Statement of Ari Schwartz
Vice President
Center for Democracy & Technology
before the
Committee on Homeland Security and Governmental Affairs

Protecting Personal Information: Is the Federal Government Doing Enough?

June 18, 2008

Chairman Lieberman, Ranking Member Collins, and members of the Committee, thank you for holding this hearing on the protection of personal information by the federal government. I am Ari Schwartz, Vice President of the Center for Democracy & Technology (CDT).

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

Summary

Current federal laws and policies provide to those agency officials who care about privacy valuable tools to protect personal information in the hands of the federal government. Unfortunately, these laws and policies clearly have not been implemented consistently in a way that prevents indifference or wanton neglect of personal information. Moreover, even diligent officials find gaps in existing laws, especially because those laws, especially the Privacy Act of 1974, have failed to keep pace with technological change.

To adequately protect privacy in this digital age, when more information is collected and shared than ever before, both Congress and the Executive Branch will need to work together to close the long-recognized gaps in existing laws and policies. At the same time, both branches must foster the leadership and insist upon the measurement capabilities needed to ensure that existing and new laws and policies are implemented uniformly and diligently.

Shortcomings of the Privacy Act

Despite a somewhat complicated structure, the Privacy Act of 1974 has generally been successful in offering a baseline standard for the protection of personal information in the hands of the federal government.[1] However, despite this success, some of the Act's flaws were recognized soon after it was passed. Most notably, the Privacy Protection Study Commission (PPSC), a Commission created by the Privacy Act itself, issued an assessment of the law in July 1977 commenting on problems in the Act that have been echoed ever since.

CDT would like to focus on three main areas of concern that have been raised in many reviews of the Privacy Act from the 1977 PPSC assessment to the GAO's report entitled "Alternatives Exist for Enhancing Protection of Personally Identifiable Information" released at this hearing.

I. Scope of the Act

A major concern with the Privacy Act today centers on its most important term, "system of records," which is ill-suited to the current data environment. The definition of "system of records" excludes from the coverage of the Privacy Act information that is not regularly "retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."[2] Thus, as used in the Act, the "system of records" concept is overly restrictive. As the PPSC suggested 30 years ago, the system of records requirement acts as an "on/off" switch for the Privacy Act's other requirements. Information that falls outside of the definition is not covered, no matter how it is used or misused. A classic example of this, that will be familiar to many on this Committee, is the controversy involving the secret acquisition of airline passenger data by the Department of Homeland Security, in which the Privacy Officer for the Department was compelled to conclude that there had been no violation of the Privacy Act despite the fact that the Transportation Safety Administration (TSA) "participation was essential to encourage the data transfer" and "TSA employees involved acted without appropriate regard for individual privacy interests or the spirit of the Privacy Act" no violation occurred in part because the information was not officially a "system of records" under the law.[3]

---

[1] See, for example, Daniel Solove, The Digital Person, NYU Press, 2004, p. 222.

[2] 5 U.S.C. § 552a(a)(5).

[3] Department of Homeland Security Privacy Office, "Report to the Public on Events Surrounding jetBlue Data Transfer: Findings and Recomendations," February 20, 2004, p9. http://www.cdt.org/privacy/20040220dhsreport.pdf.

The definition has also clearly become narrower over time because of major advancements in database technology. Today, it is rare that a system is created with a specific identifier that will be used for searching as was commonplace in the 1970s. Instead, agency personnel and contractors can search on a range of different types of criteria, thereby skirting the law. For example, because it did not specifically search on an identifier, the DHS "ADVISE" data mining program was not covered by a system of records notice. The systems that it linked were, but the narrowness of the concept of a "system of records" gave an incomplete picture of the privacy risks of the ADVISE system. Because of scrutiny, DHS eventually suspended the system. [4] The Privacy Act was certainly intended to address the full range of issue posed by a data mining program like ADVISE, but changes in technology have blurred the scope of the Act's most basic definition.

Another major flaw in the scope of the Act relates to the increased government use of private sector data. In passing the Privacy Act, Congress made it very clear that an agency could not get around the Act by having a contractor hold the data,[5] yet Congress clearly did not envision that data services companies in the private sector would amass enormous databases that federal government agencies could subscribe to and search without either bringing the information into a government database or falling under the provision of the Act that covers contractors. Nevertheless, data brokers that sell information to the federal government today are not held accountable to the privacy, security or data quality standards of the Privacy Act.

II. Breadth of Routine Use Exemptions

The issue that has caused the most concern over the history of the Privacy Act has been the frequent, seemingly standardless invocation of the "routine use" exemption to override the Act's limits on reuse and sharing of information between agencies. The "routine use" exemption was designed to allow agencies to share information in limited circumstances based on the frequency and administrative burden of the project. As early as 1977, the PPSC raised major concerns about how the "routine use" exemption was already being exploited to justify vague exemptions that went beyond the original intention of the Act. Successive Administrations have become ever more accepting of this exemption. Routine uses are now so widely used and utterly unchecked that almost every Privacy Act Notice required by the law lists numerous routine uses, including vague boilerplate language confusing both citizens who want to understand what is happening to their data and the agency personnel responsible for it care. For example, the Department of Defense regularly

---

[4] Ryan Singel, "DHS Data Mining Program Suspended After Evading Privacy Review, Audit Finds," Wired Threat Level Blog, August 20, 2007 http://blog.wired.com/27bstroke6/2007/08/dhs-data-mining.html.

[5] 5 U.S.C. § 552a(m).

lists over 20 routine uses and then includes a Web link to a set of 16 "Blanket Routine Uses" that are included with every Privacy Act Notice it publishes.[6] Clearly, this is not what Congress intended.

III. Enforcement

For years GAO and others have reported that the federal government has not properly implemented or enforced the Privacy Act.

For example, implementation difficulties continue to be found in the following areas:

- Publishing all required system of records notices;[7]
- Consistency in determining how the "system of records" definition and the disclosure provisions apply;[8]
- Building reliable internal assessment measures to ensure personal data are appropriately collected and safeguarded;[9] and
- Establishing basic rules for federal agencies' use of personal information obtained from data resellers.[10]

The problem of lack of enforcement runs deeper than just privacy concerns. Many agencies have simply lost the personal data of millions of Americans. For example, the Chief Privacy Officer of a large agency privately reported to CDT that, when the agency did an audit of its Privacy Act systems of records, it found that half of the systems (and all the records involved) were lost. Other cabinet level agencies do not even audit the existence, location or condition of their systems. As one retiring security official from the Department of Interior recently explained, Interior has been "promiscuous with our data… we don't know anything about our data… we don't know where our data is."[11]

---

[6] The "Blanket Routine Uses" are available at http://www.defenselink.mil/privacy/dod_blanket_uses.html

[7] This problem, identified as early as 1987, "Privacy Act System Notices," November 30 1987, GAO/GGD-88-15BR http://archive.gao.gov/d29t5/134673.pdf, is still a major concern today as evidenced in GAO's report released today. In 1990, a more comprehensive GAO study suggested that only 65% of systems covered by the Privacy Act had proper notice procedures. GAO, "Computers and Privacy: How the Government Obtains, Verifies, Uses and Protects Personal Data," August 1990, GAO/IMTEC-90-70BR. Agency personnel have regularly told CDT that there are thousands of systems of records that do not have systems of records notices, suggesting that a substantial proportion of covered systems have still not been properly noticed.

[8] GAO "OMB Leadership Needed to Improve Agency Compliance," June 30, 2003, GAO-03-304 http://www.gao.gov/new.items/d03304.pdf

[9] GAO, "Privacy Act: Federal Agencies' Implementation Can Be Improved," August 22, 1986, GGD-86-107 http://archive.gao.gov/d4t4/130974.pdf

[10] GAO "Agency and Reseller Adherence to Key Privacy Principles," April 4, 2006, GAO-06-421 http://www.gao.gov/new.items/d06421.pdf.

[11] Comments of Ed Meagher, Deputy Chief Information Officer, Department of Interior, before the National Institute of Standards and Technology Information Security and Privacy Advisory Board, June 5, 2008.

Shortcomings of the Privacy Impact Assessment Process

The Privacy Act is not the only federal law affecting the privacy of personal information. Important steps toward updating government privacy policy were taken with the passage of the E-Government Act and efforts toward its effective implementation. In particular, Section 208 of the Act was designed to "ensure sufficient protections for the privacy of personal information."[12] To improve how the government collects, manages and uses personal information about individuals, Section 208 requires that agencies post privacy notices on their Web sites and that they conduct privacy impact assessments (PIAs).

Section 208(b) of the E-Government Act requires that agencies perform PIAs before (i) developing or procuring new technology that collects, maintains, or disseminates personal information or (ii) initiating new collections of personally identifiable information. These PIAs are supposed to be public documents and are supposed to contain a description of the project, a risk assessment, a discussion of potential threats to privacy, and ways to mitigate those risks. PIAs are intended to 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.[13] Unfortunately, as with the other privacy laws, federal agencies unevenly implement even the basic requirement of PIAs.

PIA Reporting

The recent OMB Federal Information Security Management Act (FISMA) report to Congress highlighted the fact that agencies, as rated by their own Inspectors General, range from "excellent" to "failing" in their implementations of the PIA requirement.[14] This wide range of compliance is due to two major factors: 1) 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 and 2) the reporting standards themselves are not uniform, as each Inspector General is basically developing its own standards for issuing these ratings.

---

[12] PL 107-347, Section 208.

[13] DHS Chief Privacy Officer Hugo Teufel, *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.

[14] MB FY 2007 Report to Congress on Implementation of the Federal Information Security Management Act of 2002. http://www.whitehouse.gov/omb/inforeg/reports/2007_fisma_report.pdf.

While some agencies, like the Department of Homeland Security (DHS),[15] 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.[16] Yet DHS received only a "good" mark and the State Department received a "satisfactory" mark in the FISMA report.

Even more troubling is the finding that some agencies simply do not perform PIAs on as many as half their qualifying technologies.[17] 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.

Finally, and perhaps most importantly, 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. They are supposed to be prepared early in the system design process, so they can be used to identify privacy problems before the system design is finalized. They cannot serve this crucial role is they are done after design is completed.

While OMB has begun to take steps to address the inconsistent implementation of PIAs, it should be of great concern to this Committee 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 supports this provision.

Private Sector Data

Another concern with Section 208, similar to concern about the coverage of the Privacy Act, is the failure to specifically require PIAs for government access to private sector data. OMB guidelines allow agencies to exempt the government's use

---

[15] 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.

[16] 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 .

[17] 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.

of private sector databases from the requirement to conduct PIAs when the commercial data is not "systematically incorporated" into existing databases. CDT believes that this permissive approach is wrong. Companies that provide private sector data to the government have a range of 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 agencies are already requiring PIAs for uses of commercial data even when the data is not integrated into existing databases despite OMB's guidance.

GAO's report published today points out that, in 2006, it recommended that OMB revise its guidance to clarify the applicability of requirements for PIAs with respect to agency use of data obtained from commercial re-sellers. The GAO further notes that OMB did not address that recommendation[18] and openly disagreed with it in House Oversight and Government Affairs Committee testimony.[19] Simply put, OMB has ignored the serious concerns raised by the ease with which an agency can avoid the PIA requirement simply by subscribing to an information service rather than creating a database of the same information within the agency.

Government Employee Information

Section 208 does not require Privacy Impact Assessments for collections and systems involving information about federal employees. Recent data breaches at federal agencies suggest that the government is not adequately protecting information about its own personnel. For example, earlier this month there was a major breach of patient information at Walter Reed Hospital, [20] presumably no PIA was required for this important database because the patients were federal government employees. PIAs would be one good mechanism for beginning to improve not only the privacy but also the security of systems containing the sensitive data of federal employees.

Lack of Privacy Leadership

Some of the blame for the uneven implementation of the Privacy Act clearly falls on the leadership of those individual federal agencies that have not given adequate attention to information privacy and security; their failure stands out because others have done better. But blame also falls on OMB because it is responsible for interpreting and overseeing the implementation of the Privacy Act and Section 208

[18] GAO-03-304.

[19] Karen Evans 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. http://informationpolicy.oversight.house.gov/documents/20080318172705.pdf.

[20] Jennifer C. Kerr, "Walter Reed: Data Breach at Military Hospitals," Army Times, June 3, 2008. http://www.armytimes.com/news/2008/06/ap_walterreed_data_060208/.

of the E-Government Act. In June 2003, GAO issued a report at the request of Chairman Lieberman that is still timely, entitled "Privacy Act: OMB Leadership Needed to Improve Agency Compliance." In that report, the GAO identified deficiencies in compliance 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."[21] Yet, criticism of OMB for failing to provide adequate oversight and guidance to agencies is not new. In 1983, the House Committee on Government Operations raised concerns that OMB had not updated its guidance in the first nine years of the Act's passage.[22] The Department of Justice, which had published an official case law guide to the Act every two years since the late 1980s, has neglected to do so for the past four years.[23]

OMB is now just beginning to provide the kind of leadership that is needed to help agencies build programs to protect privacy, as evidenced by the changes in its FISMA report to Congress to require some kind of yearly reporting by agencies and the creation of a privacy working group within the CIO Council, led by E-Government Administrator Karen Evans. While these are important steps in the right direction, they are not long-term leadership solutions. The next Administration should be encouraged, on a bi-partisan basis, to make major improvements in Privacy Act implementation and oversight.

Recommendations

1) Expanding Privacy Act Coverage — CDT agrees with GAO's basic assertion that the Privacy Act definition of "system of records" is out of date. We believe that this issue must be addressed in legislation, and we urge the Committee to introduce such legislation in this Congress. We suggest a new definition that would ensure coverage of all information that reasonably can be expected to specifically identify an individual.

2) Closing Privacy Act Loopholes — CDT also urges the Committee to consider legislation that would limit the "routine use" exemptions. This could be accomplished by limiting the definition to encompass only uses compatible with the purpose for which the information in the record was collected or obtained, and consistent with the conditions or reasonable expectations of use and disclosure

[21] GAO-03-304.

[22] House Report No. 98-455.

[23] Ken Mortenson, Acting Chief Privacy and Civil Liberties Officer at DOJ suggested that the delay in publishing the Privacy Act Overview was due to internal changes at the Department and a new version would be released this summer.

under which the information in the record was provided, collected, or obtained. In addition, we urge clarifying the Act to make it clear that its core principles apply to commercial data used by the government.

3) Improving Privacy Impact Assessments — As we testified before this Committee last year,[24] CDT supports the creation of best practices for PIAs as called for in the E-Government Act Reauthorization Act (S.2327) as passed by this Committee. CDT also urges the Committee to require PIAs for any program that uses commercial data, whether the personal information used will be stored at the agency or kept by the commercial entity. CDT supports requiring PIAs government-wide for rulemakings as well as information collections. This is currently the law only for DHS. CDT also supports requiring PIAs for systems of government employee information. Finally, we stress the importance of ensuring that PIAs are begun early in the development of a system or program and that they are completed before the project or procurement begins, so that the findings of the PIA can shape rather than merely ratify the activity's impact on privacy.

4) Creating a Chief Privacy Officer Position at OMB Who Will Run a Separate CPO Council — Undoubtedly, at the end of the Clinton Administration, privacy had a higher profile within the federal government than at any other time. The main reason for this level of greater attention was the creation of a Chief Privacy Counselor at OMB staffed by Peter Swire, who is testifying here today. CDT would like to see a similar permanent Chief Privacy Officer (CPO) position at OMB written into law.

At the agency level, the new legislative requirements for appointment of CPOs have clearly been a success, Yet many large agencies that have a lot of personal information still do not have statutory CPO, including cabinet agencies such as the Department of Veterans Affairs, the Department of the Interior and the Department of Housing and Urban Development. Based on this experience, we believe that all large agencies (the so called "CFO agencies" based on the threshold from the CFO Act) should be required to have a CPO. These privacy officials should be placed outside of the structure of the CIO office where resources and attention are almost always rightly focused on systems procurement and maintenance instead of information policy. In addition, department heads should ensure that CPOs are engaged in the early stages of developing policies and planning systems or programs that will have a privacy impact. CDT also urges the creation of a CPO Council with

[24] Statement of Ari Schwartz, Deputy Director, Center for Democracy & Technology before the Committee on Homeland Security and Governmental Affairs on E-Government, December 11, 2007 http://www.cdt.org/testimony/Schwartz_egov_Testimony_20071211.pdf.

a similar structure to the CIO and CFO Councils. While E-Government Administrator Karen Evans' leadership to build a privacy working group of CPOs at the CIO Council utilizing CIO funds is greatly appreciated and a step forward, in the long-run it is not a sustainable model for intergovernmental privacy efforts.

5) Increasing and Improving Privacy Reporting and Audits — OMB requirements for privacy reporting in FISMA are a major leap forward in focusing attention on privacy issues, but getting the right implementation and accountability processes in place is an essential goal. Most importantly, OMB should be required to create standardized measurements for privacy protecting processes (such as, quality of both the PIA process and the PIAs themselves) and make them public. CDT also believes that the Committee should require that the systems of greatest privacy risk (both in size and in program activity) undergo regular audits by IGs and/or, when IGs are overwhelmed or not experts in privacy, by outside third party audit firms.

Conclusions

In the past, CDT has called for creation of a new one-year commission to study the Privacy Act and privacy policy in the government and offer solutions. With the release of the GAO report and the numerous hearings on this and related issues in this Congress, we believe that the basic work that would have been done by such a commission has been completed. In essence there is now consensus around a set of sound recommendations for action by Congress and the Executive Branch to fill gaps and loopholes in privacy law and policy. CDT urges this Committee to draft a bill with the recommendations outlined above and quickly bring it to the Senate floor so that the next President can have the right tools in place upon taking office and can get started immediately on strengthening privacy in the federal government.

CENTER FOR DEMOCRACY & TECHNOLOGY

FOR MORE INFORMATION

Please contact: Brock Meeks
Director of Communications
202-637-9800