CENTER FOR
DEMOCRACY
&
TECHNOLOGY
Keeping the Internet Open, Innovative and Free

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. In a report on a program where similar data was shared, GAO suggested that the Privacy Act may have been violated and the DHS Chief Privacy Officer agreed that the agency did, in fact, violate the Privacy Act in that case.[4]

---

[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. Also see CDT Policy Post, "JetBlue Case," Volume 9, Number 20, October 17, 2003, http://www.cdt.org/publications/pp_9.20.shtml.

[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,
Privacy Office, Department of Homeland Security, "Secure Flight Report," December, 2006/ http://www.cdt.org/security/20061222secure.pdf,

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 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.

[5] PL 107-347, Section 208.

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. 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 —

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

---

http://www.cdt.org/security/identity/20070502rice.pdf.

[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.

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 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.