PRIVACY: THE USE OF COMMERCIAL INFORMATION RESELLERS BY FEDERAL AGENCIES

HEARING

BEFORE THE

SUBCOMMITTEE ON INFORMATION POLICY, CENSUS, AND NATIONAL ARCHIVES

OF THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

SECOND SESSION

MARCH 11, 2008

Serial No. 110–108

Printed for the use of the Committee on Oversight and Government Reform

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html
http://www.oversight.house.gov

U.S. GOVERNMENT PRINTING OFFICE

46–195 PDF WASHINGTON : 2009

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) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

HENRY A. WAXMAN, California, *Chairman*

EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts
BRIAN HIGGINS, New York
JOHN A. YARMUTH, Kentucky
BRUCE L. BRALEY, Iowa
ELEANOR HOLMES NORTON, District of Columbia
BETTY McCOLLUM, Minnesota
JIM COOPER, Tennessee
CHRIS VAN HOLLEN, Maryland
PAUL W. HODES, New Hampshire
CHRISTOPHER S. MURPHY, Connecticut
JOHN P. SARBANES, Maryland
PETER WELCH, Vermont

TOM DAVIS, Virginia
DAN BURTON, Indiana
CHRISTOPHER SHAYS, Connecticut
JOHN M. McHUGH, New York
JOHN L. MICA, Florida
MARK E. SOUDER, Indiana
TODD RUSSELL PLATTS, Pennsylvania
CHRIS CANNON, Utah
JOHN J. DUNCAN, Jr., Tennessee
MICHAEL R. TURNER, Ohio
DARRELL E. ISSA, California
KENNY MARCHANT, Texas
LYNN A. WESTMORELAND, Georgia
PATRICK T. McHENRY, North Carolina
VIRGINIA FOXX, North Carolina
BRIAN P. BILBRAY, California
BILL SALI, Idaho
JIM JORDAN, Ohio

PHIL SCHILIRO, *Chief of Staff*
PHIL BARNETT, *Staff Director*
EARLEY GREEN, *Chief Clerk*
LAWRENCE HALLORAN, *Minority Staff Director*

SUBCOMMITTEE ON INFORMATION POLICY, CENSUS, AND NATIONAL ARCHIVES

WM. LACY CLAY, Missouri, *Chairman*

PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York
JOHN A. YARMUTH, Kentucky
PAUL W. HODES, New Hampshire

MICHAEL R. TURNER, Ohio
CHRIS CANNON, Utah
BILL SALI, Idaho

TONY HAYWOOD, *Staff Director*

CONTENTS

	Page
Hearing held on March 11, 2008	1
Statement of:	
Evans, Karen S., Administrator, Office of E-Government and Information Technology, OMB; Linda D. Koontz, Director, Information Management Issues, GAO; and Hugo Teufel III, Chief Privacy Officer, Department of Homeland Security	6
Evans, Karen S.	6
Koontz, Linda D.	12
Teufel, Hugo, III	43
Schwartz, Ari, deputy director, Center for Democracy and Technology; Stuart Pratt, president, Consumer Data Industry Association; and Paula J. Bruening, deputy director, Center for Information Policy Leadership	66
Bruening, Paula J.	93
Pratt, Stuart	79
Schwartz, Ari	66
Letters, statements, etc., submitted for the record by:	
Bruening, Paula J., deputy director, Center for Information Policy Leadership, prepared statement of	95
Clay, Hon. Wm. Lacy, a Representative in Congress from the State of Missouri, prepared statement of	3
Evans, Karen S., Administrator, Office of E-Government and Information Technology, OMB, prepared statement of	8
Koontz, Linda D., Director, Information Management Issues, GAO, prepared statement of	14
Pratt, Stuart, president, Consumer Data Industry Association, prepared statement of	81
Schwartz, Ari, deputy director, Center for Democracy and Technology, prepared statement of	68
Teufel, Hugo, III, Chief Privacy Officer, Department of Homeland Security:	
Prepared statement of	45
Various e-mails	58

PRIVACY: THE USE OF COMMERCIAL INFORMATION RESELLERS BY FEDERAL AGENCIES

TUESDAY, MARCH 11, 2008

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON INFORMATION POLICY, CENSUS, AND NATIONAL ARCHIVES,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 2:12 p.m., in room 2203, Rayburn House Office Building, Hon. Wm. Lacy Clay (chairman of the subcommittee) presiding.

Present: Representatives Clay and Turner.

Staff present: Darryl Piggee, staff director/counsel; Jean Gosa, clerk; Adam Bordes, professional staff member; Michelle Mitchell, legislative assistant, Office of Wm. Lacy Clay; Leneal Scott, information systems manager; and Charles Phillips, minority counsel.

Mr. CLAY. The Information Policy, Census, and National Archives Subcommittee of the Oversight and Government Reform Committee will now come to order. Today's hearing will examine the role of the agencies using commercial information resellers to obtain personal information about individuals and whether there are adequate privacy safeguards in place for such transaction. We will hear from both government and private sector witnesses about the adequacy of current privacy safeguards and solicit their recommendations for improving the protections afforded to personal information that is obtained and used by our agencies. And we will also examine whether our current privacy laws and regulations require additional privacy safeguards, such as those offered in my bill H.R. 4791, the Federal Agency Data Protection Act.

Without objection, the Chair and ranking minority member will have 5 minutes to make opening statements, followed by opening statements not to exceed 3 minutes by any other Member who seeks recognition. Without objection, Members and witnesses may have 5 legislative days to submit a written statement or extraneous materials for the record.

Since the enactment of our Nation's first comprehensive privacy laws over three decades ago, advances in computing and data mining have enabled agencies and the information service industry to aggregate and combine different sources of personal information in ways that no one could anticipate.

From a privacy perspective, however, such activities have increased the risk of personal information being misused by agency

personnel or inadequately protected by data bases that are used for multiple purposes. This problem has been further magnified by the agency community's use of commercial data. Brokers obtain specific and detailed information on individuals without ensuring that adequate privacy measures are in place. In fact, a recent GAO report confirms that both agencies and commercial data brokers are uneven in their application of those information safeguards required under the Privacy Act and that agencies continue to lack effective privacy practices in the handling of such information from commercial sources.

While I realize that obtaining such information from private sources is vital to the work of our agencies, it is critical that such information be afforded the same privacy protections as data maintained on agency systems.

I welcome all of our witnesses today and look forward to their testimony and I now yield to the distinguished ranking minority member, Mr. Turner of Ohio.

[The prepared statement of Hon. Wm. Lacy Clay follows:]

HENRY A. WAXMAN, CALIFORNIA
CHAIRMAN

TOM LANTOS, CALIFORNIA
EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
CAROLYN B. MALONEY, NEW YORK
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
DANNY K. DAVIS, ILLINOIS
JOHN F. TIERNEY, MASSACHUSETTS
WM. LACY CLAY, MISSOURI
DIANE E. WATSON, CALIFORNIA
STEPHEN F. LYNCH, MASSACHUSETTS
BRIAN HIGGINS, NEW YORK
JOHN A. YARMUTH, KENTUCKY
BRUCE L. BRALEY, IOWA
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
BETTY McCOLLUM, MINNESOTA
JIM COOPER, TENNESSEE
CHRIS VAN HOLLEN, MARYLAND
PAUL W. HODES, NEW HAMPSHIRE
CHRISTOPHER S. MURPHY, CONNECTICUT
JOHN P. SARBANES, MARYLAND
PETER WELCH, VERMONT

ONE HUNDRED TENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5051
FACSIMILE (202) 225–4784
MINORITY (202) 225–5074

www.oversight.house.gov

TOM DAVIS, VIRGINIA,
RANKING MINORITY MEMBER

DAN BURTON, INDIANA
CHRISTOPHER SHAYS, CONNECTICUT
JOHN M. McHUGH, NEW YORK
JOHN L. MICA, FLORIDA
MARK E. SOUDER, INDIANA
TODD RUSSELL PLATTS, PENNSYLVANIA
CHRIS CANNON, UTAH
JOHN J. DUNCAN, JR., TENNESSEE
MICHAEL R. TURNER, OHIO
DARRELL E. ISSA, CALIFORNIA
KENNY MARCHANT, TEXAS
LYNN A. WESTMORELAND, GEORGIA
PATRICK T. McHENRY, NORTH CAROLINA
VIRGINIA FOXX, NORTH CAROLINA
BRIAN P. BILBRAY, CALIFORNIA
BILL SALI, IDAHO
JIM JORDAN, OHIO

Opening Statement
Wm. Lacy Clay (D-MO), Chairman
Information Policy, Census, and National Archives Subcommittee
Oversight and Government Reform Committee
Tuesday, March 11, 2008
2203 Rayburn HOB
2:00 P.M.

"Privacy: the Use of Commercial Information Resellers by Federal Agencies"

Good afternoon and welcome to today's hearing on the use of commercial information resellers by our federal agencies, and whether there are adequate privacy safeguards in place for such transactions. We will also examine whether our current privacy laws and regulations require additional privacy safeguards, such as those offered in my bill, H.R. 4791, the Federal Agency Data Protection Act.

Since the enactment of our nation's first comprehensive privacy laws over three decades ago, advances in computing and data mining have enabled agency users to utilize different sources of personal information in ways that no one could anticipate. From a privacy perspective, however, such activities have increased the risk of personal information being misused by agency personnel, as well as being inadequately protected by databases that are used for multiple purposes.

This problem has been further magnified by the agency community's use of commercial data brokers to obtain specific and detailed information on individuals without ensuring that adequate privacy measures are in place. In fact, a recent GAO report confirms that both agencies and commercial data brokers are uneven in their application of information safeguards required under the Privacy Act, and that agencies continue to lack effective privacy practices in their handling of information from data brokers. While I realize that obtaining such information is vital to the work of our agencies, it's critical that the government provide the same privacy protections to all data that is obtained from all sources -- not just the data maintained on agency systems.

I welcome all of our witnesses today and look forward to their testimony.

Mr. TURNER. Thank you, Mr. Chairman.

Mr. Chairman, I greatly appreciate your holding this hearing. This issue involves the careful balancing of individuals' right to privacy and the Federal Government's need to obtain information to protect national security in the war on terror and to provide other vital services. The role of commercial information resellers in supplying data about individuals to Federal agencies is certainly a new dimension both for opportunity and the need for concern. The government act requires that agencies conduct private investment assessments [PIAs], analysis of how personal information is collected, stored, shared and managed in a Federal system.

Under the E-Government Act and related Office of Management and Budget's guidance, agencies must conduct PIAs before developing or procuring information technology that collects, maintains or disseminates information that is in a personally identifiable form. Some are concerned that OMB has not provided sufficient guidance on PIAs and that some agencies have not always notified the public that commercial information resellers were among the sources used.

The importance of this hearing, obviously, is for us to be able to provide a balance. I understand that there will be a significant amount of concern of the impact of our looking at this issue on the commercial sector, and we also have concerns as to protecting individual privacy. This will be helpful because as we get more information, we can ensure that we do the right thing in proceeding.

We certainly want to make certain that on all these issues that we have a balance. We're going to hear from all sides and perspectives that we can work together to improve the situation, address valid concerns while avoiding overreaching legislation that could negatively impact agency missions. As we look to the successes that have occurred in the commercial sector, we certainly don't want to overly restrict the ability of the Federal Government to overlook these resources, but we must look to affording protections.

Mr. Chairman, I look forward to all the witnesses' testimony and yield back the balance of my time.

Mr. CLAY. If there are no additional opening statements, the subcommittee will now receive testimony from witnesses before us today. I want to start by introducing our first panel. Ms. Karen Evans is the Adiminstrator for the office of E-Government and Information Technology at the Office of Management and Budget. She is an experienced IT professional and leads the administration's program in information security. And welcome today.

Ms. EVANS. Thank you.

Mr. CLAY. We also have Ms. Linda Koontz who is the Director of Information Management issues at the U.S. Government Accountability Office. She is responsible for issues concerning the collection, use and dissemination of government information in an era of rapidly changing technology. Welcome, Ms. Koontz. Welcome back.

We also have Mr. Hugo Teufel as the Chief Privacy Officer at the Department of Homeland Security. His office is responsible for all privacy policies throughout DHS, including agency compliance with the Privacy Act of 1974, the conducting of Privacy Impact Assessments and oversight of all agency activities relating to the use, col-

lection and disclosure of personal information. Thank you too, Mr. Teufel, for being here today.

It is the policy of the committee to swear in all witnesses before they testify. I'd like to ask you to please stand and raise your right hand.

[Witnesses sworn.]

Mr. CLAY. Let the record reflect that the witnesses answered in the affirmative. I ask that each of the witnesses now give a brief summary of their testimony and to keep the summary under 5 minutes in duration. Your complete written statement will be included in the hearing record. Ms. Evans, let's begin with you.

STATEMENTS OF KAREN S. EVANS, ADMINISTRATOR, OFFICE OF E-GOVERNMENT AND INFORMATION TECHNOLOGY, OMB; LINDA D. KOONTZ, DIRECTOR, INFORMATION MANAGEMENT ISSUES, GAO; AND HUGO TEUFEL III, CHIEF PRIVACY OFFICER, DEPARTMENT OF HOMELAND SECURITY

STATEMENT OF KAREN S. EVANS

Ms. EVANS. Good afternoon, Mr. Chairman and members of the subcommittee. Thank you for inviting me to speak about the use of commercial information resellers by Federal agencies and privacy safeguards on such information.

Safeguarding the privacy of individuals and ensuring transparent agency use of personally identifiable information has been an administration priority. The administration has demonstrated progress through implementing the recommendations of the President's Identity Theft Task Force OMB guidance, diligent execution, and statutory requirements for the System of Record Notice [SORN], and Privacy Impact Assessments [PIAs], in increasing agency reporting.

Building on the work of the President's task force, OMB issued memorandum 0716 in May 2007 to enhance agency PII protections. The guidance required agencies to establish breach notification policies and provided a framework for reducing the risk of PII breaches. M–07–16 required agencies to review their use of Social Security numbers and to identify incidences in which the collection or the use of Social Security numbers was unnecessary. Within 120 days, agencies were required to establish a plan to eliminate the unnecessary collection and use of Social Security numbers.

In response to one of the task force recommendations, OMB and DHS also issued a list of 10 common risks impeding adequate protection of government information and best practices for avoiding and mitigating those risks. The risk covers a range of areas, such as security and privacy training, contracts and data sharing agreements, and physical security. All the best practices and important resources are interrelated and complementary and can be broadly applied when administering agency information security and privacy programs.

Federal agencies have pursued diligent execution of the statutory requirements for SORN in the Privacy Act and PIAs in the E-Gov Act to ensure transparent agency use and handling of individuals' information. OMB released the Fiscal Year 2007 Report on the Implementation of the Federal Information Security Management Act

of 2002 on March 1st, which reports on key measures of agencies' security and privacy programs, including SORNs and PIAs.

For example, the goal of the Federal Government is for 90 percent of the applicable systems to have publicly posted PIAs. In 2007 we reached 84 percent. While this percent remains the same as it was in 2006, a substantial increase in the number of systems identified requiring PIAs from 2006 to 2007 is indicative of the agency progress.

In next year's FISMA report, we are requiring new key privacy measures as outlined in memorandum 08–09 issued in January 2008. The increased reporting will enhance public confidence in the Federal agency privacy programs and further drive agency progress.

Privacy warrants the administration's close attention. We need to ensure Federal agencies are adhering to the enduring principles of the Privacy Act and the E-Gov Act in the face of advancing technology that allows for greater collection, analysis and storage of information by the government and industry. In the course of pursuing their missions, agencies may determine if it's necessary to obtain these products for a variety of reasons, such as verifying beneficiary addresses or for law enforcement efforts.

H.R. 4791 contains two provisions amending the E-Gov Act of 2002 intended to strengthen privacy practices specifically related to agency use of commercial information resellers. In testimony provided to the subcommittee on February 14th, I shared concerns covering the entire bill. Today I focus my written statement on concerns related to sections 8 and 9, the data broker provisions.

Although we strongly support enhancing privacy protections for information obtained by Federal agencies, we share several concerns expressed across the Federal agencies about the effect of this legislation. We are concerned these provisions would have a negative unintended consequence without the resulting enhancements and privacy protections. Information Federal agencies receive from commercial resellers must receive the same Privacy Act and E-Gov Act protections provided to other information obtained by agencies.

We look forward to working with you to ensure agency privacy policies effectively provide those protections for reseller information while enabling each agency to maintain privacy policies that align with their diverse missions.

I'd be happy to take questions at the appropriate time.

Mr. CLAY. Thank you so much, Ms. Evans.

[The prepared statement of Ms. Evans follows:]

STATEMENT OF
THE HONORABLE KAREN EVANS
ADMINISTRATOR FOR ELECTRONIC GOVERNMENT AND INFORMATION TECHNOLOGY
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE
HOUSE SUBCOMMITTEE ON INFORMATION POLICY, CENSUS, AND NATIONAL ARCHIVES OF THE COMMITTEE OF OVERSIGHT AND GOVERNMENT REFORM

March 11, 2008

Good morning, Mr. Chairman and Members of the Subcommittee. Thank you for inviting me to speak about the use of commercial information resellers by federal agencies, related provisions contained in H.R. 4791, and privacy safeguards on such information.

Safeguarding the privacy of individuals and ensuring the transparent use of personally identifiable information (PII) by federal agencies has been an Administration priority. Through implementing the recommendations of the President's Identity Theft Task Force, Office of Management and Budget (OMB) guidance, diligent execution of the statutory requirements for System of Record Notices (SORNs) and Privacy Impact Assessments (PIAs), and increased agency reporting, the Administration has improved the protection of personally identifiable information and the transparency of federal use of such information.

Protecting Personally Identifiable Information

Building on the work of the President's Identity Theft Task Force, OMB issued Memorandum 07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," in May 2007 to enhance agency PII protections. M-07-16 required the establishment of agency breach notification policies as well as provided a framework for reducing the risk of PII breaches.

M-07-16 required agencies to review their use of Social Security Numbers (SSNs) and to identify instances in which collection or use of the SSN was unnecessary. Within 120 days from the date of the memo, M-07-16 required agencies to establish a plan to eliminate the unnecessary collection and use of SSNs within 18 months. We are partnering with agencies to explore alternatives to agency use of SSNs as a personal identifier in Federal programs. For Federal employees, the Office of Personnel Management (OPM) is leading the effort to develop a policy for employee identifiers to minimize risk of identify theft.

Additionally, M-07-16 included reminders to encrypt all data on mobile computers/devices carrying agency data, unless the Deputy Secretary makes a written determination that the data is not sensitive. This reminder would apply to agency laptops

and other devices which contain personal information. The encryption must meet National Institute of Standards and Technology (NIST) requirements.

In each Agency's Fourth Quarter FY 2007 E-Government scorecard, OMB included language requiring agencies to submit a status update by December 14th as well as a date when each agency would be in full compliance of the M-07-16 requirements.

In response to one of the task force recommendations, OMB and the Department of Homeland Security (DHS) issued a list of ten common risks impeding adequate protection of government information and best practices for avoiding and mitigating those risks. The risks cover a range of areas, such as security and privacy training, contracts and data sharing agreements, and physical security. All of the best practices and important resources are inter-related and complementary, and can be broadly applied when administering agency information security and privacy programs. The publication can be found at the following site: http://csrc.nist.gov/pcig/document/Common-Risks-Impeding-Adequate-Protection-Govt-Info.pdf.

Federal Agency Transparency and Key Privacy Measures

Federal agencies have pursued diligent execution of the statutory requirements for SORNs in the Privacy Act and PIAs in the E-Government Act to ensure transparency for agency use and handling of individuals' information. OMB recently released the FY 2007 Report to Congress on Implementation of the Federal Information Security Management Act of 2002 (FISMA), which reports on key measures of agency privacy programs, including SORNs and PIAs.

For example, the Federal goal is for 90 percent of applicable systems to have publicly posted PIAs. In 2007, 84 percent of applicable systems within the 25 large agencies have publicly posted PIAs. While this percentage remains the same as it was in 2006, the substantial increase in the number of systems identified as requiring a PIA from 2006 to 2007 (an increase of more than 500 systems) is indicative of progress despite no overall increase in the percentage of systems with a PIA. In addition to the high rate of applicable systems with publicly posted PIAs, nineteen of 23 agency Inspectors General reported having its agency PIA process as "satisfactory" or better.

For the percentage of applicable systems of records covered by the Privacy Act to have developed, published, and maintained SORNs, the Federal goal is 90 percent. In 2007, the actual performance was 83. Similar to the PIAs, this percentage remains steady from 2006, though the number of systems identified as requiring a SORN increased by more than 700 systems.

The NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems," also identifies conducting PIAs as a control agencies should use and be reviewed during the Certification & Accreditation process. As required by 44 U.S.C. § 3543, Federal agencies must adopt and comply with standards

promulgated by NIST, and identify information security protections consistent with these standards.

In OMB Memorandum 08-09, "New FISMA Privacy Reporting Requirements for FY 2008," we outlined increased reporting of key privacy measures for next year's FISMA report that will enhance public confidence in federal agency privacy programs and further drive agency progress.

Commercial Information Reseller Provisions in H.R. 4791

Privacy warrants the Administration's close attention, in part, due to the need to ensure federal agencies are adhering to the enduring principles of the Privacy Act and the E-Government Act in the face of advances in technology that allow for greater collection, analysis, and storage of information by government, industry, and the non-profit sector. Commercial information resellers, commercial entities that collect information from a range of sources and package them into useful products, are a result of these technological advances. In the course of pursuing their missions, agencies may determine it necessary to obtain these products for a variety of reasons, such as verifying beneficiary addresses or law enforcement efforts. Personally identifiable information federal agencies receive from commercial resellers must receive the same Privacy Act and E-Government protections provided to other information obtained by agencies.

H.R. 4791, the proposed "Federal Agency Data Protection Act" contains two provisions amending the E-Government Act of 2002 intended to strengthen privacy practices specifically relating to agency use of commercial information resellers.

Section 8 defines the term "data broker" and requires agencies to conduct a Privacy Impact Assessment when "purchasing or subscribing for a fee to information in identifiable form from a data broker." I will address the bill's definition of "data broker" later in my testimony. Section 9 prohibits agencies from contracts with data brokers for databases primarily with personally identifiable information without a Privacy Impact Assessment of the data broker's database and requires each agency to promulgate regulations on a range of related standards governing the access, analysis, accuracy, timeliness, use, retention, disclosure, redress for adverse consequences, and enforcement mechanisms to prevent unlawful use.

Although we strongly support enhancing privacy protections for personal information obtained by federal agencies, including information from data brokers, we share several concerns expressed across Federal agencies about the effect of this legislation. In testimony provided to this subcommittee and the Subcommittee on Government Management, Organization, and Procurement on February 14th, I shared concerns that covered the entire bill. Today, I will focus on concerns relating to Sections 8 and 9.

We are concerned the commercial information reseller provisions would have negative unintended consequences without resulting in enhanced privacy protections for agency collection, use, and storage of personal information.

Section 8's and Section 9's new PIA requirements are somewhat duplicative, since federal agencies already conduct PIAs for IT systems receiving information shared by data brokers. OMB guidance on conducing PIAs, M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," directs agencies to conduct a PIA when systematically incorporating identifiable information from commercial sources into its information systems.

For the Section 9 PIA requirement, conducting PIAs on data brokers' propriety systems is legally problematic and could seriously discourage data brokers from offering their services to assist federal agencies. Data brokers could charge agencies substantially higher fees for the increased invasiveness without adding new transparency into how agencies handle personal information, which is already reflected in current PIAs. The applicability of the National Security System exemptions in the E-Government Act to the new requirements is also unclear.

Section 9 also would require specific regulations for agencies to promulgate for contracting with data brokers. Such regulatory rigidity would make it difficult for agencies to adapt to changing realities. Over time, this could leave both agencies and data brokers unable to employ the most effective privacy policies and practices.

Section 8 also broadly defines a "data broker" as "a business entity that, for monetary fees ... regularly engages in the practice of collecting, transmitting, or providing access to sensitive information in identifiable form on more than 5,000 individuals who are not the customers or employees of that business entity or affiliate primarily for the purposes of providing such information to non-affiliated third parties on an interstate basis.'' This definition could cover a range of widely used research and reference services as well as routine services, such as change-of-address notification.

We look forward to working with you to ensure that federal agencies privacy policies effectively provide the Privacy Act and E-Government protections for information agencies obtain from commercial resellers, while allowing each agency the ability to maintain privacy policies that align with the ways agencies use and handle the data to pursue their diverse missions.

Mr. CLAY. Ms. Koontz, you may proceed.

STATEMENT OF LINDA D. KOONTZ

Ms. KOONTZ. Mr. Chairman and members of the subcommittee, I appreciate the opportunity to be here today to discuss issues surrounding the Federal Government's purchase of personal information from businesses known as information resellers.

I'd like to briefly summarize the results of our work on this topic. Information is an extremely valuable resource and the services provided by information resellers are important to a variety of Federal agency functions. Our work has shown that agencies make significant use of information obtained from information resellers. Specifically for fiscal year 2005, four agencies we reviewed—Justice, Homeland Security, State, and Social Security reported a combined total of approximately $30 million to purchase personal information from resellers. The vast majority of the spending, just over 90 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, researching assets held by individuals of interest and detecting fraud in prescription drug transactions. Reseller information was also used to detect and investigate fraud, verify identities and determine benefit eligibility.

While agencies took steps to address privacy and security of the information acquired from resellers, they did not do all that they could to protect individuals' privacy rights. Specifically, although agencies issued public notices on information they were collecting about individuals, these did not always specifically state that information resellers were among the sources used. In several of these cases, agency sources for personal information were described only in vague terms such as private organization, other public resources, or public source material.

We also found that few agencies were conducting Privacy Impact Assessments which can be important tools for helping agencies identify privacy implications because they did not think they were required. Contributing to this rather uneven application of privacy principles were ambiguities in OMB guidance regarding the applicability of privacy requirements for Federal agency uses of reseller information.

As a result we made recommendations to OMB to clarify its guidance and direct agencies to review their uses of information obtained from resellers. We've also recommended that the agencies we reviewed develop specific policies for the use of commercial data. OMB and the four agencies generally agreed with our report. Since then, agencies have taken action to address our recommendations.

For example, DHS incorporated direction on the use of commercial data into its May 2007 Guidance on Privacy Impact Assessments. However, OMB has not taken the actions we've recommended.

We would also like to comment on the proposed Federal Agency Data Protection Act which would require that agencies conduct Privacy Impact Assessments for their uses of commercial data and develop regulations governing the use of such data. These provisions

are very consistent with our previous recommendations and should help ensure that Federal agencies appropriately tend to privacy concerns when using commercial data.

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

That concludes my statement. Thank you.

Mr. CLAY. Thank you so much, Ms. Koontz.

[The prepared statement of Ms. Koontz follows:]

United States Government Accountability Office

GAO

Testimony

Subcommittee on Information Policy, Census, and National Archives, Committee on Oversight and Government Reform

For Release on Delivery
Expected at 2 p.m. EDT
Tuesday, March 11, 2008

PRIVACY

Government Use of Data from Information Resellers Could Include Better Protections

Statement of Linda D. Koontz, Director
Information Management Issues

GAO-08-543T

Abbreviations

DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DOJ	Department of Justice
FBI	Federal Bureau of Investigation
OECD	Organization for Economic Cooperation and Development
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PIA	privacy impact assessments
SSA	Social Security Administration
State	Department of State
TSA	Transportation Security Administration

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product 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.

March 11, 2008

GAO
Accountability·Integrity·Reliability
Highlights

Highlights of GAO-08-543T, a testimony before Subcommittee on Information Policy, Census, and National Archives, Committee on Oversight and Government Reform

PRIVACY

Government Use of Data from Information Resellers Could Include Better Protections

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 April 2006 report 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 used personal data from resellers and to review the extent to which agencies' policies and practices for handling this information reflected the Fair Information Practices, a set of widely accepted principles for protecting the privacy and security of personal data. GAO was also asked to provide an update on the implementation status of its recommendations and to comment on provisions of the proposed Federal Agency Data Protection Act. In preparing this testimony, GAO relied primarily on its April 2006 report.

What GAO Recommends

GAO is not making additional recommendations at this time. However, in its 2006 report, GAO made recommendations to the Office of Management and Budget and the four agencies to address agency use of personal information from commercial sources. Agency officials generally agreed with the content of the report. Since then, 2 of the 4 agencies have taken steps to address its recommendations; however, OMB has not issued clarified guidance.

To view the full product, including the scope and methodology, click on GAO-08-543T. For more information, contact Linda Koontz at (202) 512-6240 or KoontzL@gao.gov.

What GAO Found

In fiscal year 2005, the Departments of Justice, Homeland Security, and State and the Social Security Administration reported that they used personal information obtained from resellers for a variety of purposes, including performing criminal investigations, locating witnesses and fugitives, researching assets held by individuals of interest, and detecting prescription drug fraud. The agencies planned spending 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).

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 (OMB) regarding the applicability of privacy requirements to federal agency uses of reseller information. In addition, agencies generally lacked policies that specifically address these uses.

GAO 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. The five agencies generally agreed with the report and described actions initiated to address the recommendations. Since GAO issued its report, agencies have taken steps to address the recommendations. For example, the Department of Homeland Security Privacy Office incorporated specific questions in its May 2007 Privacy Impact Assessment guidance concerning use of commercial data. In addition, the Department of Justice took steps to update its public notices to specify their use of data from information resellers. OMB, however, has not implemented GAO's recommendation to clarify guidance on use of commercial data.

The Federal Agency Data Protection Act was introduced on December 18, 2007. The legislation, among other things would require that agencies (1) conduct privacy impact assessments for their uses of commercial data, and (2) promulgate regulations concerning the use of commercial data brokers. GAO considers these requirements to be consistent with the results and the recommendations made to the agencies in its 2006 report

Mr. Chairman and Members of the Subcommittee:

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, 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—and especially whether their practices are fully consistent with widely accepted practices for protecting the privacy and security of personal information.

Federal agency use of personal information is governed primarily by the E-Government Act of 2002 and the Privacy Act of 1974. The E-Government Act of 2002 strives to enhance protection for personal information in government information systems 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. The Privacy Act of 1974[2] 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

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

[2]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.

first proposed in 1973 by a U.S. government advisory committee.[3] These principles, now widely accepted, include

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, and New Zealand, as well as the European Union.

As agreed, my testimony today will be based primarily on the agency information contained in a report we issued in April 2006.[5] For 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 (DOJ), Homeland Security (DHS), and State (State) and the Social Security Administration (SSA). We compared relevant agency guidelines and management policies and

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

[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).

procedures to the Fair Information Practices. We also updated the implementation status of recommendations contained in our 2006 report and analyzed provisions of the proposed Federal Agency Data Protection Act.[6] Our work was performed in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Today, after a brief summary of the laws that govern agency use of personal information, I will summarize the information contained in our 2006 report on how the selected agencies used the personal information that they purchased from resellers and the extent to which the agencies had policies and practices that reflected the Fair Information Practices. I will also provide an update on steps taken by the agencies to address the recommendations contained in our 2006 report. Finally, I will comment on specific privacy related provisions of the proposed Federal Agency Data Protection Act.

Results in Brief

In fiscal year 2005, DOJ, 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

[6]H.R. 4791, Federal Agency Data Protection Act, 110th Cong., introduced by Representative Wm. Lacy Clay, December 18, 2007.

[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.

percent). For example, components of DOJ (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 benefits eligibility.

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

- Although agencies notified the public through *Federal Register* notices and published PIAs that they collected personal information from various sources, they did not always indicate specifically that information resellers were among those sources.
- Some agencies lacked robust audit mechanisms to ensure that use of personal information from information resellers was for permissible purposes, reflecting an uneven application of the *accountability* principle.

Contributing to agencies' uneven application of the Fair Information Practices were ambiguities in guidance from the Office of Management and Budget (OMB) on how privacy requirements apply to federal agency uses of reseller information. In addition, agencies generally lacked 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. The agencies generally agreed with the report and described actions initiated to address our recommendations. Since we issued our report, two of the four agencies have taken steps to address our recommendations. For example, the DHS Privacy Office incorporated specific questions in its May 2007 PIA guidance concerning use of commercial data. In addition, DOJ took steps to ensure that their system-of-records notices specifically reference their use of data from information resellers. OMB, however, has not implemented our recommendation to clarify guidance on use of commercial data.

On December 18, 2007, the Federal Agency Data Protection Act was introduced. This legislation, among other things would require that agencies (1) conduct PIAs for their uses of commercial data and (2) promulgate regulations concerning the use of commercial data brokers. We believe that these requirements are consistent with the results of our 2006 report and the recommendations we made to the agencies.

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 collecting and aggregating personal information from multiple sources and making 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.

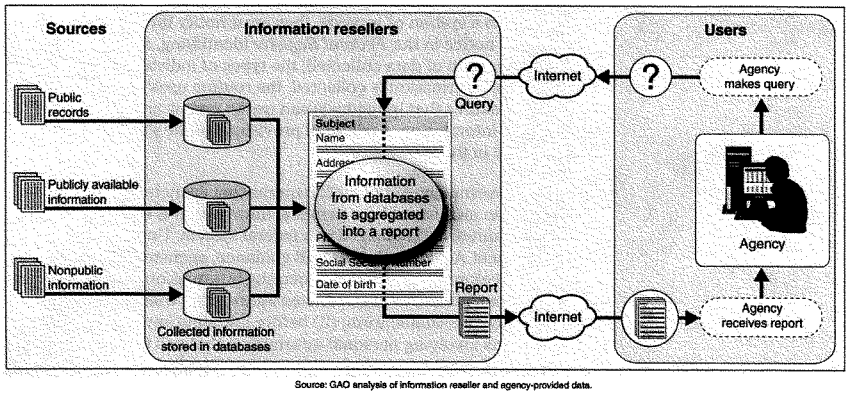
Information resellers have now amassed extensive amounts of personal information about large numbers of Americans. They supply it to customers in both government and the private sector, typically via a centralized online resource. Generally, three types of information are collected:

- *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,[8] product warranty registrations, and other application information provided to private businesses directly by consumers.

[8]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.

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

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'

[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.

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 the information is collected, the routine uses[10] of the data, and procedures that individuals can use to review and correct their personal information. Additional provisions of the Privacy Act are discussed in the 2006 report.

The E-Government Act of 2002 requires that agencies conduct PIAs. 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.

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,

[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)).

issued in 1975.[11] 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 PIA mandate in the E-Government Act of 2002 provided a mechanism by which agencies can consider privacy in the earliest stages of system development. 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 made publicly available,[12] 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.

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.[13] The Organization for Economic Cooperation and Development (OECD)[14] developed a revised

[11]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 has periodically published additional guidance. Further information regarding OMB Privacy Act guidance can be found on the OMB Web site at http://www.whitehouse.gov/omb/inforeg/infopoltech.html.

[12]The E-Government Act requires agencies, if practicable, to make PIAs 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).

[13]U.S. Department of Health, Education, and Welfare, *Records, Computers and the Rights of Citizens*.

[14]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.

version of the Fair Information Practices in 1980. This version of the principles was reaffirmed by OECD ministers in a 1998 declaration and further endorsed in a 2006 OECD report.[15] The Fair Information Practices, have, with some variation, formed the basis of privacy laws and related policies in many countries, including the United States, Germany, Sweden, Australia, and New Zealand, as well as the European Union.[16]

In addition, in its 2007 report, *Engaging Privacy and Information Technology in a Digital Age*, the National Research Council[17] found that the principles of fair information practice for the protection of personal information are as relevant today as they were in 1973. Accordingly, the committee recommended that the Fair Information Practices should be extended as far as reasonably feasible to apply to private sector organizations that collect and use personal information. The eight 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.

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

[16]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).

[17]National Research Council of the National Academies, *Engaging Privacy and Information Technology in a Digital Age* (Washington, D.C.; 2007).

Principle	Description
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.

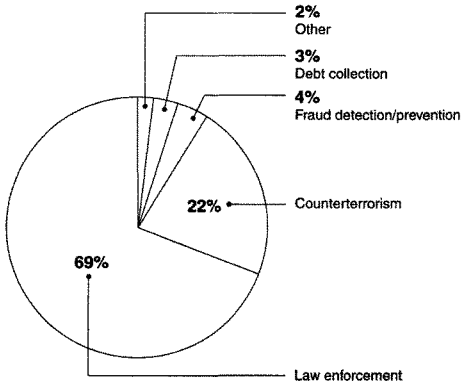
Agencies Used Governmentwide Contracts to Obtain Personal Information from Information Resellers for a Variety of Purposes

DOJ, DHS, State, and SSA reported approximately $30 million through contracts with information resellers in fiscal year 2005.[18] 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

[18] 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 for 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 the 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.

(22 percent). Figure 2 details contract values categorized by their reported use.

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.

DOJ, 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 benefits eligibility determination.

DOJ and DHS Used Information Resellers Primarily for Law Enforcement and Counterterrorism

In fiscal year 2005, DOJ and its components reported approximately $19 million through contracts with 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 DOJ's largest user of information resellers, used 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 provided 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.[19]

The Drug Enforcement Administration (DEA), the second largest DOJ user of information resellers in fiscal year 2005, obtained reseller data primarily to detect fraud in prescription drug transactions.[20] Agents used reseller data to detect irregular prescription patterns for specific drugs and trace this information to the pharmacy and prescribing doctor.[21]

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 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 collected data such as address and vehicle information for criminal investigations and background security checks. Another DHS component, U.S. Customs and Border Protection, conducts queries on people, businesses, property. The Federal Emergency Management Agency, an additional component, used an information reseller to detect fraud in disaster assistance applications.

[19]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).

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

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

DHS also reported using information resellers in its counterterrorism efforts. For example, the Transportation Security Administration (TSA), a DHS component, used data obtained from information resellers as part of a test associated with the development of its domestic passenger prescreening program, called Secure Flight.[22] TSA planned 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.[23]

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

In an effort to ensure the accuracy of Social Security benefit payments, the SSA 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),[24] 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, used several information resellers to assist investigative agents in detecting benefits 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.

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

[22]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).

[23]TSA's current plans for Secure Flight do not include the use of reseller information.

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

submitted on immigrant and nonimmigrant visa petitions. State also used reseller data to investigate passport and visa fraud cases.

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

Agencies generally lacked policies that specifically addressed their use of personal information from commercial sources (although DHS Privacy Office officials reported in 2006 that they were drafting such a policy[25]), 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, were often not conducted. Finally, components within each of the four agencies did not

[25]Subsequent to the 2006 report, the DHS Privacy Office took steps to develop guidance on the use of personal information from information resellers in its PIA guidance.

consistently hold staff accountable by monitoring usage of personal information from information resellers and ensuring that it was appropriate; thus, their application of the fourth principle, *accountability,* 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 did not generally monitor usage of personal information from information resellers to hold users accountable for appropriate use; instead, they relied 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.

Source: GAO analysis of agency-supplied data.

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.

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 of State and SSA as a whole and by major components of DOJ and DHS. We did not obtain information on smaller components of DOJ 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 that 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.[26]

[26]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 DOJ, 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 Contributed 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.[27]

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—is required of 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.[28] OMB guidance on implementing the Privacy Act does not specifically

[27]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 uses, including investigative records compiled for criminal or civil law enforcement purposes.

[28]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).

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.[29]

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

[29]As we have 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."[30] Although the guidance is unclear as to 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[31] 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 Were 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

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

[31]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,[32] they provide explanations to the public about things such 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."[33] 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.

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.

[32]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).

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

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 on management oversight of usage details. 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 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.

Not All Agencies Have Taken Steps to Address our Recommendations

In our report, we recommended that the agencies develop specific policies for the collection, maintenance, and use of personal information obtained from resellers. We also recommended that OMB revise its 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. The agencies generally agreed with our findings and described actions initiated to address our recommendations.

Since the issuance of our 2006 report, two of the four agencies have taken action to address our recommendation. For example, the DHS Privacy Office incorporated specific questions in its May 2007 PIA guidance concerning use of commercial data. The guidance requires programs that use commercial or publicly available data to explain why and how such data are used. Further, the guidance for systems that use or rely on commercial data requires an explanation of how data accuracy and integrity are preserved and the reliability of the data assessed with regard to its value to the purpose of the system. According to DHS Privacy Office officials, after identifying use of commercial data through the PIA process, the Privacy Office works with the relevant DHS component to review uses of commercial data to ensure appropriate controls are in place and that the planned uses are appropriately disclosed in privacy notices. In addition, officials at DOJ informed us that the Privacy and Civil Liberties Office has in place a verbal agreement with agency components that there are to be no bulk acquisitions of commercial data and that when the agency takes in data from commercial sources, there should be a valid system-of-records notice that specifically identifies commercial data as a source. Further, DOJ has updated several of its system-of-records notices to reflect their use of data from information resellers. SSA and State have not yet addressed our recommendation.

However, OMB has not addressed our recommendations. In an August 2006 letter to congressional committees in response to the recommendations contained in our April 2006 report, OMB noted

that work on the protection of personal information through the Identity Theft Task Force was ongoing and that following the completion of this work, they would consider issuing appropriate clarifying guidance concerning reseller data. Since then, OMB's efforts on the Identity Theft Task Force have been completed and on May 22, 2007 OMB issued M-07-16, "Safeguarding Against the Breach of Personally Identifiable Information." To date, OMB has not issued additional clarifying guidance concerning reseller data.

Privacy Provisions of the Proposed Federal Agency Data Protection Act are Consistent with Our Recommendations

The Federal Agency Data Protection Act was introduced on December 18, 2007. Among other things, the legislation contains privacy provisions that would require agencies to conduct PIAs when "purchasing or subscribing for a fee to information in identifiable form from a data broker." We believe that such a requirement is consistent with the recommendations contained in our report, particularly given the debate concerning whether or not agencies "systematically incorporate" information or are "merely pinging or querying the information." Our report found that PIAs could serve to address certain Fair Information Practice principles such as *purpose specification* and *openness*, but often were not conducted. Such a requirement could more readily ensure agencies perform these assessments. Further, since OMB has not clarified its guidance on this issue, a requirement in law could provide needed direction to agencies.

The proposed Federal Agency Data Protection Act would also require each agency to prescribe regulations that specify, among other things, the personnel permitted to access, analyze, or otherwise use commercial reseller databases. This legislation is consistent with our recommendation that agencies develop policies concerning their use of personal information from information resellers.

In summary, services provided by information resellers are important to federal agency functions such as law enforcement and fraud protection and identification. While agencies have taken steps

to adhere to some 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 use the specific processes of the 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. Since we issued our report in 2006, two of the four agencies have taken steps to address our recommendations. However, OMB has not modified its guidance. 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 being adequately protected. Absent action from OMB to revise guidance, privacy provisions contained in the proposed Federal Agency Data Protection Act could clarify the need to conduct privacy impact assessments wherever reseller data are involved and promote the development of agency policies and procedures concerning the use of such data. We believe these provisions are consistent with the results and recommendations contained in our 2006 report.

Mr. Chairman, this concludes my testimony today. I would be happy to answer any questions you or other members of the subcommittee 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 Susan Czachor, John de Ferrari, Nancy Glover, Rebecca LaPaze, David Plocher, and Jamie Pressman.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Mail or Phone

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

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

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Congressional Relations

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

Public Affairs

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

PRINTED ON RECYCLED PAPER

Mr. CLAY. Mr. Teufel.

STATEMENT OF HUGO TEUFEL III

Mr. TEUFEL. Good afternoon, Mr. Chairman and Ranking Member Turner and members of the committee. It's an honor to be here today to talk to you about commercial information and privacy. And it's also a pleasure to be here today with my colleagues who I hold in very high regard: Ms. Evans from OMB and Ms. Koontz from GAO, and we work together often. I gather I'm here to give an agency perspective and I will endeavor to do my best in giving that perspective.

In my oral statement, which will be brief, I want to touch on a few highlights beyond what's in my written statement. And I note that the privacy implications of the use of commercial information are not new to my office, and so I want to go through a little timeline here for you.

In September 2005 the Privacy Office held a workshop on commercial information.

September 28, 2005, our Data Privacy and Integrity Advisory Committee issued the first of two reports on this information.

And on April 4, 2006, Acting Chief Privacy Officer Maureen Cooney testified, I think before this committee, on the subject.

Following that, on December 6, 2006, our Data Privacy and Integrity Advisory Committee issued its second report on commercial information.

As Ms. Koontz noted, our PIA guidance has been updated to take into account the use of commercial information, and section 2 of the Privacy Impact Assessment Guidance talks about the sorts of things that operational components, Department-Level components, programs at the Department thinking about using personally identifiable information, should consider when using commercial information.

So we've got our PIA guidance that addresses this type of information, and our PIA guidance. And our authority to conduct Privacy Impact Assessments comes not just from section 208 of the E-Government Act, which is one of the three pillars of Federal privacy law, but also comes from section 222, subsection 4, which allows us to conduct Privacy Impact Assessments on proposed rules, and the subsection 1 of the old section 222, which relates to the uses of technology at the Department to make sure that they sustain privacy and do not erode privacy.

So the next thing I want to talk about is training. We provide privacy impact assessment training throughout the government. We are looking at doing another workshop for Federal agency privacy officers in probably May or June this year. We recently have begun doing smaller training for 20 or fewer within the Department of Homeland Security on Privacy Impact Assessments. And we find that when we give PIA training, other agencies follow the lead that we have—the trail that we have blazed.

System of Records Notices, which as you will recall were required under the privacy impact of 1974, and GAO and Ms. Koontz recently issued a report—actually I guess it was not so recent, it was maybe 9 months ago—on my office. And one of the things that Ms. Koontz mentioned was that we had a number of legacy agency Sys-

tem of Records Notices that we have to update. About 208 to be exact, give or take a couple. We have made substantial progress in revising our legacy agency System of Records Notices. We've just sent over 28 to Coast Guard for them to consider. And we anticipate that there will be a substantial number more that will be updated in the coming months. And of course we take into account the types of information that go into Systems of Records, as required under the Privacy Act of 1974.

Then the last highlight I wanted to mention to you is component privacy officers. One of my recommendations that existed prior to Ms. Koontz's report but was highlighted or mentioned independently in her report was for an increase in component privacy officers at the Department. At the time of the report there were two component privacy officers at the Transportation Security Administration and at US-VISIT. In November, the Secretary—of last year—the Secretary agreed with me that there should be additional component privacy officers, and four operational components and two Department-level components. And we and the components are moving forward on the hiring or the selection of those component privacy officers.

So the last thing that I wanted to mention to you is something that you won't see on paper, and that's what happens day in and day out in my Office. And that is when operational components and program personnel come to my folks who work in the Compliance Section of the Office to talk about new systems. And one of the things that is discussed is whether commercial information is being used and if so, how it's being used. And using the Fair Information Practice Principles, which are set forth in my written testimony, we work through with the components and program personnel to make sure that commercial information is used appropriately.

That's all I have to say. Thank you very much.

Mr. CLAY. Thank you so much, Mr. Teufel.

[The prepared statement of Mr. Teufel follows:]

WRITTEN STATEMENT

OF

HUGO TEUFEL III
CHIEF PRIVACY OFFICER
U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
SUBCOMMITTEE ON INFORMATION POLICY, CENSUS AND
NATIONAL ARCHIVES

FOR A HEARING ENTITLED:

PRIVACY: THE USE OF COMMERCIAL INFORMATION RESELLERS
BY FEDERAL AGENCIES

MARCH 11, 2008

Introduction

Chairman Clay, Ranking Member Turner, and Members of the Subcommittee, I thank you for the opportunity to address the Subcommittee on Information Policy, Census and National Archives, on efforts of the Department of Homeland Security to promote privacy protections within Department programs, particularly those utilizing personally identifiable information (PII) obtained from commercial sources.

On April 4, 2006, the then Acting Chief Privacy Officer, Maureen Cooney, appeared before a Subcommittee of the House Judiciary Committee to address the uses of information acquired from commercial information resellers, following the issuance of a Government Accountability Office Report entitled "PERSONAL INFORMATION: Agency Reseller Adherence to Key Privacy Principles."[1] During her testimony, Ms. Cooney outlined the procedures then in place to understand the uses of commercially available information in the Department, and to identify and mitigate the privacy concerns raised by that use. She also outlined additional steps the Department planned in order to foster the effective use of commercial data in a manner that respects individual privacy interests.

Although the basic framework is the same today, the Privacy Office has made a number of improvements to the process to ensure that information obtained from information resellers will be used in accordance with the Fair Information Practice Principles (FIPPs), which overarch all DHS uses of information, however obtained. Therefore, my testimony will focus on the Privacy Office's robust privacy compliance program and update the Subcommittee on enhancements made since 2006 to understand and evaluate the use of commercial data in DHS programs.

Use of Commercially Available Data by DHS

As an initial matter, it is important to acknowledge that GAO accurately described the uses of commercial information in DHS programs in its 2006 report. Although the specific contract amounts and other particulars may be slightly out of date today, the report shows that a number of components use commercially available PII, including Immigration and Customs Enforcement, Customs and Border Protection, U.S. Citizenship and Immigration Services, the Transportation Security Administration, U.S. Secret Service, the Federal Emergency Management Agency, Office of Inspector General, U.S. Coast Guard, and the Federal Law Enforcement Training Center. As noted in the report, moreover, the three principal uses of this commercial data at the

[1] GAO-06-421, April 2006.

Department support (1) law enforcement, (2) counterterrorism, and (3) fraud detection and prevention missions.

Government use of commercial data aggregators may pose particular privacy concerns, because the information was initially compiled for commercial purposes and not for government purposes. Commercial purposes may have different acceptable levels of accuracy. The need for accuracy is lower, for example, for a company mailing a catalog than for the government relying on information to issue a government-issued credential. The impact to the individual for inaccuracy in a commercial setting can be lower than in a government setting, as well.

In recognition of this fact, the Privacy Office first held a Privacy and Technology Public Workshop on September 8 and 9, 2005, which Ms. Cooney highlighted in her testimony in April 2006. The workshop focused on the government's use of commercial data and its associated privacy concerns. We also committed the question to our panel of outside experts serving on the Data Privacy and Integrity Advisory Committee (DPIAC).

Efforts of the Data Privacy and Integrity Advisory Committee

The DPIAC was established under the Federal Advisory Committee Act (5 U.S.C. App.) to advise the Secretary and the Chief Privacy Officer on the privacy implications of DHS programs.

Given the importance of understanding the privacy issues surrounding the use of PII obtained from commercial information resellers, the Privacy Office twice tasked the DPIAC to provide recommendations on how to apply the FIPPs to this practice.

On September 28, 2005, the DPIAC issued a report entitled "The Use of Commercial Data to Reduce False Positives in Screening Programs."[2] The committee recommended 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
- Assess to the data is tightly controlled
- The potential harm to the individual from a false positive misidentification is substantial
- Use for the secondary purpose 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

[2] DPIAC Report No. 2005-01, available from http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_rpt_1streport.pdf; Internet; accessed 5 March 2008.

- 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

When these recommendations proved valuable, the Privacy Office asked the DPIAC to expand the scope of its examination to include the full range of DHS programs using commercial data, in addition to screening programs. On December 6, 2006, the committee issued a report entitled "Use of Commercial Data."[3] After advocating universal application of the recommendation from its screening report, the committee offered the following additional recommendations:

- The definition of Commercial Data should not exclude the following: (a) Publicly Available Data, data in the public domain that can be obtained or accessed from publicly accessible sources, both public and private; and (b) Public Record Data, data collected and maintained by a government entity for a public purpose and used outside of that public purpose.
- DHS should publish System of Records Notices (SORNs) for new or revised systems of records that use Commercial Data in a systematic manner or where there is substantial risk of harm.
- Apply Privacy Impact Assessments (PIAs) to programs that use Commercial Data, where the Privacy Threshold Analysis (PTAs) shows Commercial Data is used systematically or where there is substantial risk of harm.
- Revise the PIA template and guidance documents to include a Commercial Data module and amend the analysis of completed PIAs where necessary.
- Have the DHS Privacy Office analyze the template contract language for Commercial Data vendor relationships, propose any necessary modifications, and review each relationship and contract.
- Make certain the DHS Privacy Office can effectively require the accurate and timely processing of PIAs, and mitigation of privacy risks noted therein.
- Make certain DHS commits sufficient resources to the DHS Privacy Office to (a) review the PIAs, (b) follow up to make certain privacy risks are mitigated, and (c) ensure the PIA continues to be accurate as programs change.

As we have come to expect from the DPIAC, these recommendations were valuable as well. The Privacy Office spent the early months of 2007 evaluating how to incorporate them into the Department's PIA process.

---

[3] DPIAC Report No. 2006-03, available from http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_commdata.pdf; Internet; accessed 5 March 2008.

Privacy Impact Assessments under E-Government Act and PIA Guidance

The Privacy Office agrees with GAO's assessment in its'06 report that PIAs are an important tool for agencies to publicly address privacy issues early in the process of developing new information technology (IT) systems. Indeed, the *E-Government Act of 2002* requires agencies to conduct a PIA when developing or procuring IT systems or projects that collect, maintain, or disseminate information in an identifiable form or about members of the public.

As the Chief Privacy Officer, I was pleased to note that GAO found DHS had increased both the number and quality of our PIAs during its last review of our office.[4] This impressive improvement is due to the regular review and revision of the PIA Guidance and accompanying training presentations, developed by the Privacy Office's Director of Privacy Compliance. The last revision issued in May 2007 incorporates the recommendations of two DPIAC reports on the use of commercial data.

The connection between the need for a PIA and the use of commercial data is made plain in the PIA Guidance. Under the heading *When to Conduct a PIA*, for instance, program or system officials are instructed to complete a PIA "if a program or system adds additional sharing of information either with another agency or incorporates commercial data from an outside data aggregator..."[5]

The PIA Guidance then calls for information and analysis about the proposed use of commercial data in no fewer than nine places, giving expression to the DPIAC's recommendations. These include a required discussion of why the commercial data is "relevant and necessary" to the system's purpose, and how it is used to fulfill these purposes. Additionally, PIAs now call for a discussion of the "levels of accuracy" of the commercial data required by the contract between DHS and the commercial aggregator. This is consistent with the DPIAC recommendation that the Privacy Office review certain provisions of vendor contracts.

Additional Authority for PIAs

It is well understood that the E-Government Act requires PIAs for many government IT systems, including most making use of commercial data. As the GAO report points out, however, DHS cites OMB guidance in an Appendix to its PIA Guidance, which includes a parenthetical exception to this requirement: "Merely querying [a commercial source] on an ad hoc basis using existing technology does not trigger the PIA requirement."[6] Thus, the undefined difference between "systematic" and "ad hoc" uses, prompted GAO to

[4] GAO-07-522, DHS PRIVACY OFFICE: Progress Made but Challenges Remain in Notifying and Reporting to the Public, April 2007.
[5] Privacy Impact Assessment: Guidance, DHS Privacy Office, May 2007,
[6] Id. Appendix I: PIA Triggers (citing OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 30, 2003).

recommend that OMB revise its guidance to clarify the applicability of the Privacy Act and the E-Government act to the use of PII from resellers.

When the DPIAC examined this question for the Department, it recommended that a PIA be conducted where commercial data is used systematically as required by E-Government Act or where there "is substantial risk of harm" from the use, even if that use is ad hoc and exempt from the requirement under OMB guidance. This recommendation recognizes that the DHS Chief Privacy Officer has additional authority to conduct PIAs beyond the authority under the E-Government Act.

Section 222 of the Homeland Security Act of 2002, the Privacy Office's organic legislation, gives the Chief Privacy Officer separate and distinct authority to conduct PIAs on his own initiative in order to "assure that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information." We have found that PIAs are an invaluable tool for programs to understand how their use of information impacts privacy. In addition, PIAs enhance the confidence the public has in the steps DHS takes to protect privacy. Under this additional authority, the Privacy Office has pioneered the use of PIAs beyond what the E-Government Act requires in two ways.

First, the Privacy Office recognizes that privacy can be impacted by programs, policies, certain uses of information, and rules, in addition to information technology. Therefore, as a matter of policy the Privacy Office conducts PIAs to examine these offices, policies, uses, and rules, as well, even though it is not required to under the E-Government Act.

These PIAs examine the application of the Fair Information Practice Principles (FIPPs) to the policy or, in this case, a particular use. The eight FIPPs are rooted in the tenets of the Privacy Act and govern the appropriate use of personally identifiable information (PII) at the Department.[7] They are:

1. Transparency: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate. There should be no system whose existence and purpose is a secret.
2. Individual Participation: DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should

[7] The Department's PIA Guidance defines PII as "any information that permits the identity of an individual to be directly or indirectly inferred, including any information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department." Section 208 of the E-Gov Act requires agencies to conduct a PIA for systems which collect, maintain, or disseminate information in an identifiable form, which is defined as "any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means." (P.L. 107-347)

provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

3. Purpose Specification: DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used and shared.
4. Data Minimization: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).
5. Use Limitation: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department is limited to purposes compatible with the purpose for which the PII was collected.
6. Data Quality and Integrity: DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.
7. Security: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
8. Accountability and Auditing: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

Second, although it is less relevant in this context, as a matter of policy the Privacy Office conducts PIAs on national security systems, which are exempted from the requirement under Title II of the E-Government Act (Section 202(i)); although, consistent with the need to protect the processes associated with national security, the Privacy Office refrains from publishing these PIAs on our public facing website, www.dhs.gov/privacy.

Armed with the authority of Section 222 of the Homeland Security Act, and mindful of the issues associated with commercial data, the Privacy Office implements the DPIAC recommendation that the Department conduct a PIA whenever there is a substantial risk of harm flowing from the use of commercial data, even if the use is exempt from the requirement under the E-Government.

Conclusion

The Privacy Office is committed to ensuring DHS programs are a success, both in terms of forwarding the critical law enforcement, counterterrorism, and fraud detection missions of the Department and the United States Government to ensure the safety and

well-being of our citizens, and equally in preserving the privacy protections the American public has a right to expect.

This will require close scrutiny of the use of PII, particularly when it is obtained from commercial information resellers. The Privacy Office will continue to use the Privacy Impact Assessment to examine the use of commercial data whenever it is required by the E-Government Act or under the authority of Section 222 of the Homeland Security Act, when even ad hoc use presents a substantial risk of harm.

In sum, the Privacy Office has taken a leadership role on the use of PII from commercial sources data benefiting what we have learned from our Advisory Committee, a public workshop, and robust implementation of Privacy Impact Assessments.

I thank the Subcommittee for this opportunity to testify about the use of commercial data at the Department and the steps we take to make sure it is used consistent with the Fair Information Practice Principles. I look forward to answering your questions.

Mr. CLAY. I will recognize Ranking Member Turner for 5 minutes.

Mr. TURNER. Thank you, Mr. Chairman. I want to thank each of you because you have outlined very clearly some of the dangers and problems that—is my mic on?

Mr. CLAY. Yes.

Mr. TURNER. Can you guys hear me? OK. Good. Because it doesn't sound like it's on.

You've outlined the dangers and concerns that individuals have about the privacy aspect of their personal information. But I'm going to ask you a question that really goes to the broader umbrella of how we have to be concerned, why we protect personal information that we don't commercially restrict, some important information gathering for our economy.

I want to tell you a story. I just recently took some people from my community on a tour of the Supreme Court building. And I had not been to the floor that had the library. And we walked into the library of the Supreme Court and here was this beautifully ornate room with all of these books and absolutely gorgeous and reverent to the point of the information that it contained—absolutely empty.

Now, I'm a member of the Supreme Court Bar but I've never been to the library and I'd not researched in the library. So I asked the librarian, has this always been empty? And they were telling us, no; but in fact, by the advent of technology, a library that used to be packed now has information that is readily accessible to others. And certainly in the area of law.

I know that we have had increased efficiency but also higher quality and that the level—the playing field has been leveled more among individuals seeking attorneys, that those attorneys might have access to information that could be vital to their case, as opposed to just hiring those that have the best research skills. We have people who are now more able to bring to bear in their case in their defense, or they are advocating information that's available to them.

I noted, Ms. Koontz, that in your GAO report—and it seems like I'm always referring to footnotes—but you have a footnote.

Ms. KOONTZ. That's where we put our best stuff.

Mr. TURNER. In footnote 7, when you cite that there's $30 million that is planned to be spent to purchase personal information, your footnote No. 7 says, this figure may include information that—uses that do not involve or include personal information. And you go down to cite LexisNexis and West, and LexisNexis is in my district. And of course being a lawyer, I've used both.

I would like each of you to speak for a moment on the issue of although we want to protect privacy, some of the things that we are actually seeking in a commercial marketplace where someone has taken the data information and reconfigured it for our use so that we can all do a better job of whatever we are doing; that our things that are just available in the library, how do we—how do we balance privacy and personal information without restricting things that we've seen in the law practice that actually makes the system work better?

Ms. KOONTZ. And I do think that this issue is all about balance. It's clear from our work that the information obtained from infor-

mation resellers is valuable to a number of agency functions, it's very important. But the balance then is that we have to do this within the context of personal privacy and with the laws and the guidance that we have now.

I just want to speak for a minute to that footnote. The footnote, we love to be very exacting. And in all cases we knew that information from—you know, services from LexisNexis, for example, are procured sort of in bulk. And so it wasn't—we weren't able—we were mostly able to sever the legal services sorts of things from the purchase of personal information. But there were a few places where we thought, well, there might be a small amount of that still in there. But I mean, generally speaking, I think we were able to put things in separate buckets. But we wanted to make the reader aware it's not down to the dollar, probably. So I think that this is general—you know, generally a good number.

But, again, that's what this is about, it is about balance. And I think that the PIA requirement, you know, is a very valuable way for agencies to think through how they're going to use information before they collect it, before they invest in information technology, and to look at the reason for collecting this information, any privacy risks that might present themselves and then come up with specific mitigation strategies. And this is a way of ensuring that we've done the right things in terms of privacy.

Mr. TURNER. Would you like to comment?

Ms. EVANS. Well, following off of your example, so looking at our guidance, we feel that the example that you gave, like LexisNexis, or looking at data for one-time use and querying into a system, is already covered. And so, you know, that would not necessarily require us to do or require, like LexisNexis, to do a privacy impact assessment. I believe the distinction that we are making, which GAO may agree or may not agree upon, is when we bring that data into a Federal system and we then start merging it in with other things that we are doing. That is where our guidance says where you're using it on a recurring basis, where it's more than just a one-time inquiry, like going into a library and looking at something, then you have to do the full privacy impact assessment. And that's where we are drawing the line with the commercial resellers, because you are bringing that information in, you're using it and you need to let the public know how you are using the information and where the source is coming from.

So in your example, we think our guidance allows for you to still go to the library. It's when you start taking the information from the library and bringing it back into your agency and using it on a recurring basis that you need to disclose to the public how you're doing that.

Mr. TURNER. I appreciate that, because that really is the other distinction, I'm looking to your No. 1 footnote. When you described what it is that we are talking about here for this type of information, you include things such as an individual's name, their date, place of birth, mother's maiden name, biometric records. You go on to talk about employment. And some of those things—excluding biometric information, obviously—are things that are available in the daily newspaper that may have been reported.

Ms. EVANS. Right.

Mr. TURNER. And we don't want our use, even commercial use of what would be in fact the evolution of our library, to also then be the same as data collection on the Federal Government.

Ms. EVANS. Right.

Mr. TURNER. And how do we do one without inhibiting what has become—what we have all become now used to as our sense of what a library is. Mr. Teufel.

Mr. TEUFEL. Sure. I'm a nonpracticing lawyer as well, and it's a wonderful thing. You know, no billable hours for one thing.

So what caught my eye as I went—as I was reading the legislation was—were the definitions. And I'm not sure that—the definition seemed to be broad and would include the uses of Lexis and Westlaw or Nexis. I think maybe there's a provision in the definitions that talks about news, news clippings services, or news reporting services. But when I think about Lexis and Nexis and Westlaw, I'm not necessarily thinking about the data bases of driver's license records, marriages and divorces. I'm thinking about—I need to look up a GSBCA ruling or a Federal circuit ruling or a 10th Circuit ruling, or other things that are more of the types of things that lawyers tend to look at, than my concern was this definition within the legislation so broad as to encompass those lawyer-types of uses. So that was a concern that came to my eye as I read the legislation.

Mr. TURNER. Thank you. Mr. Chairman.

Mr. CLAY. Thank you, Mr. Turner.

Ms. Evans, the April 2006 GAO report contained recommendations to OMB to clarify its guidance on the use of commercial data, yet nearly 2 years have passed and OMB has not taken steps to address its recommendations. Why hasn't OMB acted on this issue? And can we expect to see new guidance? And if so, when?

Ms. EVANS. Well, actually, we feel that we've taken the steps based on the actions that were identified by the President's Identity Theft Task Force, so we have issued additional guidance. We've also taken additional steps and asked the inspector generals to review the quality associated with Privacy Impact Assessments because we feel that's a very holistic approach in how the agencies look at it. We didn't issue guidance specifically for data commercial resellers because we were really looking at the program holistically.

But every year as we send the guidance out—the draft guidance which will come out again this spring, and we are adding new requirements in for privacy—we also solicit GAO's comments before it becomes final. So if they feel that the actions that we've taken to date since the time that they've issued that report, how we've improved, I believe, the quality and have the measures and have the IG looking at the privacy aspects of the programs, we can work with GAO to issue any further guidance if necessary at this point.

Mr. CLAY. Ms. Koontz, any response?

Ms. KOONTZ. I think what we've found in our work, that OMB's guidance says that agencies are to do a PIA if they systematically incorporate commercial data into existing data bases. The same guidance says if you merely query the data base, the reseller's data base, then that does not trigger the PIA requirement. And I think that our feeling was that there was a lot of room between system-

atic incorporation and merely querying a data base and that OMB's guidance can't go further to say, well, what does systematic incorporation mean? And when we went to agencies, they said, well, most of what we do is of the querying nature but sometimes we keep the queries, sometimes we keep the information. And that's somewhere in between, and we wanted more clarity around when—when agencies should do PIAs. And I think we were particularly concerned about the instance where the information was safe in that agency.

Mr. CLAY. Yes, sir.

Mr. TEUFEL. Well, I would refer the committee to our PIA guidance. And we asked the questions, how are you using the information? Are you keeping it or not? And when we have our conversations with programmatic personnel, we talk about these sorts of things. And so we—I mean, the big issue is the ad hoc or one-time querying use versus the systematic use and that necessarily entails judgment. We think we do a very good job in exercising judgment and discretion, and certainly with our authorities to conduct Privacy Impact Assessments, some may feel that sometimes we do more PIAs than are necessary. But we think that's an important thing because PIAs are part of the transparency process, letting the public know what it is that the Department's doing. So in an ideal world, there is trust and confidence in what the Department is doing, but also so that the public is informed, can make informed decisions and advise its elected representatives of where it wants government to go.

Mr. CLAY. Thank you.

Ms. Evans, OMB's PIA guidance from 2003 requires a PIA to be performed when an agency systematically incorporate information into their system; but then merely pinging or querying a data base does not require a PIA. Given the systematic use of this information by the Federal Government, why is this distinction necessary? Isn't the government using this information to inform decision-making?

Ms. EVANS. Well, and I think—well, the short answer is yes, you are using the information to inform decisions. But the example—I mean one example that I would give is, I also go out and do Google, and I Google information, and it comes up about a whole bunch of different things. But I don't incorporate the results of the Google search into a Federal information system.

We are making a distinction between the systems that the Federal Government manages, the information we manage, versus just a general type of query. The point, though, that GAO has made—and we could go back and look at this—and that my colleague Hugo has also made, is that it may not necessarily be a change to the guidance or the policy because the framework exists to allow flexibility for each agency head and how they use the information. But it might be more of a sharing of best practices.

Now, we do have a committee that we formalized off of the CIO Council that specifically deals with privacy practices. So some of the activities that DHS does and some of the other activities that the agencies do could help level the playing field across the board and share these best practices so that agencies then incorporate them into their existing ways that they then do their PIAs.

Mr. CLAY. Thank you.

Ms. Koontz, in its 2006 report, GAO identified instances in which the use of reseller information was either not identified in Federal Register notices or was identified only in vague terms.

In your opinion, why haven't agencies been identifying commercial resellers as a source of personal information?

Ms. KOONTZ. We thought that both the OMB guidance and the agency guidance were not clear on this particular point. And it may be simply that the guidance predates—substantial use of personal information obtained from resellers. And it's a case of perhaps the guidance needs to catch up with what the current practice is.

Mr. CLAY. OK. And Mr. Teufel, the information contained in the 2006 GAO report on this subject is based on fiscal year 2005 contracts with information sellers. Can you tell us what the value of DHS's contracts with the information resellers was for years—fiscal years 2006 and 2007?

Mr. TEUFEL. I'm sorry, sir. I don't have that information available but I would be happy to get back to the committee with that information.

Mr. CLAY. OK. And you'll provide the committee with that?

Mr. TEUFEL. I'll do my best, sir.

[The information referred to follows:]

Please be advised that the Chairman and Staff Director have extended time until 5:00 p.m., Monday, April 1, 2008. The record will be closed and a statement will be placed in with the email from you on 03208 with no further response to our last email to you.

Jean A. Gosa
Clerk

From: Gosa, Jean
Sent: Thursday, March 20, 2008 11:35 AM
To: 'Readinger, Jeff'; Piggee, Darryl; Mitchell, Michelle
Cc: Gosa, Jean
Subject: RE: Response due tomorrow Tuesday, March 18th, 2008 IP Hearing Record

You state in your response "it will take some time?" Is there a tiime frame?

Jean A. Gosa
Clerk

-----Original Message-----
From: Readinger, Jeff [mailto:jeff.readinger@dhs.gov]
Sent: Wednesday, March 19, 2008 10:33 AM
To: Gosa, Jean; Piggee, Darryl; Mitchell, Michelle
Cc: Bordes, Adam
Subject: RE: Response due tomorrow Tuesday, March 18th, 2008 IP Hearing Record

All,
After the hearing we sent the "get back" request the DHS Chief Procurement Officer to ask for the data to respond to the Chairman. It is involving a "data call" across the department and I understand it will take some time. We can not meet the five days for the record, but once we get the information we will provide it to the committee.

Also, I'm not at my desk due to computer problems but the best way to reach me is via cell phone 202-557-5234.

Jeffrey T. Readinger
Office of Legislative Affairs
U.S. Department of Homeland Security
202-447-5462

-----Original Message-----
From: Gosa, Jean [mailto:Jean.Gosa@mail.house.gov]
Sent: Wednesday, March 19, 2008 9:01 AM
To: Piggee, Darryl; Mitchell, Michelle
Cc: Readinger, Jeffrey T
Subject: Response due tomorrow Tuesday, March 18th, 2008 IP Hearing Record

A follow-up response was due in yesterday, Tuesday, March 18, 2008 from DHS by
Mr. Readinger (Staff). Hugo Teufel III, follow-up response to questions Chairman Clay asked (hearing date March 11, 2008) regarding the value of DHS's contracts with the information resellers FY 06 & 07. (Please see email from Adam that Mr. Readinger would have the information into the office yesterday).

I have had no correspondence nor phone call from Mr. Readinger and the transcript is ready to be turned in to be printed. In the transcript it can reflect that the witness failed to answer questions posed by the Chairman even though staff (Mr. Readinger) stated that the response would be emailed to me directly by 03/18/08., and go forward turning the transcript in for printing.

Jean A. Gosa
Clerk
-----Original Message-----
From: Bordes, Adam
Sent: Monday, March 17, 2008 1:17 PM
To: Gosa, Jean
Subject: Re: Response due tomorrow Tuesday, March 18th, 2008 IP Hearing Record

I did. He knows tomorrow

Sent from my BlackBerry Wireless Handheld

----- Original Message -----
From: Gosa, Jean
To: Bordes, Adam
Cc: Piggee, Darryl; Mitchell, Michelle
Sent: Mon Mar 17 12:35:52 2008
Subject: RE: Response due tomorrow Tuesday, March 18th, 2008 IP Hearing Record

When you spoke to him did you advise him it's due tomorrow?

From: Bordes, Adam
Sent: Monday, March 17, 2008 12:09 PM
To: Gosa, Jean
Subject: RE: Response due tomorrow Tuesday, March 18th, 2008 IP Hearing Record

I called Jeff Readinger at DHS leg affairs. He's been asked to submit the info directly to you. His number is 202-447-5890 and email is jeff.readinger@dhs.gov

---

From: Gosa, Jean
Sent: Monday, March 17, 2008 11:30 AM
To: Bordes, Adam
Cc: Piggee, Darryl; Mitchell, Michelle
Subject: Response due tomorrow Tuesday, March 18th, 2008 IP Hearing Record

Importance: High

Adam,

Please contact the staffer you were in contact regarding: Hugo Teufel 031108 regarding the above attachment.

Jean A. Gosa
Clerk

Mr. CLAY. OK. Is it fair to say that the 2006 GAO report still accurately characterizes DHS's use of information reseller data? Have there been significant privacy improvements made that we should know about?

Mr. TEUFEL. Well, sir, I think other than the numbers being different, I think the report probably does a pretty good job of describing things at the Department. That commercial information is used by—I'm guessing all, I'm trying to recall now—almost all, if not all, of the seven operational components and some of the Department-Level components.

We've been doing a pretty good job of privacy. And since that report came out, we've made some improvements in how we do privacy. We are updating the legacy agency system of records notices. We've added to our Privacy Impact Assessment Guidance on how the Department handles commercial information. So so we've made improvements. We were doing a good job before. We are doing a better job today.

Mr. CLAY. Mr. Turner, you are recognized.

Mr. TURNER. Another issue that I'd like you to address that we should be concerned about is there are things that we do want our government to know. Whenever anything of significance happens, one of the first questions that you always hear from any reporter is, why didn't the government know? The government is expected to have knowledge of basic current events that we are all aware of, and then some information that might lead to issues of threat.

Certainly issues that are publicly available that might pose—information from which decisionmaking should occur. How do we balance making certain that we don't inhibit or discourage the data brokers or resellers from doing business or providing information to the Federal Government?

Ms. KOONTZ. I think if we talk about the kinds of recommendations that we made in our report, which were for Federal agencies to be very specific and forthright in notifying the public about their use of commercial data and also our suggestion that OMB clarify the guidance so we know when PIAs are required; admittedly, I think we have a sense that we would like to see PIAs done more frequently and for agencies to think through the use of this information before before they acquire it from virtually any source. But—and I think that none of these sorts of things that are intended for privacy would inhibit resellers from doing business with the government or providing the information that they provide now.

Even the bill that we are looking at today doesn't place any new obligations on resellers. It says it's—instead it asks—asks the Federal Government, as it is obligated to, to think through very carefully how they're going to use this information, and how they're going to protect it also. So I don't see it as an inhibiting factor.

Mr. TURNER. Any other thoughts?

Ms. EVANS. First and foremost, I'd like to clarify one thing. I think just because we haven't issued an updated policy doesn't mean that we are focusing on the use of the information and how the agencies do Privacy Impact Assessments. I would say that the administration has really stepped up its efforts in this area as we continue with the implementation of the E-Gov Act and as we've

built out on the foundation of what a Privacy Impact Assessment is supposed to be.

So we have issued subsequent guidance to the agencies dealing with privacy information, how they collect information, what their systems are doing and for them to go back and look at it. We followup on this on a quarterly basis through the President's management agenda. So we track what the agencies are doing, what they said they're doing, how they're using the information. And we track the number of Privacy Impact Assessments, Systems of Records of Notice, what they say they're going to do, how you match that against everything that they're doing.

So we have issued guidance in the bigger, broader aspect of information protection, information security and privacy. Not to this specific issue of commercial resellers, because we think that they need to look at this in a holistic way of how they're doing everything, not just necessarily narrowly focused on the use of commercial resellers.

I don't think that what we are doing when you bring the information into the Federal Government would prohibit data brokers from working with the Federal Government. But I do agree with GAO that the agencies need to be very transparent about how we are using information to make sure that the public has the ability to comment on that.

Mr. TEUFEL. Rigorous application of the fair information practice principles.

Mr. TURNER. One question that personally triggered me, you were talking about Google. And there's been some discussion on systematic use versus pinging. I have a question for you; this is for my own personal information. How do those distinctions fall within—I understand one computer doing 100 searches on the same thing. But what if 100 computers are doing the searches on the same thing? How does that get balanced?

Like I'll give you an example. I won't use the Mayflower Hotel as an example. But we have a satellite that is coming into orbit and we are going to hit it down with an Aegis system. I'm assuming that there are a number of computers, as that current event was happening, was doing an inquiry similar on public records and information for that. So you have a number of computers all focused on the same current event that has happened versus one computer that is trying to determine as much information about a narrow topic.

How does that affect you? You have a number of agencies perhaps with the same needs for the same information. How does that affect the analysis? The distinction between systematic and pinging?

Ms. EVANS. OK. So I'm going to try and not get real technical here. But let's focus on the agency and the use of the agency. And this is one of the reasons why we always talk about trying to keep things technology-neutral, just based on the example that you gave.

I think the distinction here in GAO, Ms. Koontz has laid this out, is it's one thing when 1 agency or 100 agencies go and ask a question. It's what you do with the results of that question. And if you store that result back into a Federal information system is when all of these triggers then happen.

If I go out and I look at that satellite, but I don't do anything with the information, it's for informational purposes and I'm looking, it doesn't matter whether 1 person did it or 100 people did it. It makes a difference if one person, like, searches on you, and then I take that information in and now I store it in a Federal system and I start using it in conjunction with other information I have. That's when it's important for the Federal agency to say how they're using the information, what they're storing and how they're retrieving it. That's the Privacy Act implications of when you do the Systems of Records Notice, and then that is the PIA piece, Privacy Impact Assessment.

Do you want to add anything?

Ms. KOONTZ. I'll just add that there is definitely an issue here about whether we make decisions on the basis of storing information or we make decisions based on how we use information. And I think that it would be fair to say that the PIA guidance right now is more based on the storage model; that if we are going to bring it in and systematically incorporate—although I would say I'm not sure what systematically incorporate means versus incorporate versus somehow keep the information—but the point is is that even if I ping a data base and I—I have existing data and I confirm that an address I have is—I think that's now the correct address because I have—I have corroborating information now. I am using that information despite the fact I'm not, quote, bringing it in or incorporating it into any kind of data base, but I'm using that as part of my decisionmaking ability. And I think that's one of the things that we need to look at going forward, concerning how we approach the use of reseller information from the Federal Government.

Mr. TEUFEL. Well, when we mentioned satellite, I thought we were going to be talking about another DHS program. But we are not. Its use. I mean, it's all about use. Your example sounded more like situational awareness with the hundred computers as opposed to information that was mission-essential for the conduct of the operation of that particular agency's use.

Mr. TURNER. Your descriptions have been very helpful. Thank you, Mr. Chairman.

Mr. CLAY. This is a panel-wide question. Should information resellers that are governed under the Fair Credit Reporting Act and Gramm-Leach-Bliley Act be exempted from requirements in the proposed Federal Agency Data Protection Act? Why or why not? We'll start with Ms. Evans.

Ms. EVANS. Those particular acts are covered by the FTC and how they use that. I would not feel that it would be appropriate for me to answer that question right now. What I would rather do is take it for the record and be able to go back and discuss it more specifically with the FTC on that.

Mr. CLAY. Yes. That's right. Thank you, Ms. Evans. Ms. Koontz.

Ms. KOONTZ. We do not think it's appropriate to exempt any data source, any specific data source, from the proposed provisions of the bill if it passes. Our feeling is that what this does is to bring the treatment of reseller information—the requirements into line with how we treat other information sources as well.

I also would question to some extent what the basis or the rationale would be for exempting—making exemption for Federal agencies not to do PIAs because resellers are covered by the two laws that you mentioned. These two laws do place restrictions on resellers' use and collection and disclosure of certain kinds of consumer and financial information. But I don't—you know, despite these requirements, I wouldn't think that would mean that we would be any less interested in having Federal agencies critically think through their use of commercial data.

Mr. CLAY. Thank you for that response.

Mr. Teufel.

Mr. TEUFEL. I'm with Karen. I'm very hesitant to answer the question without the benefit of guidance from FTC.

Mr. CLAY. OK. Let me start with you. Shouldn't we also be looking to add greater privacy safeguards with personal information that is shared with us by all nongovernmental sources such as employers, contractors, banks, etc.?

Mr. TEUFEL. Well, sir, I think at DHS we do that.

Mr. CLAY. You do it now?

Mr. TEUFEL. Certainly there's always room for improvement. But I think at DHS, as I'm thinking through the various programs at the Department and how we handle that with our PIA process, our SORN process and other things that we have in place, I think we do a pretty good job of protecting the privacy of individuals when we've obtained that information from non-Federal sources.

Mr. CLAY. Ms. Koontz, how about adding greater privacy?

Ms. KOONTZ. I think that there's a recognition that we need to protect personally identifiable information regardless of source. There are a number of laws, of course, that seek to do just that, and we haven't evaluated the efficacy of all those requirements. But I do think that it's important for the Federal Government to pay particular attention to personal information that's obtained from third-party resources—third-party sources, rather than from the individual themselves.

Mr. CLAY. Thank you. Ms. Evans, any comment?

Ms. EVANS. The President's Identity Theft Task Force did look at both the Federal Government as well as private industry. There were several recommendations that were made by the task force. My office was responsible for the Federal Government portion of implementing those recommendations. That group is chaired by the FTC and the Department of Justice and we are going to be issuing an update this spring, which I believe is next month, April, to where exactly we are in the progress that we've made on all the recommendations. So as soon as that report is out, I'd be happy to share that with the committee so that you can see, because it's full encompassing, private sector as well as public sector.

Mr. CLAY. Very good. We are very interested in seeing that. And let me thank this entire panel for your responses and your expert testimony. Panel one is dismissed. Thank you.

Mr. TEUFEL. Thank you.

Ms. EVANS. Thank you.

Mr. CLAY. The committee will recess for 15 minutes and we'll return with panel two when we come back.

[Recess.]

Mr. CLAY. We will now have our second panel.

And that panel will include Mr. Ari Schwartz, who is the vice president and chief operating officer of the Center for Democracy and Technology. This work focuses on increasing individual control over personal and public information by promoting privacy protection in the digital age and expanding access to Government information via the Internet.

Welcome, Mr. Schwartz.

We also have on the panel Mr. Stuart Pratt, who is the CEO of the Consumer Data Industry Association, an international trade association representing the consumer information industry. 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.

Thank you for being here, Mr. Pratt.

And our third witness, Ms. Paula Bruening, is deputy executive director of the Center for Information Policy Leadership at Hunton & Williams. At the center, she focuses on global, cyber privacy issues, as well as a frequent author and lecturer on information policy issues throughout the United States and Europe.

And welcome.

And I welcome you all.

It is the policy of the subcommittee to swear in all witnesses before they testify. At this time, I would ask that you all stand and raise your right hand.

[Witnesses sworn.]

Mr. CLAY. Let the record reflect that all the witnesses answered in the affirmative.

I would ask that each witness now give an oral summary of his or her testimony, and to keep this summary under 5 minutes in duration. Bear in mind your complete written statement will be included in the hearing record.

Mr. Schwartz, we will begin with you.

STATEMENTS OF ARI SCHWARTZ, DEPUTY DIRECTOR, CENTER FOR DEMOCRACY AND TECHNOLOGY; STUART PRATT, PRESIDENT, CONSUMER DATA INDUSTRY ASSOCIATION; AND PAULA J. BRUENING, DEPUTY DIRECTOR, CENTER FOR INFORMATION POLICY LEADERSHIP

STATEMENT OF ARI SCHWARTZ

Mr. SCHWARTZ. Chairman Clay, thank you for holding a public hearing on this important privacy issue and for inviting me to participate.

Government's use of personal information is key to the functioning of many of its most essential programs, from determining eligibility for benefits to supporting law enforcement investigations. As the information economy grows, more personal information is being provided from commercial data brokers, who aggregate and categorize this information for a wide range of purposes to the private and Government sectors alike.

As with any organization, Government agencies must take the management responsibility to ensure that their partners and em-

ployees are meeting standards of care and use of that information. In this case, there are many concerns that come from the use of personal data. Creating guidelines is a sensible and needed approach. Simply put, Congress should ensure that Americans do not lose privacy, security and quality protections that are already a part of law and policy only because a Government agency is using a private-sector data partner rather than to have the agency collect it themselves.

The chairman's bill, H.R. 4791, would move the agencies in the right direction by requiring agencies to make important management considerations, by requiring the vetting of commercial partners through the privacy impact assessment [PIA] process. The PIA requirement, which passed as part of the E-Government Act, was designed to provide greater transparency to how the Government collects and uses personal information. Over the past 6 years, PIAs have become an essential tool to help protect privacy. Mr. Teufel, on the previous panel, called one of them the three pillars of the U.S. Government privacy policy.

However, as evidenced by OMB's FISMA report to Congress last month, the Federal Government has unevenly implemented the PIA process across agencies. The guidance issued pursuant to the act with respect to PIAs was vague and has simply not provided the agencies with the tools they need to successfully implement the PIA process unless they already had privacy experts on staff.

While some agencies, like the Department of Homeland Security, have set high quality standards for the PIAs and have continued to improve them over time, the lack of clear guidance has led some agencies, such as the State Department, to create cursory PIAs or others, such as the Department of Defense, to have none at all. We, therefore, urge Congress to also require that OMB create a set of best practices for PIAs while it is updating the PIA guidance to cover agency use of any commercial partner.

Even then, the transparency provided by the PIA process must not be viewed as a full solution for privacy. Congress must begin to address more fundamental privacy issues within Government agencies to ensure the trust of the American people. This should begin with a review of the Privacy Act of 1974.

In 2000, the full committee passed a bill, sponsored by Ranking Member Davis and Representative Moran, to create a commission that would study the state of the Privacy Act and recommend updates to the law. The record shows that, even 8 years ago, it was clear that this important law, the most direct legal protections that citizens have over the Federal Governments's regular use of information, was beginning to erode due to unforeseen advances in technology. We hope that the committee will once again take up a review of the Privacy Act to help protect the privacy of Americans into the future.

We look forward to working with this subcommittee to help address these critical privacy issues in more detail in the near the future, and we thank you for your leadership on this important issue. I look forward to your questions.

[The prepared statement of Mr. Schwartz follows:]

1634 I Street, NW Suite 1100
Washington, DC 20006
202.637.9800
fax 202.637.0968
http://www.cdt.org

Statement of Ari Schwartz

Deputy Director

Center for Democracy & Technology

before the

House Committee on Oversight and Government Affairs

Subcommittee on Information Policy, Census, and National Archives

on

Privacy: The Use of Commercial Information Resellers by Federal Agencies

March 11, 2008

Chairman Clay, Ranking Member Turner and members of the Subcommittee, thank you for holding this hearing on the privacy concerns with federal agencies' use of personal information provided by commercial resellers.

CDT is a non-profit public interest organization founded in 1994 to promote democratic values and individual liberties for the digital age. CDT works to keep the Internet open, innovative and free by developing practical, real-world solutions that enhance free expression, privacy, universal access and democratic participation.

Government's Growing Use of Commercial Databases

The federal government's increasing use of technology has led to important advancements in government efficiency and productivity. It should come as no surprise that the federal government now processes more personal information about individuals than ever before. The government uses this information in many of its most essential programs, from determining eligibility for benefits to supporting law enforcement investigations.

The government not only collects personally identifiable information directly, it also buys information from commercial entities. An important category of this information is drawn from public records at courthouses and other government agencies. The companies sometimes known as data brokers provide a valuable service to the private and government sectors alike by aggregating and categorizing this information. Commercial data services companies also compile personally identifiable information that is not publicly available. This non-public, but commercially available data includes, for example, credit reporting information. Depending on the context, it may also include a broad range of other data generated by individuals in the course of commercial transactions, online and off. One of the questions that should be explored by this Subcommittee is exactly what are the types of information that the government subscribes to or otherwise acquires from commercial aggregators and resellers.

While data brokers provide important services to the government and the private sector, the collection and aggregation of personally identifiable information also raises a host of privacy issues and concerns about the accuracy, reliability and security of this information. Security breaches at all of the major data brokers have prompted calls for examination of security standards for this evolving industry. The rules that for the federal government's use of commercial databases have been vague and sometimes non-existent. The Privacy Act of 1974 was supposed to subject government agencies that collect personally identifiable information to the fair information practices, but the Act's

protections only apply to federal "systems of records."[1] That means that the government may be able to bypass the protections of the Privacy Act by accessing existing private sector databases, rather than collecting the information itself.

Updating the Privacy Act of 1974

The Privacy Act of 1974 is the primary law regulating the federal government's use of personal information. The Act regulates federal agencies' collection, maintenance, use, and dissemination of personal information.

Among other provisions, the Act contains the following protections:

- **Prevention of secret systems of records.** Whenever an agency establishes or changes a system of records, it must publish in the Federal Register a notice known as a System of Records Notice (SORN). The notice must contain the name and location of the system, the categories of individuals on whom records are maintained in the system, the uses of the system, and other information.

- **Collection of only necessary information.** Under the Privacy Act, agencies are permitted to maintain personal information about an individual only when it is relevant and necessary to accomplish a purpose the agency is authorized to perform by statute or executive order. The goal of this provision is to reduce the risk of agencies' using personal information improperly and to avoid mission creep.

- **Ensuring data quality.** Agencies are required to maintain all records used in making any determination about individuals with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the

[1] The term "system of records" is defined as "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." 5 U.S.C. § 552a(a).

individual. This provision is specifically meant to protect against erroneous decisions.

- **Information security.** Agencies are required to establish appropriate administrative, technical, and physical security protections to ensure the confidentiality of records and to protect against anticipated threats or hazards to their security or integrity that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

- **Access and correction.** Individuals are entitled to obtain a copy of records about themselves and to request correction of any information that is not accurate, relevant, timely, or complete.

- **Accounting for disclosures.** Agencies must keep an accounting of the date, nature, and purpose of each disclosure of personal information to other agencies.

- **Training employees.** Agencies are required to provide training on the requirements of the Act to employees and contractors involved in the design, development, operation, or maintenance of any system of records.

- **Providing notice of exemptions.** Agencies are permitted to exempt certain categories of records from some of the Act's provisions, but before an agency can do so, it must do so by means of a process in which it justifies the exemption.

While the Privacy Act offers US citizens and permanent resident aliens important privacy protections and has been effective in raising awareness of privacy issues within the government and among the public at large, it is widely acknowledged that the Act is not being well enforced and that agencies lack proper guidance from the Office of Management and Budget (OMB), which has responsibilities for interpreting and overseeing the implementation of the Act. In June 2003, the Government Accountability

Office (GAO) issued a report that is still timely, entitled "Privacy Act: OMB Leadership Needed to Improve Agency Compliance." In that report, the GAO identified deficiencies in compliance with the Act and concluded: "If these implementation issues and the overall uneven compliance are not addressed, the government will not be able to provide the public with sufficient assurance that all legislated individual privacy rights are adequately protected."[2] Five years later, OMB has just begun to provide the kind of leadership that is needed to help agencies build programs to protect privacy as evidenced in the changes in its FISMA report to Congress.

While OMB leadership is welcomed, it is also increasingly clear that the Privacy Act itself is outdated and is in need of improvements to ensure its relevance into the future. The Act's limitations are particularly apparent with regard to government use of commercially-compiled personal information. Subsection (m) of the Act covers government contractors. It was designed to ensure that an agency could not simply contract away its responsibilities for privacy protection under the Act. Subsection (m) simply states that, when an agency provides by contract for the operation on behalf of the agency of a system of records to accomplish an agency function, the agency shall cause the Privacy Act to be applied to such system. Similarly, all employees of such a contractor are bound by the Act to the same extent that federal employees would be.

Situations involving Subsection (m) generally can be analyzed under categories:

1. **Private Collection Under Government Contract** — The Privacy Act as currently written clearly applies when the government contracts with a commercial entity to collect, maintain or analyze PII for use in carrying out a government function or program. The fact that the data is held by the commercial entity, and even the fact that no data ever enters government computers, makes no difference: all Privacy Act principles apply to the data in the private entity's computers that was collected *at the behest* of the government.

[2] http://www.gao.gov/new.items/d03304.pdf

While this application is clear, it may merit reaffirmation by the Committee and DHS.

2. **Receipt of Commercial Data** – It should also be clear that the Privacy Act applies when PII is transferred to the government or its contractors from the private sector. However, there seems to be a lack of clarity about this issue. Under the Act, as narrowly interpreted, no covered "system of records" exists unless the identifiable information is not just "searchable" by name or other identifier but is actually searched by such means on multiple occasions. For example, the DHS Inspector General examined cases where commercial data on millions of individuals was appended to passenger flight records from airlines and held by a government contractor or by the government itself. The IG said that the Privacy Act was not violated because "the airline passenger records were not maintained in such a way as to have required TSA to publish a Privacy Act system of records notice,"[3] presumably because data was not regularly searched on the basis of name. GAO disagreed and suggested that the Privacy Act may have been violated and the DHS Chief Privacy Officer ultimately agreed that the agency did, in fact, violate the Privacy Act.[4]

3. **Merging of Private Sector Data** — The Privacy Act should also apply when commercial data is brought into government databases. A new SORN should be

---

[3] "Review of the Transportation Security Administration's Role in the Use and Dissemination of Airline Passenger Data," (Redacted), OIG-05-12, March 2005 http://www.dhs.gov/dhspublic/interweb/assetlibrary/OIGr-05-12_Mar05.pdf, at p. 45.

[4] 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" Memo to Congressional Committees, July 22, 2005, http://www.gao.gov/new.items/d05864r.pdf,
CDT Policy Post, "JetBlue Case," Volume 9, Number 20, October 17, 2003, http://www.cdt.org/publications/pp_9.20.shtml.
Privacy Office, Department of Homeland Security, "Secure Flight Report," December, 2006/ http://www.cdt.org/security/20061222secure.pdf,

issued whenever contractor databases containing private sector data are used to augment existing systems of records housed by the government or its contractors.

4. **Direct Use of Private Sector Data** — The greatest lack of clarity about whether the Act applies to commercial databases used by the government occurs when: 1) the database was not created at the government's behest; 2) the database remains in the control of the contractor; and 3) is queried by the government remotely. In our view, this question should be resolved in favor of Privacy Act application. The Act's goals are clearly relevant, since decisions are being made about individuals based on the information in the commercial database.

Agencies seem confused by these different situations and there is a concern that agency officials and government contractors are using this confusion to ignore or subvert the Privacy Act. At the least, application of the privacy Act to each of the scenarios set out above should be clearly spelled out in guidance to the agencies.

Improving Privacy Impact Assessments

Important steps toward updating government privacy policy were taken with the passage of the E-Government Act and efforts toward its effective implementation. Section 208 of the Act was specifically designed to "ensure sufficient protections for the privacy of personal information."[5] Section 208 was intended to increase transparency about how the government collects, manages and uses personal information about individuals through Web privacy notices and privacy impact assessments (PIAs).

Section 208 of the E-Government Act requires that agencies perform PIAs before adopting new technology or using collections of personally identifiable information. These PIAs are public documents, containing a description of the project, a risk assessment, a discussion of potential threats to privacy, and ways to mitigate those risks.

---

[5] PL 107-347, Section 208.

PIAs ensure that privacy concerns are considered as part of the design of information systems, and that the public has access to this element of the decision making process.

Over the past five years, PIAs have become an essential tool to help protect privacy. They are sometimes called "one of the three pillars" of the US government privacy policy.[6] Unfortunately, as with the other privacy laws, the federal government has unevenly implemented even the basic transparency requirement of PIAs across agencies.

The recent OMB FISMA report to Congress highlighted the fact that agencies range from "excellent" to "failing" in their implementations of the PIA requirement.[7] This wide range of compliance is partially due to the fact that the guidance issued by OMB with respect to PIAs is vague and has simply not provided agencies with the tools they need to successfully implement the PIA requirement. While some agencies, like the Department of Homeland Security (DHS),[8] have set a high standard for the quality of their PIAs and have continued to improve them over time, the lack of clear guidance has led other agencies to conduct cursory PIAs or none at all. For example, even though the use of RFID in passports has major privacy implications, the US Department of State gave the issue only cursory consideration in its PIA, a document of only ten sentences.[9]

---

[6] DHS Chief Privacy Officer Hugo Teuffel, *Presentation before the European Commission's Conference on Public Security, Privacy and Technology,* November 20, 2007 Brussels, Belgium. Mr. Teuffel suggested that the three current pillars are the Privacy Act of 1974, Section 208 of the E-Government Act and the Freedom of Information Act.

[7] Office of Management and Budget, "Fiscal Year 2007 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002."

[8] The DHS Website on Privacy Impact Assessment offers a range of resources to DHS components and to other agencies — http://www.dhs.gov/xinfoshare/publications/editorial_0511.shtm.

[9] http://foia.state.gov/SPIAS/20061.DOS.PIA.Summary.Passport-cleared.pdf Also see CDT's letter May 2, 2007 letter to Secretary of State Rice on the agencies failure to provide adequate PIAs for this and a related project — http://www.cdt.org/security/identity/20070502rice.pdf.

Even more troubling is the finding that some agencies simply do not perform PIAs on as many as half their qualifying technologies.[10] An official at the Department of Defense, which received a failing mark in the FISMA report, suggested to CDT that PIAs are still just not considered a priority there and are not taken seriously as an important tool for identifying and addressing privacy and security issues. Moreover, even those agencies that prepare in depth PIAs too often complete them after a project has been developed and approved. PIAs are supposed to inform the decision making process, not ratify it.

While OMB has begun to take steps to address the inconsistent implementation of PIAs, it should be of great concern to this Subcommittee that some agencies are still not conducting PIAs in a timely and comprehensive manner. The work of those agencies that have taken seriously the mandate to develop PIAs and used them as a tool for analysis and change should be a starting point for developing best practices for all federal agencies. The E-Government Act Reauthorization Act (S.2321) currently in front of the Senate includes a provision that would help address these concerns by specifically requiring OMB to create best practices for PIAs across the government. CDT urges the Subcommittee to add this best practice language to H.R. 4791 e.

Another major weakness in Section 208 is that it did not specifically require PIAs for government access to private sector data, and the OMB guidelines allow agencies to exempt the government's use of private sector databases from the requirement to conduct PIAs when they are not "systematically incorporated" into existing databases of information. CDT believes that this permissive approach is wrong. Different companies that provide private sector data to the government have different security and privacy practices. Government agencies should use the PIA process to take those issues into account when making decisions about the use of commercial data. Notably, some

---

[10] OMB FY2006 Report to Congress on Implementation of the Federal Information Security Management Act of 2002, at www.whitehouse.gov/omb/inforegreports/2006_fisma_report.pdf. In the 2007 report, OMB suggested that progress has been made because more systems have been identified as qualifying for PIAs even though the percentage of completed PIAs has not increased. CDT agrees with this assessment and applauds OMB on this progress as a major step toward better implementation despite the fact that the numbers show little progress.

agencies are conducting PIAs for uses of commercial data even when the data is not integrated into existing databases.

H.R. 4791 would clarify this issue and bring all agencies in line with the best practices of those agencies that have chosen to conduct PIAs for non-integrated data sources when they are used with regularity. CDT supports this change and hopes that the Committee will pass this important provision.

Conclusion

Commercial information can and should play a key role in important government functions including law enforcement and national security investigations. However, agencies relying on that data should have clear guidelines for its use—guidelines that both protect individual rights and ensure the information is reliable for the government purpose for which it is proposed to be used. Considering the harms that can occur when the government makes decisions about individuals based on inaccurate or irrelevant data, it is imperative that the federal government develop better and more consistent rules for use of commercial data to make decisions about individuals, regardless of whether the data is stored on government computers or stored on commercial systems.

Today, PIAs are playing an essential, albeit uneven role, in ensuring that our privacy is protected by government agencies. The amendments that will create best practices for PIAs (included in S.2321) and require PIAs for government use of commercial databases (included in HR 4791 will help to insure that PIAs are implemented consistently.

Even then, the transparency provided by PIAs must not be viewed as a full solution. Congress needs to begin to address more fundamental privacy issues within government agencies to ensure the trust of the American people. This should begin with a review of the Privacy Act of 1974 and a look into whether the law is adequate to address how the federal government today is using personal information. In testimony last month, Bruce McConnell suggested that the committee revisit the idea of a Commission to study

reforms to the Privacy Act.[11] We support this proposal and would also like to point out that Ranking Member Davis introduced a bill to create such a Commission in 2000.[12]

We look forward to working with this committee to help address these critical privacy issues in more detail in the near future.

---

[11] http://governmentmanagement.oversight.house.gov/documents/20080214132027.pdf

[12] Privacy Commission Act, H.R. 4049 (Reported in House), 106th Congress, 2nd Sess. (2000). CDT testified in support of this legislation — http://www.cdt.org/testimony/000412schwartz.shtml.

Mr. CLAY. Thank you so much, Mr. Schwartz.

Mr. Pratt, you are recognized for 5 minutes.

STATEMENT OF STUART PRATT

Mr. PRATT. Thank you, Mr. Chairman, for this opportunity to appear before you today.

Government's use of CDIA member products brings value to citizens individually and to Government, which works on their behalf. This is an important context, I think, for the committee as it considers H.R. 4791. Let me just share a couple of examples of how products are used and, really, the logic behind these.

Our members provide products which help Government agencies to enforce child support enforcement orders, to locate missing and exploited children, to prevent entitlement fraud, to provide background screening for employment and security clearances, to assist with various natural disasters, and also with witness location and with various law enforcement investigations.

Equally important, I think, to the context of our discussion today is the fact that these many products that I've just described are heavily regulated under a range of current Federal laws. And these laws affect both the public and the private sector. Two laws that are particularly important, I think, for today are the Fair Credit Reporting Act and the Gramm-Leach-Bliley Act, which have already been mentioned in the first panel.

H.R. 4791 proposes to improve Government's effort to protect personal information and to ensure that citizens are notified when personal information is lost. Actually, both of these goals make a lot of sense for us. Our members live under data security requirements today. Our members live under breach notification requirements today. And so, having those apply to the Government in the same way that they would apply to the private sector makes all the sense in the world.

Our written comments provide some thoughts on how you might tailor those provisions just a little bit to make sure that they are very effective. But, overall, those are good ideas.

The bill also proposes privacy impact assessments and certain contractual requirements where the Government obtains data from an entity, termed a "data broker." And this is really some new territory that is being built within this proposal. And we understand the importance of this focus on governmental uses to ensure there is a trust between Government and its citizens. And that really goes all the way back to the Privacy Act.

In this case, though, is seems to us perhaps the question is where the data is regulated, or where the data is not regulated—in other words, where is the trust, and how do consumers feel about their personal information being used by Government.

In the case of our members' products, the bridge of trust already exists through existing laws. And it is for this reason that we urge the committee to exclude from the definition of "data broker" entities that are subject to the Gramm-Leach-Bliley Act privacy rules, consumer reporting agencies regulated under the Fair Credit Reporting Act, and publicly available data sources provided by the private sector.

And our reasons for this are several. For example, the contract requirements in this proposal stipulate that a Government agency must obtain data from a data broker, and they appear to assume that data is unregulated. Further, the contract would, for example, impose an accuracy requirement on a consumer reporting agency which already has an accuracy requirement under the Fair Credit Reporting Act.

So, Mr. Chairman, here, perhaps, it's just an alignment question. You already have a Federal law. The Government is going to purchase data that's already under an accuracy standard. And then the question is, how would the contractual accuracy standard interplay with the standard of law that's already provided for under the Fair Credit Reporting Act?

The contractual provisions also would impose, more or less, a one-size-fits-all approach to the concept of—well, let me just back up here—would also provide a one-size-fits-all to location tools. And a location tool is a tool that's used to try to find a noncustodial parent to enforce a child support enforcement order. That's not really an accuracy tool or a tool based on accuracy, but it's a way to try to locate that individual and to get them to pay what they owe in delinquent child support. So, again, here maybe the one-size-fits-all approach of the accuracy requirement might go a little outside of the bounds of where you might like it to be at the end of the day.

The concept of a privacy impact assessment is sound, there is no doubt about it, and it's appropriate to Government processes. However, we think that requiring a PIA across the board may well have some adverse effects. For example, will Government continue to use the private-sector tools for skip tracing where a consumer hasn't paid his student loan if the PIA requirements are highly restrictive? Where the Government is a user, defined under the Fair Credit Reporting Act, and is using a consumer report for background screening, is there a need for a privacy impact assessment, when the Government is regulated under the FCRA, as is the private sector?

So, Mr. Chairman, in conclusion, there seem to be a lot of good ideas in this proposal that you have put together. I think there may be some places where we have other good laws already on the books. Some of these laws come from other committees on which you serve, as well. And here today, we're just offering some thoughts on how we might be able to more effectively align current Federal laws with the ideas that you have in this bill.

And, with that, I will look forward to your questions. Thank you.

[The prepared statement of Mr. Pratt follows:]

STATEMENT OF STUART K. PRATT

CONSUMER DATA INDUSTRY ASSOCIATION

WASHINGTON, D.C.

Hearing on

"Privacy: the Use of Commercial Information Resellers by Federal Agencies"

Subcommittee on Information Policy, Census and National Archives

Committee on Oversight and Government Reform

United States House of Representatives

Washington, D.C.

Tuesday, March 11, 2008

Chairman Clay, Ranking Member Turner and Members of this Subcommittee, thank you for the opportunity to appear before you here today.

My name is Stuart Pratt, and I am President and CEO of the Consumer Data Industry Association, CDIA. CDIA 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.

There are 3 main points that I plan to discuss with you this afternoon:

1) The Recognized value of CDIA members' systems;
2) CDIA members are heavily regulated, and their reasonable, lawful collection, use and sale of consumer data are governed by a wide variety of laws;
3) Comments on H.R 4791.

I) THE RECOGNIZED VALUE OF CDIA MEMBERS' SYSTEMS

First, I would like to discuss how the government uses our members' products and services. We believe this is an important context for the committee as it continues to consider action on H.R. 4791.

Government's use of CDIA member products brings value to citizens individually and to the government which works on their behalf. CDIA's members are the leading companies producing consumer data products and services for both the private and public sector. Consider the following examples of uses of our members' products and services:

- Assisting lenders, insurance companies, landlords and others to make risk-based decisions with relevant data about the individual applying for the benefit;
- Preventing money laundering and terrorist financing;

- Enforcing child support orders;[1]
- Working with the IRS to locate assets of tax evaders;
- Assisting law enforcement and private agencies locate missing and exploited children through location tools;
- Researching fugitives, such as determining assets held by individuals of interest through the use of investigative tools which allow law enforcement agencies to tie together disparate data on given individuals;
- Witness location;
- Entitlement fraud prevention, eligibility determinations, and identity verification;
- Background screening for employment and security clearances; and
- Disaster assistance.

Our prior testimony before the House Judiciary Committee in 2006, attached as Supplement A, goes through in detail what government representatives themselves have said about the value they derive from the use of consumer reporting agencies and other consumer data companies.

II) CDIA MEMBERS ARE HEAVILY REGULATED

Equal in importance to knowing that our members' products bring great value by ensuring tax payers' money is well-spent, that government resources are used effectively, that government databases are made more accurate, that fraud is reduced and that laws are fairly enforced all for the benefit of citizens is the fact that many of these products are heavily regulated under current federal laws. This, too, is important context as the committee considers the merits of H.R. 4791.

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

The federal government is also bound by these limitations, meaning that any data they obtain from regulated entities must be used only for specifically enumerated "permissible purposes" if the data is obtained from a consumer reporting agency, and subject to other limits if obtained from CDIA member companies regulated under Gramm-Leach-Bliley Act (GLB) or other laws.

Companies in our membership are not only subject to Section 5 of the FTC Act (unfairness and deception), and a range of state laws that regulate PII, but face significant federal regulations that govern many of their operations:

a) Fair Credit Reporting Act (FCRA)

It is important to note that not only was the Fair Credit Reporting Act enacted before 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, but it has also been the focus of careful oversight by the Congress, resulting in significant changes in both 1996 and again in 2003. There is no other law that is so current in ensuring consumer rights and protections are adequate.

The FCRA applies to both the private and public sectors, and thus is extremely relevant to today's discussion.

The FCRA 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, 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 to include or exclude a consumer is enormous. If a decision maker, including a government agency, uses a consumer report as a basis for denying a consumer a particular benefit, the consumer has the right to be notified when a consumer report has been used to take an adverse action, and he/she can obtain a free copy of his/her consumer report that was the basis of the decision.

The FCRA provides significant rights to consumers:

- The right of access:

Consumers have an absolute right at any time to obtain the disclosure of all information in their file at the time of the request. This right is enhanced by requirements that mandate free disclosure 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 may not have the means to pay. Further, for some specific companies – credit bureaus – consumers have a right to obtain their consumer report annually free of charge.

This right of access not only provides consumers with the opportunity to see information about them, but also provides them with the right to know who has seen or reviewed information in the consumer's file.

- The right of correction:

Consumers may dispute any information in the file free of charge, and there is a very short time frame to respond.

- Accuracy:

All such products are regulated for accuracy with a "reasonable procedures to ensure maximum possible accuracy" standard, a standard that was first enacted in 1970, and has withstood the test of time and two major revisions of the FCRA. 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 right to only have the data used for specific, enumerated purposes:

The FCRA enumerates very specific "permissible purposes" that a user of a consumer report can do with a consumer report, such as the provision of credit or employment. These limited uses protect consumers from broad disclosure and prevent the use of this data for marketing or other purposes.

- The right to a notice of all other rights:

With every disclosure of a file, consumers receive a notice providing a complete listing of all consumer rights.

b) Financial institutions under the Gramm-Leach-Bliley Act:

Outside of the FCRA, Congress has applied different standards of protection to data that are appropriate to the use and sensitivity of data. Similar to the FCRA, GLB establishes a number of restrictions on how data can be used, along with wide ranging privacy and data security standards. CDIA members produce and sell a range of fraud prevention (e.g., identity verification to prevent entitlement fraud) and location products (e.g. locating a non-custodial parent for purposes of enforcing a child support order) which are governed by other laws such as GLB.

III) COMMENTS ON H.R. 4791

Finally, we would like to comment on H.R. 4791, which touches on many of the issues we have raised today.

a) Role of "data broker" should not be primary focus; how government uses data is the relevant question.

There is a general misperception that this legislation carries forward: that all "data brokers" are unregulated, and possess vast amounts of data which may be used to profile consumers.

Instead, we believe that the Committee and this legislation should focus on whether the government legally obtained the information that it uses, for example by demonstrating that it had a permissible purpose for obtaining the data under the FCRA, and that it intended to use the data only for those limited purposes, and whether or not it actually followed those rules. In other words, if the government uses data that it obtains in lawful ways, and protects that data from unauthorized access and use, it should not matter whether the data was obtained from a public source or a regulated entity. On the other hand, if it misrepresents how it intends to use data, then that should be investigated.

We therefore believe the data broker provisions should be struck, and the proposed law should simply focus on the legal status of the data which is being acquired and then managed.

However, absent a willingness to take this step, we urge the Committee to exclude entities subject to the GLBA privacy rules and consumer reporting agencies regulated under FCRA (and all products produced therein), along with and distributors of publicly available data from the definition of data broker.

If, as discussed above, the goal of this legislation is to determine possibly unregulated uses of private sector data, then regulated entities are, by definition not contributing to this perceived problem, and should be exempted from these requirements. These time-tested statutes already protect consumers' information before it is provided to the government, and duplicative or contradictory requirements should not be imposed.

b) Requirements of this legislation are unnecessary and possibly inconsistent with current law for CDIA members

a. Privacy Impact Assessments (PIAs) are unnecessary in this context

As OMB has recognized, for regulated entities under GLB, the concept of a PIA does not make sense. Generally the products that we are referring to are simple look up services to find a non-custodial parent for purposes of child support enforcement or a delinquent government-backed student loan held by the Department of Education, or a tenant screen for a prospective HUD tenant, and OMB Guidance has explicitly exempted these types of services from PIA requirements.[2]

b. Section 9 requirements are inconsistent with current law

Many of the requirements of this Act that would place on regulated entities are inconsistent with FCRA and GLB, and thus could make compliance difficult. For instance, the accuracy standard for consumer reporting agencies, as discussed above, is "reasonable procedures to ensure maximum accuracy." The accuracy standard that would be required under this Act is fundamentally different, and could make it more difficult for consumer reporting agencies to comply. In fact, as discussed in our prior testimony, data

[2] Guidance given by the OMB in Memorandum M-03-22, paragraph f of Section II.B of Attachment A: "Commercial Sources - when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources. (*Merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement*)." (Emphasis added.)

provided to the federal government by CDIA members is generally *more accurate* than data the federal government collects itself or obtains from other sources.[3] Similarly, although the data security standard in the bill is similar to the GLB standard that regulated entities have to comply with, it is different enough that compliance could be complicated.

Therefore, for these additional reasons we have suggested exempting regulated entities from the coverage of this act – they already follow the standards that are equal to or more stringent than the standards that would be required by this legislation, so requiring them to comply with this additional program does not improve either data quality or consumer protections.

b) Data security/Data breach provisions

We agree that the government should secure data much as our members do today, and have advocated for the expansion of GLB Safeguards requirements beyond financial institutions. GAO reports suggest progress has been made, but also that more could be done (see "Information Security - Protecting Personally Identifiable Information - January 2008). It appears many agencies are taking more steps today and that current laws such as the Federal Information Security Management Act (FISMA), executive orders issued by OMB, and NIST technical standards establish prescriptive duties and provide helpful guidelines for implementation of data security.

Unfortunately, however, federal, state and local governments and educational institutions are the source of 60% of all data breaches. When governments and universities suffer

[3] Grace Mastalli, Principle Deputy Director for the Information Sharing and Collaboration Program for the Department of Homeland Security stated that CDIA-member products:

- are more accurate than government databases: "...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;"
- "in many respects, the commercial enterprises have done better jobs of organizing and, what I call 'cleaning' data to eliminate errors in data."

breaches, sensitive personally identifiable information is frequently lost, creating some risk of identity theft.

We agree the government should notify consumers where there is a breach of sensitive personal information (as opposed to just personal information). Consistent with the FTC, we believe that notification is appropriate where there is a significant risk of identity theft.

It is important to understand the role that CDIA members play after someone else has a breach. When a government entity, educational institution or private company suffers a data breach, CDIA members are usually called upon to help, even if they have absolutely no relationship with the breached entity, and often are forced to bear significant costs as a result of a breach with little or no opportunity to recoup costs. For instance, when a data breach notification is sent to consumers, the notice inevitably suggests that consumers call one of the three nation-wide credit bureaus. However, the credit bureaus are then often flooded with calls with little or no notice, and often have to scramble to ensure that their call centers are adequately staffed to deal with the increased demand. Further, consumers often expect that the credit bureau is going to know about the breach and have answers as to what happened and what their level of risk is, when the bureau may find out about the notification only through the increased call volume.

Therefore, we believe that it is appropriate to require the federal government to provide pre-notification to credit bureaus, so they can prepare for a possible increase in consumer calls, along with encouraging the federal government to offer remediation services, such as credit monitoring services, to consumers who are at increased risk of identity theft.

CDIA-member companies take identity theft and data security very seriously, and have been proactively on the cutting edge of developing a number of significant products and processes that help consumers and businesses protect themselves from identity theft, and mitigate its affects if it does occur.

For instance, CDIA member companies:

- have developed world-class tools for businesses to assist them in fraud detection and authentication efforts to help them identify fraud and ensure that the person that they are doing business with is indeed who they claim they are;
- pioneered the use of fraud alerts for consumers years before that idea was codified in the FACT Act in 2003;
- encouraged data furnishers to supply encrypted data;
- have developed credit monitoring and other services that enable consumers to proactively protect themselves from identity theft; and
- proactively established the availability for consumers to obtain a credit freeze across the country, even in states where the state legislature has not provided such an ability;

In part because of these tools, along with increased consumer education and awareness, including use of credit-file monitoring products that help consumers identify a problem while it is still easy to have it corrected, more vigorous law enforcement and more attention by the business community, including wider use of our members' fraud-prevention and identity-verification products, which help businesses stop fraud before it happens, all of the major investigations into identity-theft have found a decline in identity theft rates and in the costs to consumers and businesses across the board, as the charts in Supplement B demonstrate.

c) Other issues:

Section 3. The definition of "personally identifiable information" is extraordinarily broad, and may capture anonymous data, which by definition does not include PII.

Section 9. Subclause (d)(2)(C)(i)(II) establishes penalties for supplying inaccurate information "if the entity knows or has reason to know that the information being provided is inaccurate." However, entities sometimes intentionally provide inaccurate information, for their investigation, because the recipient wants both the accurate and the inaccurate information. This is particularly true in the case of a law enforcement

activity. Consider the case of someone with several aliases – law enforcement may want to know what other aliases are, even though they are not accurate.

CONCLUSION

In conclusion, CDIA's members create incredible value for government agencies. 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 with complying each and every day.

We appreciate this opportunity to testify and welcome your questions.

Mr. CLAY. Thank you so much for your testimony.

Ms. Bruening, you are recognized for 5 minutes.

STATEMENT OF PAULA BRUENING

Ms. BRUENING. Thank you, Chairman Clay, for having me here today. I am honored to testify about Government use of commercial information and H.R. 4791.

The Center for Information Policy Leadership is a think tank in policy development organization located in the law firm of Hunton & Williams. The center and its 41 member companies believe that difficult information policy issues must be resolved in a responsible fashion if we're to fully realize the benefits of an information economy.

While I've consulted with center colleagues and members, my comments today reflect my views and do not necessarily reflect the views of the center member companies, Hunton & Williams or any firm clients.

The provisions of H.R. 4791 highlight the growing practice of Government access and use of information collected and retained by business and the lack of comprehensive, overarching legal protections for that information when such access is obtained.

Without question, the information collected by companies can serve as a critical resource for Government in law enforcement, anti-terrorism efforts, fraud reduction, delivery of services, and administration of programs. With appropriate controls, Government should continue to be able to access it. Government should not be precluded from using valuable information for these important purposes, but it should do so under established, rigorous guidance that ensures its use is both effective and responsible.

Today, the lack of legal protections related to the Government's use of data collected in the private sector, due in part to the limitations of the Privacy Act, raises serious risks to U.S. business and compromises opportunities for growth. Access to information by the Government without the protection of law places companies of all kinds in the position of acting as Government data gatherers that are unable to assure their customers that information they release to the Government will be used for specified limited purposes, that it will be handled properly when it is no longer useful, and that the consumer has redress when data it is mishandled. This failure of governance erodes consumer confidence in the companies themselves, reduces trust in the information field commerce more generally, and compromises the growth of the digital marketplace.

Moreover, because of the lack of sound guidance and potential for nearly unfettered access by Government to this information, every privacy question related to data collection in the private sector is shattered by the issues of undisciplined Government access and use of information.

Efforts to resolve issues of consumer protection and privacy in new services, products, business models and technologies are complicated by this constant concern, making it more difficult to build consumer confidence that data is being used responsibly.

The lack of oversight further compromises U.S. businesses' ability to engage with organizations and consumers internationally. Even as companies become more global in presence and reach, it

has become increasingly unattractive to transfer data to U.S. companies because of concerns about U.S. Government access to information about foreign nationals that might occur outside the bounds of law of their home countries and without any real oversight in U.S. law. Lack of broad protection and accountability challenges businesses' ability to make the case that information from foreign companies and about foreign nationals will be managed in a trustworthy fashion, limiting opportunities to transfer and exchange data that can enable innovative business models, research and services.

It is time to consider the myriad ways in which Government accesses, maintains and uses information collected throughout the private sector and develop an overarching governing structure for data use that establishes discipline and accountability in the practice. This inquiry must be forward-thinking and broad in scope, as the solutions we arrive at must be sufficiently rigorous to promote trust and sufficiently flexible to adapt to as-yet-unanticipated technological and marketplace developments.

Developing guidance will require a review of new and emerging technologies for data collection and storage and the trajectory of future technological development. It will be important to consider the legitimate needs and activities of Government for this data and the manner in which it is to be used to further legitimate Government objectives. It must involve development of reliable structures that establish accountability, oversight and protocols for Government collection, retention, use and disposal of data. At the same time, it must assure that access to data is not unduly hindered when it is legitimately needed.

The goal of this inquiry must be to develop a system of governance that fosters data use that is both effective and responsible. Government entities must be required to identify clear objectives for data use and to understand what and how data will be used to accomplish those objectives. Limits must be set for data use and procedures established for data management. Citizens must have redress when data has been misused. Governance must include oversight, both within agencies and by other branches of Government, to instill confidence that the goals of effectiveness and responsibility are achieved.

Thank you very much, and I look forward to the discussion this afternoon.

[The prepared statement of Ms. Bruening follows:]

Hearing on
Privacy: The Use of Commercial Information Resellers by Federal Agencies
March 11, 2008

Testimony of Paula J. Bruening
Deputy Executive Director
Center for Information Policy Leadership
Hunton & Williams LLP

before the
U. S. House of Representatives Committee on Oversight and Government Reform
Subcommittee on Information Policy, Census and National Archives

Distinguished Chairman, honorable committee members, I am Paula J. Bruening, Deputy Executive Director of the Center for Information Policy Leadership. I am honored to testify on government use of information collected and retained in the private sector and H.R. 4791.

The Center for Information Policy Leadership is a think tank and policy development organization located in the law firm of Hunton & Williams LLP. The Center was established to develop innovative, pragmatic solutions to privacy and information security issues that reflect the dynamic and evolving nature of information intensive business processes and at the same time respect the privacy interests of individuals. The Center's member companies include leading organizations in health care, information services, retail, technology, financial services and consumer products. Since its establishment, the Center has addressed such issues as conflicting national legal requirements, cross-border data transfers, and government use of private sector data, with a view to how the future direction of business practices and emerging technologies will impact those issues.

The Center and its forty-one member companies believe that difficult information policy issues must be resolved in a responsible fashion if we are to fully realize the benefits of an information age. Center experts and staff, however, speak only for themselves. While I have consulted with Center colleagues and Center members, my comments today reflect my views and do not necessarily reflect the views of the Center member companies, Hunton & Williams LLP, or any firm clients.

I. Summary

The provisions of H.R. 4791 highlight the growing practice of government's access and use of information collected and retained by business, and the lack of legal protections for that information when such access is obtained. Private sector data provides government with important tools to further government objectives, particularly in law enforcement and national security.

The wide-ranging collection of data by government from third parties challenges traditional notions of information governance. The Privacy Act, which was designed to govern the collection and use of information by the federal government, did not anticipate current information collection practices, and interpretations of the Fourth Amendment, leaves data collected from third parties without Constitutional protections.

This failure of protection raises significant concerns for American business by compromising the trust relationship they work to establish with consumers, and by jeopardizing their opportunities to engage in ventures that involve data transfers into the United States.

It is time to establish a disciplined system for data collection and use by government that fosters use of information that is effective and responsible. The system must be forward looking, anticipating developments in technologies and data collection methods. The goal must be a governance approach that is sufficiently rigorous to re-establish trust, and sufficiently flexible to adapt to changes in the marketplace and technology.

II. Government use of information collected by the private sector lacks meaningful protections that take into account the realities of a data-driven society.

Government use of data about individuals is not new. Government has a long history of collecting information from its citizens for census purposes, to administer the tax system, to record births and deaths, to maintain voter registration, and to record real estate transactions. Government traditionally maintained records in courthouses, town halls, public offices and record repositories. Information once stored on paper is now located in government computer databases.

Today, a smaller percentage of the information used by the government is collected and stored by government itself. Increasingly, government turns to business as a source of all manner of data made available by consumers as they conduct their lives and engage in contemporary society. The proliferation of new technologies for data collection, the development of creative, information-dependent business models to deliver goods and services to consumers, the rapid advances in analytics tools, and the migration of such common activities as shopping, managing finances, using a public library and accessing health information to online and computer-based systems greatly increase the volume of data made available by individuals. Individuals leave trails of data as they purchase their morning coffee, access public transportation, use their mobile phone, visit a health clinic, shop, use e-mail and surf the web. Data now drives our most basic activities and interactions, and businesses of all kinds collect and store that data.

Government makes use of these data sources, seeking information to help them deliver services, administer social programs, manage health care delivery costs, combat fraud, secure the transportation infrastructure, protect cyber networks, investigate criminal behavior and combat terrorism. The data available to government from business is not only plentiful, it is powerful.

The protections in place to protect citizens from government abuse of data collected about them, however, no longer serve their intended purpose. The federal privacy law with the greatest sweep, the Privacy Act of 1974, was a response to growing concerns about the computerized databases of information maintained by the government. Based on principles of fair information practices, the Privacy Act was an effort to regulate the government collection and use of personal information. It limits storage of information by federal agencies to that which is relevant and necessary and only for purposes established by statute or executive order. The Privacy Act implements the principle of openness and transparency by requiring notice of the existence of record systems, and requires that the data subject be able to access and copy their records. It provides individuals with redress if an agency violates the Act with respect to data concerning them.

The Privacy Act no longer provides adequate protection for citizen privacy. As written, the Act did not anticipate the way in which our data collection systems would change, the manner in which government would access data, the ubiquity of data collection, or the robust data systems that would proliferate in the private sector to such an extent that business would serve as a primary source of data about United States citizens.

The most often cited limitation of the Privacy Act is that it applies only to information maintained in a "system of records," which the Act defines as a "group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." The U.S. Court of Appeals for the District of Columbia Circuit held that "retrieval capability is not sufficient to create a system of records. . . 'To be in a system of records, a record must. . . in practice [be] retrieved by an individual's name or other personal identifier.'" In many cases government uses methods to access and use information collected by the private sector that do not involve a personal identifier. In other instances government accesses data but never establishes it in its own database, such that the information falls outside the protections of the Act.

This access to information collected in the private sector is further facilitated by Supreme Court interpretations of the Fourth Amendment to the Constitution that do not reflect the realities of a society and an economy in which sharing of data with third parties is a requirement and not a choice in the conduct of daily life. The Supreme Court held in 1976 in *United States v. Miller*[1] that there can be no reasonable expectation of privacy in information held by a third party. The case involved cancelled checks that the Court stated "contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business." The Court found that the Fourth Amendment was not implicated when the government sought access to them. The Court stated that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the

[1] *United States v. Miller*, 425 U.S. 435 (1976). The Supreme Court reinforced its holding in the context of information about telephone calls in *Miller* in *Smith v. Maryland,* 442 U.S. 735 (1979).

information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."

Under the *Miller* holding, personal information can be freely accessed by government, without judicial review, simply because individuals have revealed that information to a third party. In an environment where the volume and sensitivity of information about individuals necessarily held by third parties continues to grow, this holding, taken together with the limitations of the Privacy Act, leaves the information of U.S. citizens extraordinarily open to undisciplined government access, scrutiny and use with little transparency, oversight or accountability.

Without question, the information collected by companies can serve as a critical resource for government, and with appropriate controls, government should continue to be able to access it. The data collected by companies provide keys to furthering law enforcement goals. With appropriate analytic tools, the data reveals points of vulnerability in our national infrastructure. Data helps government deliver services, administer programs and reduce fraud. Government should not be precluded from using valuable information collected by the private sector for these important purposes, but it should do so under established, rigorous guidance that ensures its use is both effective and responsible.

III. Government use of private sector data without legal protections and disciplined governance raises serious risks to U.S. business and compromises their opportunities for growth.

Companies sensitive to concerns about appropriate handling of information invest considerable resources to establish and maintain the trust of their customers by implementing data management and privacy practices that provide transparency and accountability about their data practices. Access to that information by the government without the protection of law places companies of all kinds in the position of acting as government data gatherers that are unable to assure their customers that the information they release to the government will be used for specified, limited purposes, that it will be properly handled when it is no longer useful, that it is accurate, or that the consumer has redress when data is mishandled. This failure of governance erodes consumer confidence in the companies themselves, reduces trust in information-fueled commerce more generally, and compromises growth of the digital marketplace.

Moreover, because of the lack of sound governance and the potential for nearly unfettered access by government to this information, every privacy question related to data collection in the private sector is shadowed by the issue of undisciplined government access and use of information. Efforts to resolve issues of consumer protection and privacy in new services, products, business models and technologies are complicated by this constant concern, making it more difficult to build consumer confidence that their data is being used responsibly. Without the necessary controls around government use of private sector information, companies are left to respond to the argument that because the government can so easily obtain data, it should not be collected at all.

The lack of oversight further compromises U.S. business' ability to engage with organizations and consumers internationally. Even as companies become more global in presence and reach, it has become increasingly unattractive to transfer data to U.S. companies because of foreign concerns about U.S. government access to information about foreign nationals that might occur outside the bounds of the laws of their home countries, and moreover, without any real oversight under U.S. law. The lack of systemic protections related to how the government obtains and uses private sector data sends a message that information about foreign nationals cannot be entrusted to U.S. business, limiting their opportunities to transfer and exchange data that can enable innovative business models, medical research and education initiatives. Lack of discipline and accountability challenges business' ability to make the case that information from foreign companies and about foreign nationals will be managed in a trustworthy fashion.

IV. This practice demands a system for privacy governance that fosters effective and responsible use of private sector data across government agencies.

The data brokers that are the focus of H.R. 4791 represent only one source of private sector data. Data sharing between the public and private sector takes place across a range of business sectors. Government turns to telecommunications firms, health care providers, retailers, financial institutions and Internet service providers for data that would further government objectives. While the provisions of H.R. 4791 single out one data resource, the issues raised by government access to information are not limited to information gathered from data brokers. The bill would not address the broader question of governance related to the government's access, management and retention of data accessed from all private sector sources.

It is time to consider the myriad ways in which government accesses, maintains and uses information collected in the private sector, and develop a governance structure for data use that establishes discipline and accountability in that practice. This inquiry must be forward-thinking and broad in scope, as the solutions we arrive at must be sufficiently rigorous to promote trust, and sufficiently flexible to adapt to as yet unanticipated technological and market developments.

The goal of this inquiry must be to develop a system of governance for government access and management of private sector data that fosters data use that is both effective and responsible. Such principles must mandate that government entities identify clear objectives, and understand what data will be used and how data will be used to accomplish those objectives. They must also set limits for its use, establish procedures for handling of data within government agencies and provide for its disposal. They must provide redress for citizens when their data has been misused.

Developing this guidance will require review of new and emerging technologies for data collection and storage, and the trajectory of future technological development. It will be important to consider the legitimate needs and activities of government for this data and the manner in which it uses it to further legitimate government objectives. It must involve development of reliable structures that establish accountability, oversight and

protocols for government collection, retention, use and disposal of data. At the same time, it must ensure that access to data is not unduly hindered when it is legitimately needed.

While the results of this effort must reflect the current and emerging environment for data collection and use, the Privacy Act can serve as a starting point for this inquiry. The fair information practices that form the foundation of the law continue to provide sound goals and guidance for establishing responsible information management practices, even as they are challenged by new technological and data processing developments.

I also recommend to the committee "Government Data Mining: The Need for a Legal Framework," an article authored by my colleague at the Center for Information Privacy Leadership, Professor Fred H. Cate,[2] to be published in the spring of this year in the *Harvard Civil Rights-Civil Liberties Law Review.* Professor Cate proposes recommendations for marshalling the power of data mining for appropriate uses while protecting personal privacy. While his comments are focused on data mining for national security, he notes that his recommendations apply equally to government data mining for other purposes. I would be happy to provide this article to the Subcommittee upon its publication.

V. Conclusion

Data about individuals collected in the private sector can provide government with an important tool in furthering its objectives, many of them critical to our national security and law enforcement. However, the failure of discipline and accountability in accessing, using and managing this data jeopardizes the trust between business and their consumers, and compromises their opportunities to engage in ventures that reach outside of the U.S. This gap in trust has implications for the development of information-driven businesses and services, the ability of companies to share data across borders, and ultimately the growth of the domestic online economy.

The provisions of H.R. 4791, while well-intended, do not reach the overarching question of trust in government access and use of private sector data across industries. Information maintained by data brokers is not the issue, nor is the private sector collection of data. The urgent issue is the lack of governance and accountability surrounding government access, use and management of data.

It is time to address this important question and to develop privacy governance for government that fosters effective, responsible data collection and use.

Thank you again for the opportunity to testify. The Center looks forward to working with the Committee as it pursues this important issue.

---

[2] Professor Cate is a Distinguished Professor and the Director of the Center for Applied Cybersecurity Research, Indiana University and Senior Policy Advisor, Center for Information Policy Leadership at Hunton & Williams LLP.

Mr. CLAY. Thank you so much for your testimony.

Let's start with Mr. Schwartz.

This question is similar to the one I asked Ms. Evans from OMB earlier. OMB's PIA guidance from 2003 requires a PIA to be performed when agencies systematically incorporate information into their system, but that merely pinging or querying a data base does not require a PIA.

Given the systematic use of this information by the Federal Government, why is this distinction necessary? And isn't the Government using this information to inform decisionmaking?

Mr. SCHWARTZ. It's an excellent question. I think that it really gets to the heart of the matter about where we stand with PIAs today.

I think we agree with Ms. Evans about agency flexibility, and there would be room for agency flexibility. But I disagree with her in how she was talking about that flexibility. To me, it doesn't matter where the information is stored; it is how the information is used and what it is going to be used for.

And I can illustrate this pretty easily in some of the other issues by talking about that the PIA is really a management function of the agency, in terms of information policy management, which is why this——

Mr. CLAY. Why should it matter, how agencies are accessing the information?

Mr. SCHWARTZ. Well, I don't think that's what the distinction should be.

Mr. CLAY. OK.

Mr. SCHWARTZ. It should be how they are using information and what they are using for.

So an example I can give is that we've been talking about the use of the information, which resulted in the question of how do we stop misuse of information. The information that an agency may be pinging from a data base may be entirely accurate and may follow all the rules and laws that it is supposed to follow, but there is still the question of how that Government employee uses the information.

We've had cases where a drug enforcement agent has gone and looked up their ex-girlfriend's record using a commercial data base, looked up the ex-girlfriend's boyfriend's records using a commercial data base. That shouldn't be allowed today, and it's not allowed. The question is, how do you effect those rules? And what the privacy officers tell me today is that the only tool that they have at their disposal to make sure that's in place is the privacy impact assessment.

So if we're not covering this data and not looking at how that management goes into effect, we're going to miss those cases where we could have stopped misuse before it happens.

Mr. CLAY. It is a tool, and a needed tool. Is what you're telling me?

Mr. SCHWARTZ. Yes, absolutely.

Mr. CLAY. Thank you for that.

Any comment on that?

Mr. PRATT. If I may, let's just take a consumer reporting agency as one example.

And I think that Mr. Schwartz gives a great example of browsing. Browsing is always something that you want to control, and there's some technological strategy for how you can control browsing. If you're a using a consumer reporting agency data base, it is not an unregulated data base. It will register an inquiry showing that the Government agency accessed the data base. And, in fact, contracts and Federal law would prohibit the browsing activity.

So I think that if Mr. Schwartz is simply saying that there needs to be an effective oversight mechanism within the Government agency to ensure that browsing doesn't occur or that other data security practices are effective in protecting data, I mean, that makes sense. I just wanted to make the distinction between that and the idea that the data is just sitting on a screen and anybody should be able to walk up or that law doesn't somehow constrain it.

The same is true, by the way, for the Gramm-Leach-Bliley Act. If you are using fraud-prevention tool or a locator tool, it is used for a certain purpose, and there is a certain limited amount of data that will be made available.

So those are just two examples of where Federal laws today set up a regime where both the end user, in many cases by contract and in some cases by Federal law, is restricted in terms of its use of that information.

Mr. CLAY. You know, Mr. Pratt, in your testimony, you mention that sections 8 and 9 of H.R. 4791 are unnecessary or inconsistent with current law. Please define what those provisions are and how they would unduly burden CDIA's members.

And if we follow your train of thought, you know, there would not be many teeth left in the original intent of the bill, and it would only be a shadow of its original self.

Mr. PRATT. Well, we hope not, meaning I think we share the same goal, which is to make sure that when Government obtains information it understands why it is obtaining it, it understands the uses of that information, it understands what current Federal law requires or imposes.

And so when we talk about, for example, section 8, that's the section which defines the data broker, and then in following, section 9 is the section which establishes, not just the PIA review, but it also talks about the contract.

And so, again, one of our concerns is a Government agency imposing wrongly or imprecisely an accuracy requirement on a data product which isn't built to be accurate but to be a law enforcement research tool, or a skip tracing tool to try to locate, again, somebody who has not paid a student loan.

So there seems to be just a little bit of a one-size-fits-all in the current structure of the bill that you've proposed. And so, we're not suggesting there should be no teeth, but I'm suggesting that the FCRA has a lot of teeth with regard to accuracy and a lot of teeth with regard to the end user, the Government, and the restrictions that they must have and the contracts that they must sign off on, and the private liability and the civil enforcement powers that apply to the FCRA.

The same is true for contracts under GLB. It's that there is a limited set of uses, and they contract for those uses. So those are

not data-mining browsing data bases. Those are data bases used for particular——

Mr. CLAY. OK. I look forward to working with you on those sections.

Mr. PRATT. Thank you, sir. We appreciate that.

Mr. CLAY. Let me also say, to followup, how exactly are PIAs, which would be the responsibility of an agency to carry out, an undue burden for your membership? It seems to me that our proposed legislation places nearly all of the burden on the agencies obtaining the information, does it not?

Mr. PRATT. It does. Our concern is that—and I think I heard this at least implied in some of the previous panel's discussion—it is a resource question, first of all. Saying we will require PIAs across the board almost on a product-specific basis would require individuals with the right core competencies to be able to do that well. So there is a training issue. And there's an appropriations resource question, just how many new FTEs we have to hire on a Government agency basis.

So at the beginning of the dialog was, first, have we staffed properly each governmental agency to have the right core competency around data management? And then you move to the question of, well, how then do we use data under the Fair Credit Reporting Act? That may be a different flow.

But, for now, our concern is that what are going to find is that some agencies say, "Well, we just won't clean up our internal data base. We just can't use the private sector anymore. We don't have anybody who can do this PIA this year, so we just simply won't use private sector. We'll just be less effective in doing what it is that we're required to do by a Federal law."

Mr. CLAY. OK, then.

Please explain the information reseller industry's position regarding the appropriate use of information in public records that is not specifically restricted by law. Given that resellers aggregate information from multiple sources, including public record, and make it more readily available than paper records located in places such as courthouses, shouldn't resellers be responsible for protecting the privacy of the individuals involved?

Mr. PRATT. That it is a great question. It's actually one of the tough societal questions we're wrestling with right now.

A couple of things. First of all, and it was mentioned in the first panel, a Google search. In Maryland today, for example, I can go to my courthouse and I can go online and actually find my deed. And on my deed is a certain amount of personal information. I would say, over the last 10 years, though, the State government and local government agencies that are storing a great deal of information have been removing sensitive personal information, making those kinds of documents less prone to contributing to the risk of identity theft, for example.

But the key here is, this is all publicly available. And it's not actually in paper records, in many cases. Now it's an online process. Most of the court systems have online systems available. In fact, State laws often require online systems to be available to fulfill their mission.

So between Google searches and your ability to go to certain Web sites where you can just simply pick up the URL and click through to the public record, that data is out there today and it is publicly available information. So our view is that a data reseller that has publicly available information is in no different position than the courthouse itself with regard to the same information.

Do we want a Social Security number—this is a different question—do we want a Social Security number in a deed for a home? Our members' answer is no.

Mr. CLAY. No.

Mr. PRATT. In other words, we are working with State governments right now to try to pull back data where it is not appropriately or necessarily part of a public record.

Mr. CLAY. OK. But now, Mr. Pratt, here is what GAO has told us, is that information resellers generally allow individuals limited ability to access and correct their personal information.

Mr. PRATT. That's a great point.

Mr. CLAY. So how do we square with that?

Mr. PRATT. Well, again, this would be a general data base, not an FCRA-regulated data base. If it is built for Fair Credit Reporting Act purposes, you have the right to correct the information.

One of the big challenges is, if you don't correct the information at the courthouse level, then the same data can be gathered by another company, subsequently, under general public record and Freedom of Information Act laws today.

So it isn't so much that we don't want to correct the record, but we want to make sure if a record is going to be corrected it is not just artificially corrected in a single private-sector data base, but that the consumer goes to the right original source, so that it's corrected in the courthouse, so every data base that might have that public record are all going to reflect the correct information.

Mr. CLAY. And the court clerk has a responsibility then to redact or to block out?

Mr. PRATT. The court should. I mean, candidly, one of the challenges is for courts to make sure that they have a way for consumers to correct their information.

By the way, not every court does today. That's one of the challenges we have in the public record discussion that we've had in this country for some time. I, as an individual, may not easily get the attention of a court to correct information, or it may take a longer period of time than we would like. We think we're getting closer to solutions, but that is a problem we're still facing.

Mr. CLAY. Thank you for your response.

Let me go to Ms. Bruening.

An important thing in the testimony seems to be that information collected by the Government from all sources, not just data brokers, is inadequately protected or safeguarded. Please explain the reasons why you believe this is so. For example, is it due to an outdated Government privacy act or an effect of private-sector regulations?

Ms. BRUENING. Well, first, Mr. Chairman, I think it is important to emphasize that data is being collected from all kinds of private-sector sources, not just data resellers. Our ISPs are being asked for information, retailers are asked for information, our telecommuni-

cation services. So this practice goes on throughout the private sector.

The other point I think that's important to be made is that the Federal Privacy Act was passed in 1974 at a time during mainframe computing, and it certainly has not anticipated where we are today. It probably didn't even anticipate a couple of different jumps we've made since 1974 in terms of computing.

We're now in an age of cloud computing. We're collecting data in all kinds of different ways, through different kinds of technologies. In some cases, the Government may access that information and bring it into its own systems of records. In other cases, it doesn't. It merely pings data bases or obtains information from data bases, never bringing it into Government.

So the definitions in the Privacy Act are challenged by this new kind of technology and these new kinds of data uses. And so, given that, we're left with very little protection for the kinds of information access that the Government is using in the private sector.

Mr. CLAY. You know, you also cite the lack of a cohesive or modernized definition of what is a system of records, in your testimony. How is current law limited in its definition of what constitutes a system of record? Do you have recommendations on how to improve the current definition?

Ms. BRUENING. Well, as I mentioned, the way that information is maintained and stored today is very different from the traditional ways we've thought about that, in terms of data bases, and therefore the way we access it very different.

In the past, we thought about systems of records as the ability to search for information on the basis of an identifier or a person's name. In many cases, that's not how Government uses information anymore. And, you know, data mining is the prime example. There are other analytics tools that have very creative ways of using information about individuals that would not involve a system of records as it is defined in the Privacy Act.

I don't have the recommendation for how to fix it. I think this is a big question. It's one that would require a lot of serious thinking on the part of people in a range of areas, whether it's technology, the law, people who are involved in data management, security people. So I don't have the answer, but it is a question I think that requires some very serious attention, because it is raising some significant concerns for the business community, as I'm sure it is elsewhere.

Mr. CLAY. Please explain for us how ineffective protections for personal data negatively impact business. Is it because of legal liability or an issue of consumer trustworthiness in modern technology? Do ineffective privacy safeguards have a tangible impact on electronic commerce or online banking activities?

Ms. BRUENING. Well, I think one of the prime examples in the area of, sort of, our ability as American business to engage with companies outside of the United States is an action that was recently taken by the province of British Columbia in Canada, which limited the ability of Canadian companies in British Columbia to outsource data for processing in the United States. And that action was taken on the basis of concerns about the perceived lack of protection for information that is potentially accessed by Government.

And what that does is create inefficiencies in business, and it puts businesses at a competitive disadvantage. I think it also does impact the relationship of companies with their consumers. I think that responsible companies put a lot of time and effort into addressing the privacy concerns that are raised by some of their new businesses models and the new technologies that they deploy.

But what happens is, in attempting to address those questions, what we've come to call the elephant in the room—although, I guess in a political year that's not the best term, but we will call it the rhinoceros in the room—tends to be, no matter what we do to protect privacy, this data is accessible by Government, and where does that leave us in our relationship with consumers. And so, that is of very serious concern on the part of companies.

Mr. CLAY. Thank you for your response.

Let me start—yes, sir, Mr. Schwartz?

Mr. SCHWARTZ. I want to followup on something that Ms. Bruening said that I agree with, in terms of her comments on a definition of systems of records. And you heard Ms. Evans on the last panel talk about, in terms of, in the case of commercial resellers, information being systematically incorporated. And one of things she said then was, if it is turned into a part of a system of records. Right?

And so, this shows both the weakness of the Privacy Act in that there are fewer and fewer data bases that are qualifying as Privacy Act system of records today because of the decay that Ms. Bruening talked about in technology, being able to search out information without necessarily searching on an identifier or a name.

So we have a lot more information that is being brought into the Government that may not necessarily be in a system of records. And I think Ms. Koontz was getting at that in the last panel, too. It is hard to figure out what "systematically incorporated" means today, with this definition of system of records that we have. And because OMB has not defined that better, you have a lot of confusion at agencies about that. You have agencies with a lot of different standards.

Mr. CLAY. This is a series of questions for the entire panel. Let's start with Mr. Schwartz and move down. This is a yes-or-no question.

Is it considered a best practice today for large organizations to conduct a privacy impact assessment when purchasing or subscribing to a service that could have a major impact on the privacy of its customers or citizens?

Mr. SCHWARTZ. Yes.

Mr. CLAY. Mr. Pratt? And you can elaborate, if you'd like.

Mr. PRATT. Is it a yes-or-no?

Mr. CLAY. You can elaborate.

Mr. PRATT. Every private-sector company that's going to obtain data is going to do several things. They are going to say, is it sensitive personal information under a State data breach law, so do I have to protect it in a certain way? Is it regulated under the Fair Credit Reporting Act? Does the contract, if I'm contracting with an entity, put certain restraints on what I must do?

So I suppose, in essence, that is a privacy assessment. Am I going to secure it because it is sensitive personal information? Is

it a consumer report, so then do I have additional responsibilities such as properly disposing of it, limiting access to it and so on?

So, in that sense, yes, I think private-sector laws regulating entities all across this country are, in fact, conducting privacy assessments with regard to sensitive personal information of all types, many of which are represented by the members of the CDIA.

Mr. CLAY. OK.

Ms. Bruening.

Ms. BRUENING. Yes, privacy impact assessments are a best practice. They serve a very important role.

The concern is, however, that within Government it isn't enough to simply conduct a privacy impact assessment; that there needs to be oversight both within an agency and from other branches of Government so that you can get the kind of accountability and responsibility in that use that you need.

Mr. CLAY. Mr. Schwartz, should information resellers that are governed under the Fair Credit Reporting Act or Gramm-Leach-Bliley be exempted from requirements in the proposed Federal Agency Data Protection Act?

Mr. SCHWARTZ. I think that they should. The question of whether they take steps toward accuracy—and, again, you also heard Mr. Pratt speak earlier about different kinds of data bases, so it is not necessarily—I think that there is some distinction there about whether the information broker has to follow FCRA for certain data bases and not for other data bases, and that's confusing, I think. And it is the responsibility of the agency to figure out where the coverage lies, what the protections are, and to do that kind of review.

PIAs, in particular, are set at different levels. And the OMB guidance today has said that agencies are supposed to do the PIA based on what the potential of impact of privacy is. And that's really what the goal should be here. It is completely incumbent on the agency to do this review.

As I said earlier, beyond the accuracy issues and beyond figuring out who the partner is, it is also to figure out what the rules are internally for the use of that information, and to set that up in a way that the program officers understand those rules. The PIA is the only way do that today under U.S. law.

Mr. CLAY. OK, let me go to Ms. Bruening.

What is your feeling?

Ms. BRUENING. Unfortunately, I'm not in a position to speak to the specifics of the provisions of the bill.

However, I think what your question does highlight is the fact that we really need to be careful that we don't approach this question in a piecemeal fashion; that this really is a question about how Government treats data once it is brought into Government, so that we can—you know, are we asking the right questions? Are we setting appropriate objectives? Are we setting the right priorities about those objectives? Are we looking closely at what data is being used and how it is being used and whether it is going to get us to the objectives that we want to reach? And is there accountability around that? And do we have the right kind of processes and procedures for management of that data once it is brought into Government?

Mr. CLAY. Mr. Pratt, go ahead. You may respond.

Mr. PRATT. Thank you, Mr. Chairman.

I see it this way: There already is an assessment any time a Government agency is going to have to purchase a consumer report, whether they're going to hire an employee and they need to conduct a background check, whether it's for a national security investigation. And legal counsel, not just a privacy officer, but legal counsel are going to have to determine and ensure that the State or Federal Government agency is going to comply with the Fair Credit Reporting Act, that there is a certain permissible purpose for which the data can be obtained.

And, by the way, the permissible purpose—obtaining for a permissible purpose under the 2003 amendments made it very clear that the user had to obtain and use the data for the permissible purpose. This is not just a question of what the consumer reporting agency does to deliver a report for permissible purpose.

So, to me, it is just apples and oranges. A consumer reporting agency delivering a consumer report to a Government agency knows that Government agency, by contract and by Federal law, is going to have to comply with everything that is required of it, including notifying the consumer if the decision based on that data was adverse to the consumer, the adverse action notice that we're familiar with.

Same thing on the Gramm-Leach-Bliley Act side. I am selling you a look-up service product, you are going to use it for look-up services. Now, to the extent it should not be used for other purposes, that's probably part of what a Government agency should do well. But that's not really a privacy impact assessment, or maybe there's some semantics here in terms of what we mean by the scope of a privacy impact.

But if you are buying it for a skip tracing purpose, that's what it's going to be used for and that's what the contract's going to limit you to. That's different than ISP data. That's different than telecom data. That's different than depersonalized credit card transaction data that the U.S. Secret Service might use, for example, to try to locate a belt skimming operation in Miami.

So there really are, I think, different approaches, and so I don't think—you can look at it holistically, but at the granular level you are going to take different approaches.

Mr. CLAY. Yes, sir, Mr. Schwartz?

Mr. SCHWARTZ. I don't think it is different at all from the private impact assessments that we see from the—the ones that receive good marks from OMB in the FISMA reports. You go back and you look at their PIAs that they've done, they all go through how the information is used, what was management's intent for the use of the data. That's what they are supposed to do.

So this idea that this is only focused on what FCRA is, I think is another universe from what's going on in Government, or what should be going on in the Government, which is covering how this information is managed and used.

Mr. CLAY. Thank you very much for your responses.

And that will conclude the testimony from the second panel. This hearing is adjourned. Thank you.

[Whereupon, at 4:05 p.m., the subcommittee was adjourned.]

○