefulness with the information.

Mr. FRANKS. So just to expand on your thought there, much like the credit data that we access, you are convinced that something along those lines for generalized data, that the consumer would always have the right to ascertain what that was, or at least in nonsecurity issues?

Ms. COONEY. Right. In many circumstances, when it doesn't touch law enforcement or national security in particular, although even in our case we need to be very concerned on our end in the Federal Government to check on data accuracy.

Mr. FRANKS. My time is almost gone. Mr. Pratt, let me skip quickly to you, sir. With the proliferation of ID theft, a lot of times you can identify a particular culprit. Is this escape of data happening mostly in Government databases or is it private databases? Is there any one—is it just generalized or is there some kind of particular area where we are hemorrhaging?

Mr. PRATT. It is difficult to pin it down. Certainly, for example, it could be as simple as somebody driving down the street at the right time of the month to pick up your mail, so you have something as simple as mailbox fraud. We saw last year about 50 percent of all the media coverage focused on universities that were losing sensitive personal information, I think probably because they were at that time using Social Security numbers as student ID. I think a lot of universities have begun to change that practice.

So no, sir, I don't think there is any one place you can go.

To your point, by the way, about the Fair Credit Reporting Act and having access, let me just say it this way. The Fair Credit Reporting Act is a terrible title for the law because, in fact, the law applies to any kind of eligibility decision. So any time data is used to deny me something, I can't get it, I have a right of access. I have a right to correct it. I have a right to expect that it was accurate in the first place. I have private rights to enforce, I expect the Federal Trade Commission to enforce, State attorneys general to enforce.

So I think it is very important. That was one of the issues we had with the way the report was structured, is you might walk away from that thinking that there was not this very, very broad-based law that said whether it is my employment application, my application to purchase a home, my application to get a cellular phone account, my application to obtain a utility—no matter how and where a consumer report is used, not a credit report but a consumer report—I have all of those rights that we have just begun to discuss. So I do think we have a law on the books that is quite a bit broader than maybe the title would imply.

Mr. FRANKS. Thank you.

Thank you, Mr. Chairman.

Mr. CANNON. The gentleman yields back.

Mr. Scott.

Mr. SCOTT. Thank you, Mr. Chairman.

I guess my first question is a little more basic. Who are we talking about? Who are these resellers?

Ms. KOONTZ. I assume you mean the names of the companies?

Mr. SCOTT. Well, if you want to leave the names out, just describe them.

Ms. KOONTZ. For our study, we defined information resellers as being businesses that collect and aggregate information, personal information about individuals and make them available to consumers. So it is rather broad.

Mr. SCOTT. To consumers or to businesses?

Ms. KOONTZ. And to businesses, yes. To their customers.

Mr. SCOTT. The purpose for which you are gathering the data can vary depending on what it is going to be used for. You could be just compiling a mailing list. Is that what you are talking about?

Ms. KOONTZ. I think we are talking about information resellers who then collect this information and then they convert it into information products, some of which are used for marketing, some of which are used for other purposes.

Mr. SCOTT. Well, if you are using it for marketing you can get a list that would be interested—where a certain product would be interested in marketing to that group of people.

Ms. KOONTZ. Mm-hm.

Mr. SCOTT. Could be 80 percent accurate, but that is good enough for mass mailing. Because it is better than kind of saturation mailing. You knocked off 75 percent of the people you don't want to mail to. Are we talking about that, too?

Ms. KOONTZ. Well, that is some of it. Some of it is for marketing purposes. But I think you have hit on a key point that we talked about in our report, is that the privacy principles basically talk about accuracy for a specific purpose. And the specific purpose in

this case is often determined by the user. So it is difficult for the reseller to assure the degree of accuracy for a particular purpose because they are not the ones that are determining that purpose.

Mr. SCOTT. Well, you don't care whether it is accurate or not if all they are going to do is just mass mail. If the Government gets hold of it, it is going to take some adverse action based on this kind of superficial dragnet where you come in and gather up a lot of names, most of which would be in the category you are aiming at, where the person gathering the data didn't have any interest in accuracy. So what do you do in that case? Is that the information we are talking about?

Ms. KOONTZ. That is part of the information that we are talking about. There are all kinds of information products that are offered by resellers. And I think it does put more of a, shall we say, an obligation, too. In this case we are talking about the use of these data products by Federal agencies and it puts, I think, an obligation on the part of the Federal agency to determine that the accuracy is appropriate for the use that they are using it for. Which is, for example, the reason that law enforcement corroborates this information with other sources before they take any action against an individual.

Mr. SCOTT. Is the information subject to the Freedom of Information?

Ms. KOONTZ. I don't know.

Mr. SWIRE. There is a privacy exception to the Freedom of Information Act and it often would prevent a Freedom of Information Act request from going through.

Mr. SCOTT. To get the whole list?

Mr. SWIRE. Yes.

Mr. SCOTT. If you are doing law enforcement activities, do I understand that the Levy Guidelines are no longer in effect, where you had to actually be investigating a crime before you started gathering information on people? Professor?

Mr. SWIRE. Yes, that is correct. They were changed very substantially after 9/11.

Mr. SCOTT. Before 9/11, before you started gathering information on people and setting up dossiers, you had to actually be investigating a crime, not just gathering information. Is that right?

Mr. SWIRE. There were detailed predicates for each stage as the investigation went further, yes.

Mr. SCOTT. And that is no longer in effect, so the Government is now just gathering information?

Mr. SWIRE. There are guidelines that Attorney General Ashcroft issued. I have read them, but I don't have them clearly in my head. They are quite a bit more permissive, because the idea is share data and use data more intensively.

Mr. SCOTT. Professor, did I understand you to say there is some idea that you could actually sell tax records?

Mr. SWIRE. Well, this was actually a subject of a public hearing today somewhere else in town. But H&R Block or any other tax preparer, under the proposed rule, would be allowed to sell tax records or databases of tax records for the first time to outside parties.

Mr. SCOTT. That is records that they prepared?

Mr. SWIRE. That they prepared for you as the taxpayer. If you signed off, as one of your signatures to them, they would then be able to resell that.

It got quite a press hit a couple of weeks ago, when people found out about it. And deserves to.

Mr. SCOTT. Thank you, Mr. Chairman.

Mr. CANNON. The gentleman yields back.

Ms. Wasserman Schultz, did you have questions?

Good. Thank you. The Ranking Member is recognized for 5 minutes. Mr. Watt?

Mr. WATT. Thank you, Mr. Chairman.

Ms. Koontz, I know you all did the study and you are not doing policy, but I particularly wanted to hear from you and Mr. Pratt about whether you thought that Professor Swire's suggestion that we reinstitute a privacy officer in the White House that has kind of umbrella authority from agency to agency, whether you think that is a good idea, whether there are particular good pros to doing that or particular bad cons to doing that.

I will ask that question of you, if you can address it from a policy perspective. And I would like to get Mr. Pratt's view on it, too.

Ms. KOONTZ. We haven't studied the question of the need for a privacy officer in OMB or in the Executive Office of the President. I can see, though, that the idea probably has some merit, in terms of further discussion, as a way of having a focal point for privacy issues and the Federal Government. I mean, I think we have seen some benefits from, for example, within the Department of Homeland Security, where you have a highly placed official who has a broad privacy responsibility, and that seems to be something that is useful in terms of looking at these policy issues.

Mr. WATT. Mr. Pratt?

Mr. PRATT. Our association hasn't actually studied that same question any more—so I suspect—than the GAO. My first reaction is that sometimes centralization can be a red flag, because you start to remove the expertise and the knowledge you might need. So the knowledge you might need in HHS might be different than the knowledge you might need in DHS.

So I don't know if a—just off the top of my head, I don't know if a central office would make things better or if it is just simply important to make sure that there are knowledgeable professionals who are thinking about data use issues on an agency-by-agency basis.

And of course Federal Trade Commission has established its new division, which does focus on information use and identity theft issues as well as——

Mr. WATT. Who is that? I am sorry.

Mr. PRATT. The Federal Trade Commission has established a new division under the Bureau of Consumer Protection, which focuses specifically on information protection and identity theft. So there is an office there that focuses on data flows in that regard.

Mr. WATT. Under what authority is it doing that, and is that——

Mr. PRATT. It is not the same principle. It isn't the same principle as an omnibus individual, if you will, at the level of the White House. They really oversee—their scope of authority would be no

broader than the FTC's scope of authority generally in the marketplace.

Mr. WATT. Do you concede that despite the concerns, the potential on the downside that maybe having a more consistent set of principles across the Government would be facilitated by this suggestion?

Mr. PRATT. I don't know yet because, again, one of the difficulties we have even had with the GAO report, and we certainly appreciate the hard work that the researchers did in putting it together, it demonstrates one of the difficulties, and that is we feel that the GAO took the principles and applied them too monolithically across something called an information reseller. And really, to Mr. Scott's question, I suppose information resellers are consumer reporting agencies. They may be financial institutions under the Gramm-Leach-Bliley Act, consumer reporting agencies under the Fair Credit Reporting Act. So I don't know if centralizing expertise works better than just simply making sure that you have knowledgeable individuals operating at an agency level.

Again, I think also I am probably not in the best position to discuss the effectiveness of the current operation of the Privacy Act or the OMB guidelines that implement that. It is probably the domain of Professor Swire.

Mr. WATT. Professor Swire, there was a lot of debate about, when this Privacy and Civil Liberties Oversight Board was set up, about whether it should have subpoena power. I know that the Agency just got structured in February—I mean the people who were appointed. But can you just give us kind of the pros and cons of—or maybe better, even, what are the real problems with not having subpoena power?

Mr. SWIRE. Well, there are various jobs the Privacy and Civil Liberties Board could do. One of them is to be inside the executive branch during clearance, when they are trying to figure out how do you do a new program. And I don't think subpoena power is needed for that. That is talking to the people, being in the room, building confidence that the board can help.

When it comes to finding out if there are problems out there in the agencies, there is a question of how you find that out. One way is to go to the IGs, right. We have Inspectors General, and especially if we have some good whistleblower protections so the people are allowed to talk to the IGs, then that may be one way to do the investigation.

If you think that is not working, then you look around, who else might do it? It could be the Department of Justice, but you have to have a good step toward a criminal investigation. If you don't have that, then maybe somebody else, like this board, with subpoena power might be your best chance to find problems in the agencies and do something about it.

It really has to do with whether the IG system is working, because they were supposed to be the ones to subpoena, and whether you need a second look with some expertise.

Mr. WATT. Can I just ask one more question, Mr. Chairman?

Ms. Cooney, how is your office going to coordinate with this Privacy and Civil Liberties Oversight Board? How do you see these

two things meshing together, Homeland Security and this oversight board?

Ms. COONEY. Sure. Under the oversight board there actually is a Privacy and Civil Liberties Officer for the DNI. We coordinate with that Privacy and Civil Liberties Officer now, Alex Joel, in a very cooperative way. As he is setting up his operation, he has come to DHS to ask us what our experience has been, for advice on the startup. And we are working very closely right now, along with others, including the new Privacy and Civil Liberties Officer and DOJ and others, on building in a privacy architecture for the information sharing environment across the Federal Government.

So I think it is going to be a very collaborative process and it has been very positive so far.

Mr. WATT. Thank you, Mr. Chairman.

Mr. CANNON. I would like, before I ask a couple of questions here, I would like to thank the panel for being here today. It think this report is very, very helpful, Ms. Koontz, and you have done a remarkable job in helping us to understand it.

Ms. Cooney, we appreciate what you have done. Can I just ask, are you coordinating with the people at Justice that are setting up the same process that you are doing? Could you comment on that briefly?

Ms. COONEY. Yes, we are. Actually, before the appointment of the Privacy and Civil Liberties Officer there, we worked, really, for several months before that in providing advice in terms of our experience, our budget, the type of personnel that we have hired, which is quite multi-disciplinary. And as Mr. Pratt noted, it takes expertise along a wide range of areas. We have technology experts, we have policy experts, we coordinate closely with our Office of the General Counsel on legal issues. And I am very proud to say we have a Chief Counsel to the Privacy Office, who is embedded with us, reporting to our General Counsel, so that is very cooperative.

We have a compliance team that has a private-sector background. We have folks who had enforcement and compliance experience in the Government realm. We have international. All of those things are really needed if your agency does work across a wide scope and has a lot of different dynamic programs.

We have shared that type of information with the Department of Justice. And since Jane Horvath has joined the Department of Justice, we have met several times, e-mail, talk about issues. And I think that is the way it should be, and we are happy to do that.

Mr. CANNON. Well, I—you know, if you look at DHS, which is hard to do because it is so big—it takes the Almighty to comprehend it, and I am not sure it would take the Almighty, but it is beyond my capacity to understand the Department of Justice. It seems to me that the idea, and I guess it goes to your comment, Mr. Pratt, that having a decentralized process may be helpful.

But Professor Swire, we appreciate your comments and look forward to working with you on what a of a—how we would sort of oversee this whole process. I think it is vitally important that we take these huge, monstrous organizations and get them thinking about what they do, and then cumulate activity rather than mandating it. But at some point, you have to have some kind of overarching oversight of that. So we will revisit that.

Mr. Pratt, can I ask a couple of questions of you? The GAO has reported that information resellers generally allow individuals limited access to correct their personal information. Why can't individuals get data about themselves corrected when it is wrong? And if the consumer reporting agencies are able to accommodate such corrections, as they are required by the Fair Credit Reporting Act, why can't information resellers do likewise?

Mr. PRATT. Really, it depends. Again, it is just taking that Fair Information Practice, and then we have to walk through the various products that it might apply to. So as you say, consumer reports, absolutely. Those reports are used to deny me access to a benefit or service. And that is one of the basic fair information principles we are working off of. If I can't get something because information has told the user that I should not get the credit, I should not drive off the car lot with the car, then that makes sense to us and we understand that.

A fraud prevention product is another type of data product that is used. A fraud prevention product, were we to disclose it, would mean we are disclosing the recipe, because we would be disclosing the various data elements which are cross-matched which raise a yellow flag.

Now, a fraud prevention product doesn't deny me access, but it probably slows me down. Somebody is going to ask me more questions. You know, Congressman Cannon, are you really who you say you are; can I have another item of identification from you to make sure that you are who you say you are.

And I think that is also true of some of the investigative tools that we have, location tools. In other words, a location tool really just—and I have seen some about me, where it will show where I have lived previously. And so it is not really—it just says you lived in Houston, Texas, for a period of time, one of your friends now lives in Los Angeles. It really just shows an investigator how they might candidly conduct a national security investigation were I applying for a national security level of clearance. So that is a different kind of tool.

So accuracy and how you apply accuracy really pivots, I think, off of that.

In terms of correction, though, public records are a particular challenge. Because if you have a court record and you have simply taken that same image data and put it into a national database, the real key to correcting that is to make sure the consumer knows how to get back to the court in order to correct the information in the first place. Because if you don't correct it at the courthouse, it is still publicly available, there are is still a Web site from which you can obtain it, and in fact all you have done is fix the intermediate source.

And by the way, that principle was corrected in the Fair Credit Reporting Act to ensure that a reseller in the context of a consumer reporting agency, where access and correction do apply, that the consumer would be referred back to the data source in order to correct it at the source rather than to try to correct it at the mid level.

Mr. CANNON. Let me just get one more question before my time expires.

When a data breach occurs, shouldn't an information reseller be required to notify those whose information was compromised? And if so, how should notification take place? What follow-ups, if any, should be required of information resellers to monitor compromised information?

Mr. PRATT. Well, I don't know that we think about it in terms of information resellers. There are several different bills that have been worked on by various Committees, and the fundamental question is, when you have a certain type of information that we tend to think of as sensitive personal information—If I have secured it in the first place, of course, I have done the right thing. If for some reason my security protocols have failed, yes, we think that there is a risk of identity theft, a significant risk of identity theft. Absolutely.

The reason we make that distinction, Mr. Chairman, is because there are cases where a laptop is stolen, but when you do the forensics on the laptop, you determine that it was really stolen in order to just simply fence the laptop. And in fact it was never opened, it was never started back up again, nobody ever looked at the data, the hard drive wasn't tampered with. So notifying a thousand consumers that their data was on a hard drive of a laptop that was stolen that was never dealt with from a technology perspective probably creates false positives which move consumers away from really being proactive.

So we think the key to good notices is the trigger—when should I do it so that you and I as consumers really can act on other rights that we should have.

Mr. CANNON. Of course the question does occur, who makes that judgment?

Mr. PRATT. It is a difficult one, yes, sir.

Mr. CANNON. Thank you.

We appreciate your being here today. Since we don't have, I don't think, any further questions, we will now stand adjourned.

[Whereupon, at 1:21 p.m., the Subcommittees adjourned.]

APPENDIX

Material Submitted for the Hearing Record

ADDITIONAL MATERIAL FOR THE RECORD SUBMITTED BY LINDA D. KOONTZ, DIRECTOR, INFORMATION MANAGEMENT ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

United States Government Accountability Office

GAO

Report to Congressional Committees

April 2006

PERSONAL INFORMATION

Agency and Reseller Adherence to Key Privacy Principles

GAO

Accountability * Integrity * Reliability

GAO-06-421

April 2006

GAO
Accountability•Integrity•Reliability

Highlights

Highlights of GAO-06-421, a report to congressional committees

PERSONAL INFORMATION

Agency and Reseller Adherence to Key Privacy Principles

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.

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

What GAO Found

In fiscal year 2005, the Departments of Justice, Homeland Security, and State and the Social Security Administration reported that they used personal information obtained from resellers for a variety of purposes. 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	4
Background	7
Using Governmentwide Contracts, Federal Agencies Obtain Personal Information from Information Resellers for a Variety of Purposes	19
Resellers Take Steps to Protect Privacy, but These Measures Are Not Fully Consistent with the Fair Information Practices	37
Agencies Lack Policies on Use of Reseller Data, and Practices Do Not Consistently Reflect the Fair Information Practices	49
Conclusions	62
Matter for Congressional Consideration	63
Recommendations for Executive Action	63
Agency Comments and Our Evaluation	64
Comments from Information Resellers	68

Appendixes

Appendix I:	**Objectives, Scope, and Methodology**	70
Appendix II:	**Federal Laws Affecting Information Resellers**	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
Appendix III:	**Comments from the Department of Justice**	79
Appendix IV:	**Comments from the Department of Homeland Security**	81
Appendix V:	**Comments from the Social Security Administration**	83
Appendix VI:	**Comments from the Department of State**	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.

United States Government Accountability Office
Washington, D.C. 20548

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.[1] 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,[2] which requires that the use of personal information be limited to predefined purposes and involve only information germane to those purposes.

The provisions of the Privacy Act are largely based on a set of principles for protecting the privacy and security of personal information, known as the Fair Information Practices, which were first proposed in 1973 by a U.S. government advisory committee.[3] These principles, now widely accepted, include

[1]For purposes of this 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.

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

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

- collection limitation,
- data quality,
- purpose specification,
- use limitation,
- security safeguards,
- openness,
- individual participation, and
- accountability.[4]

These principles, with some variation, are used by organizations to address privacy considerations in their business practices and are also the basis of privacy laws and related policies in many countries, including the United States, Germany, Sweden, Australia, New Zealand, and the European Union.

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

[4]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[5] and conducted site visits at three of them[6] 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.

[5]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.

[6]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[7] 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

[7]This figure may include uses that do not involve personal information. Except for instances where the reported use was primarily for legal research, agency officials were unable to separate the dollar values associated with use of personal information from uses for other purposes (e.g., LexisNexis and West provide news and legal research in addition to public records).

collection and use of personal and other information[5] 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

[5]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,[9] product warranty registrations, and

[9]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.

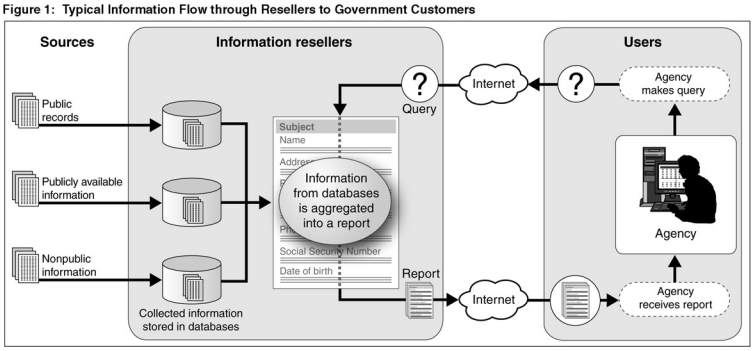
other application information provided to private businesses directly by consumers.

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.[10]

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.[11] 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

[10]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)).

[11]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,[12] 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

[12]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.[13] 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.[14] 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

[13]FISMA, Title III, E-Government Act of 2002, Pub. L. No. 107-347 (Dec. 17, 2002).

[14]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/infopolitech.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

Federal laws	Provisions
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[15] that require some form of notification upon a security breach.

[15]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.[16] A revised version of the Fair Information Practices, developed by the Organization for Economic Cooperation and Development (OECD)[17] 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.

[16]*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).

[17]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.[18] 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,[19] and including policy statements of the DHS, Justice, Housing and Urban Development, and Health and Human Services.[20] In 2004, the Chief Information Officers Council issued a coordinating draft of their Security and Privacy Profile for the Federal Enterprise Architecture[21] that links privacy protection with a set of acceptable privacy principles corresponding to the OECD's version of the Fair Information Practices.

[18]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).

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

[20]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 (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).

[21]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,[22] 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,[23] 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.[24] Justice accounted for most of the funding (about 63 percent).

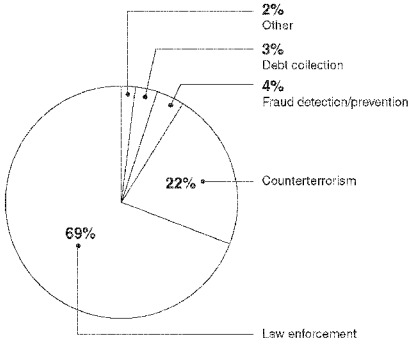
Approximately 91 percent of agency uses of reseller data were in the categories of law enforcement (69 percent) or counterterrorism (22 percent). Figure 2 details contract values categorized by their reported use. (Details on uses by each agency are given in the individual agency discussions.)

[22]H.R. 4127; introduced by Representative Clifford B. Stearns on October 25, 2005.

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

[24]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[25] offerings including a blanket purchase agreement[26] with ChoicePoint valued at approximately $15 million.[27] 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.[28]

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

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

[26]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.

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

[28]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,[29] 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.[30] 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.[31] Through these data, DEA agents can detect irregular prescription patterns for specific drugs and trace this information to the pharmacy and prescribing doctor.[32] DEA also uses an information reseller

[29]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).

[30]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.

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

[32]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.[33] 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.[34]

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

[33]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.

[34]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[a]	$11,248,000	*Public Source Information Program.* Find individuals and identify alias names, Social Security numbers, relatives, dates of birth, telephone numbers, vehicles, business affiliations, associations, and assets. The program provides FBI units with access to public record, legal, and news media information from various online commercial databases. *Criminal Investigative Division.* Same use. *Foreign Terrorist Tracking Task Force.* Obtain such information as names, addresses, telephone numbers, other biographical information, vehicle and boat registrations, and business ownership records.
Drug Enforcement Administration	ChoicePoint, LexisNexis, Dun & Bradstreet	$4,283,000	Conduct investigations of drug diversions and improper drug transactions: 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. Support criminal investigations of specific individuals and companies. Locate an individual's address in asset removal cases.
U.S. Marshals Service	ChoicePoint, LexisNexis, West	$1,661,000	Generate leads related to fugitive investigations (e.g., a fugitive's relatives and their contact information). *Asset Forfeiture Office.* Obtain information on preseized, seized, and forfeited property. 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. *Office of General Counsel.* Research assets to administer tort claims against the service. 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.
Executive Office for U.S. Attorneys	ChoicePoint, CBR Information Services	$855,000	*Financial Litigation Units.* 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.
Bureau of Alcohol, Tobacco, Firearms, and Explosives	ChoicePoint, Dun & Bradstreet, LexisNexis, West	$791,000	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.

(Continued From Previous Page)

Major component	Information resellers	Aggregate contract value	Uses involving personal information
Executive Office of the United States Trustees	ChoicePoint, Equifax,[b] 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	*Investigations Division.* 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	*Document Exploitation Division.* 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	*Office of Comptroller, Financial Management Division.* 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	*Civil Division.* 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. *Criminal Division, Office of Special Investigations.* 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. *Antitrust Division.* Locate witnesses for trials. *Tax Division.* 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.

[a]Seisint is now owned by LexisNexis.

[b]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."[35] 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.

[35]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	Acquire data (generally, address and vehicle information) for criminal investigations and background security checks. According to officials, information is either used to verify data already collected or is itself verified by investigators through other means. *Federal Protective Service.* Identify and locate potential criminal suspects using address, vehicle, and other information. *Office of Detention and Removal.* Locate and remove illegal aliens from the United States using address, vehicle, and other information.
U.S. Customs and Border Protection	ChoicePoint, LexisNexis, Dun & Bradstreet, and West	$2,375,000	Conduct queries on people, businesses, property, and corresponding links in support of law enforcement, intelligence gathering, and prosecution support. *Border Patrol Del Rio Sector.* Obtain information such as addresses, telephone numbers, and names of relatives in support of investigations involving registered owners of seized vehicles and property. *National Targeting Center.* Look up information associated with license plate data to assist in vehicle identification at northern and southern land borders. 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).
U.S. Citizenship and Immigration Services	ChoicePoint, LexisNexis, West	$960,000	*Offices of Fraud Detection and National Security and Asylum.* 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.
Transportation Security Administration	Acxiom, Insight America, Qsent[a]	$897,000	Test the feasibility of using commercial data sources to authenticate identity information contained in passenger records to support passenger prescreening. 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.

(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.

*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,[58] 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.

[58]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[a]	*Field Office Staff.* 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. *Office of Inspector General.* Access public records information to assist with investigations of fraud and abuse within the SSA programs. *Office of Hearings and Appeals.* Access public records information to locate the addresses of individuals.
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.[b]
Agencywide[c]	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[c]	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.

[a]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.

[b]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.

[c]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.

[d]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	*Criminal Investigations Division.* Obtain leads on addresses, locations, identity, etc., used in the conduct of criminal investigations of passport and visa fraud. *Diplomatic Security Command Center and Diplomatic Security agents at 26 overseas posts.* 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.[a]
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.

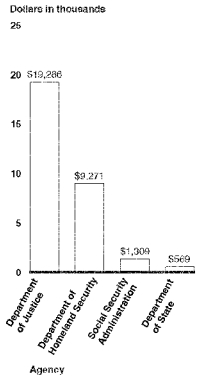
Note: The table represents fiscal year 2005 contract values and may not reflect actual expenditures. We did not verify the accuracy or completeness of the dollar figures provided to us.

[a]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.[37] FEDLINK, an intragovernmental revolving fund,[38] 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

[37]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.

[38]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[39] 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[40] 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

[39]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.

[40]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).[41] 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
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.	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.
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.	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.
Purpose specification. The purpose for the collection of personal information should be disclosed before collection and upon any change to that purpose, and its use should be limited to that purpose and compatible purposes.	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.

[41]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
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.	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.
Security safeguards. 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.
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.	Resellers generally inform the public of key aspects of privacy policies through Web sites, brochures, and so on.
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.	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.
Accountability. 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.[42]

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

[42]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.[43] 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.

[43]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[44] 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

[44]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.[45] 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.

[45]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
Collection limitation. The collection of personal information should be limited, should be obtained by lawful and fair means, and, where appropriate, with the knowledge or consent of the individual.	General	Agencies limited personal data collection to individuals under investigation or their associates.
Data quality. Personal information should be relevant to the purpose for which it is collected, and should be accurate, complete, and current as needed for that purpose.	General	Agencies corroborated information from resellers and did not take actions based exclusively on such information.
Purpose specification. The purpose for the collection of personal information should be disclosed before collection and upon any change to that purpose, and its use should be limited to that purpose and compatible purposes.	Uneven	Agency system of records notices did not generally reveal that agency systems could incorporate information from data resellers. Agencies also generally did not conduct privacy impact assessments for their systems or programs that involve use of reseller data.
Use limitation. Personal information should not be disclosed or otherwise used for other than a specified purpose without consent of the individual or legal authority.	General	Agencies generally limited their use of personal information to specific investigations (including law enforcement, counterterrorism, fraud detection, and debt collection).
Security safeguards. Personal information should be protected with reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification, or disclosure.	General	Agencies had security safeguards such as requiring passwords to access databases, basing access rights on need to know, and logging search activities (including "cloaked logging," which prevents the vendor from monitoring search content).

(Continued From Previous Page)

Principle	Agency application of principle	Agency practices
Openness. The public should be informed about privacy policies and practices, and individuals should have ready means of learning about the use of personal information.	Uneven	See *Purpose specification* above. Agencies did not have established policies specifically addressing the use of personal information obtained from resellers.
Individual participation. Individuals should have the following rights: to know about the collection of personal information, to access that information, to request correction, and to challenge the denial of those rights.	Uneven	See *Purpose specification* above. Because agencies generally did not disclose their collections of personal information from resellers, individuals were often unable to exercise these rights.
Accountability. Individuals controlling the collection or use of personal information should be accountable for taking steps to ensure the implementation of these principles.	Uneven	Agencies do not generally monitor usage of personal information from information resellers to hold users accountable for appropriate use; instead, they rely on users to be responsible for their behavior. For example, agencies may instruct users in their responsibilities to use personal information appropriately, have them sign statements of responsibility, and have them indicate what permissible purpose a given search fulfills.

Legend:

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

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

Source: GAO analysis of agency-supplied data.

Note: We did not independently assess the effectiveness of agency information security programs. Our assessment of overall agency application of the Fair Information Practices was based on the policies and management practices described by the Department State and SSA as a whole and by major components of Justice and DHS (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."[46] Regarding most law-enforcement and counterterrorism purposes, which accounted for 90 percent of usage in

[46]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.[47] 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.[48]

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

[47]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.

[48]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 informataion 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.[49]

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

[49]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.[50]

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.[51] 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.[52] For example, all four agencies cited the use of passwords to prevent unauthorized access to information

[50]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.

[51]5 U.S.C. § 552a(e)(10).

[52]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.[52]

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.[54] 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

[52]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.

[54]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.[55] 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.[56] 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,

[55]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.

[56]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."[57]

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.[58] 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

[57]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.

[58]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,[59] 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.[60] 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."[61] 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

[59]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).

[60]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.

[61]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[62] 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."[63] 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.[64] 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

[62]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."

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

[64]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."[85] 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

[85]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.

If you have any questions concerning this report, please call me at (202) 512-6240 or send E-mail to koontzl@gao.gov. Contact points for our 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

Linda D. Koontz
Director, Information Management Issues

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

Appendix I

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,[1] 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

[1]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.[2] 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

[2]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 polices 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.

Appendix III

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.

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.[1] 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

[1]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.

Appendix IV

Comments from the Department of Homeland Security

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

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 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

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

Appendix V

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,

Jo 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.

Appendix VI

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,

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). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

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

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

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Congressional Relations

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

Public Affairs

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

PRINTED ON RECYCLED PAPER