Testimony of Ari Schwartz
Vice President of the Center for Democracy & Technology
before the Senate Committee on the Judiciary
on
"Passport Files: Privacy Protection Needed For All Americans"

July 10, 2008

Chairman Leahy, Ranking Member Specter, 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

Reports of illegal browsing of passport information by federal employees and contractors highlight concerns that the State Department has neither created adequate controls to protect the personal information of Americans nor enforced the basic privacy laws on these records. Even now, most of the State Department's controls protecting passport privacy focus on flagging the browsing of celebrity passport records. Meanwhile, we simply do not know how often the records of average Americans — including the neighbors, ex-girlfriends or relatives of those with access — have been browsed or for what purposes. Clearly, more must be done to protect the privacy of all passport holders.

However, the privacy issues requiring Congressional attention go beyond passport files and beyond the State Department.

In general, the State Department's privacy program has lacked vision, direction and resources for several years, demonstrating a lack of commitment to privacy protections. However, while the State Department clearly lags behind many other agencies, it is not alone in its failure to protect the information entrusted to it. As the General Accountability Office (GAO) has shown through a number of studies, privacy procedures are weak at many, though not all, of the largest agencies with the most sensitive personal information. This is because law, policy and practice have been allowed to lag behind the government's greater use of technology.

To adequately protect privacy in this digital age, when more information is collected and shared than ever before, 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.

Passport Records Browsing Demonstrates Larger Problems in State Department Privacy Program

The recently released report from the State Department Inspector General (IG), entitled *Review of Controls and Notification for Access to Passport Records in the Department of State's Passport Information Electronic Records System (PIERS),* reveals that curious contractors and others accessed the passport files of many "high-profile" individuals. The IG concluded that there are many weaknesses in how the Department tries to prevent and detect the abuse of data in passport records. The IG also found that State Department Privacy Impact Assessments (PIAs) were not accurate in regards to the PIERS system.

The IG report shines a light on only one small part of a larger failing at the State Department. This report was a limited review to determine "whether the Department (1) adequately protects passport records and data contained in PIERS from unauthorized access and (2) responds effectively when incidents of unauthorized access occur." Furthermore, the full extent to which PIERS data has been abused is not apparent because the IG focused much of its report on the records of celebrities and there are incomplete records and little monitoring for what purposes the information was accessed. This leaves open the possibility that those with access to PIERS used it to look up their non-famous acquaintances or use it for nefarious purposes such as stalking or identity theft. Based on the information provided about PIERS privacy controls, it seems unlikely that these invasions would ever be detected.

At CDT, we were not surprised to hear that passport records were not adequately protected, because we have been raising questions about a range of privacy practices at the State Department for several years. Simply put, the State Department has failed to build a comprehensive privacy program despite the fact that the Department holds some of the most sensitive information in the federal government.

On May 2, 2007, CDT wrote a letter to Secretary of State Condoleezza Rice raising major concerns about the process for preparing Privacy Impact Assessments at the State Department.[1] In particular, we raised concerns that the PIAs for the E-Passport and PASS Card program were woefully inadequate, and we urged the Secretary to make more comprehensive analysis available to the public. CDT never received a reply.

Privacy Impact Assessments (PIAs) are mandated by the E-Government Act of 2002. We discuss below how the PIA, when treated seriously, is a valuable tool for identifying and addressing privacy concerns associated with government records systems. While PIAs at some other agencies, such as the Department of Homeland Security (DHS) are 25 to 35 pages long, most State Department PIAs are 1 or 2 pages long and contain only

---

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

limited information. In reviewing several other PIAs for systems related to PIERS mentioned in the IG report, we found that all were cursory and many were also inaccurate and incomplete. For example, the Consular Consolidated Database PIA, which allows agents Web access to PIERS and several other databases, has a one page PIA that suggests that other agencies that access it include: the Department of Defense, Department of Justice, Federal Bureau of Investigations, Office of Personnel Management and Department of Commerce, but clearly neglects to mention that the DHS has access despite the fact that several DHS components list access to the CCD as a central point in their documents.[2]

Congress must work to address the specific issue of the privacy of passport records. On that score, we suggest that Congress adopt legislation to provide for passport records the same protections and civil and criminal sanctions that have been applied to tax records held by the IRS in the Taxpayer Browsing Protection Act.[3] However, Congress must also work to strengthen privacy protections at the State Department in general through greater oversight and penalties on the agency for failures to meetmandated privacy responsibilities, starting with the timely preparation and public release of meaningful PIAs.

Similar Privacy Problems across the Federal Government

Just as Congress should not limit its concern to passport records, it should not limit the lessons from this incident to the State Department. Last month, the GAO released a government-wide report finding that agencies "may not consistently protect personally identifiable information in all circumstances of its collection and use throughout the federal government and may not fully adhere to key privacy principles."[4] While most agencies are not heedlessly violating existing laws as the State Department employees and contractors did in the passport browsing case, many agencies are clearly violating the spirit of the Privacy Act and the E-Government Act.

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:

---

[2] See: http://www.state.gov/documents/organization/93772.pdf USVISIT http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit.pdf; CPB http://www.cbp.gov/linkhandler/cgov/trade/automated/modernization/ace/quarterly_reports/ace_status_report_to_congress_march_2008/ace_2ndqtr_08.ctt/ace_2ndqtr_08.pdf and several other DHS agencies publicly list their access to the CCD.

[3] PL 105-35.

[4] GAO, "Alternatives Exist for Enhancing Protection of Personally Identifiable Information," May 2008, GAO-580-36.

- Publishing all required system of records notices;[5]
- Consistency in determining how the "system of records" definition and the disclosure provisions apply;[6]
- Building reliable internal assessment measures to ensure personal data are appropriately collected and safeguarded;[7] and
- Establishing basic rules for federal agencies' use of personal information obtained from data resellers.[8]

Data security is an important aspect of privacy and another area of broad concern. 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."[9]

Gaps in the Privacy Act

As GAO and others have noted, the existing structure of the Privacy Act and at least two of its main definitions have become outdated as a result of technology changes.[10] The gaps in the law, combined with lack of enforcement accountability, have allowed agencies to drift further from compliance with the spirit as well as the letter of the

---

[5] 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.

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

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

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

[9] 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.

[10] This issue is explored in detail in other recent testimony: Statement of Ari Schwartz before the Committee on Homeland Security and Governmental Affairs "Protecting Personal Information: Is the Federal Government Doing Enough?" June 18, 2008 http://www.cdt.org/testimony/20080618schwartz.pdf

Privacy Act. In order to address the larger privacy issues, Congress must address these concerns. In particular:

- **Scope of the Act**

A major concern with the Privacy Act centers on its most important term, "system of records." 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."[11] Information that falls outside of the definition is not covered, no matter how it is used or misused.

The definition has been outpaced by 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. For example, because it did not specifically search on an identifier, the DHS "ADVISE" datamining program was not covered by a system of records notice. (Because of scrutiny, DHS eventually suspended the system.[12])

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,[13] 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.

- **Breadth of Routine Use Exemptions**

Another major concern 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. Successive Administrations have become ever more accepting of this exemption. Routine uses are now so

---

[11] 5 U.S.C. § 552a(a)(5).
[12] 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.
[13] 5 U.S.C. § 552a(m).

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 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.[14] Clearly, this is not what Congress intended.

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."[15] 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 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. 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.[16] Unfortunately, as with the other privacy laws, federal agencies unevenly implement even the basic requirement of PIAs. The State Department is especially egregious in this regard, preparing PIAs that are not only cursory but also inaccurate. For example, the State Department Inspector General determined that information in the PIERS PIA "appears to contradict what OIG observed during the course of this review," specifically sharing information with DHS. In this case, it is especially worrisome because it is unclear from any public information which components of DHS are getting

---

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

[15] PL 107-347, Section 208.

[16] 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.

the passport data and what they are doing with it. Overall, the woefully inadequate nature of State Department PIAs highlights the need for better enforcement of the PIA requirement.

Specifc Concerns with PIAs and Steps to Address Them

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.[17] 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.

While some agencies, like the DHS,[18] 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. Yet DHS received only a "good" mark and the State Department received a "satisfactory" mark in the FISMA report because the ratings are based solely on the number of PIAs completed and not on their quality or accuracy.

Even more troubling is the finding that some agencies simply do not perform PIAs on as many as half of their qualifying technologies.[19] 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,

---

[17] 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.

[18] 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.

[19] 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.

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 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[20] and openly disagreed with it in House Oversight and Government Affairs Committee testimony.[21] 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.

The Chairman and Ranking Member's bill, S.495, would require PIAs for government access to private sector data, a highly necessary step in protecting the information of citizens as government agencies contract with private data brokers.

Lack of Privacy Leadership

---

[20] GAO-03-304.

[21] 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.

Much of the blame for privacy failures at the State Department and other agencies clearly falls on the leadership of those agencies for not giving 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 of the E-Government Act. In June 2003, GAO issued a report 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."[22] Such criticism of OMB for failing to provide adequate oversight and guidance to agencies is not new. Going back as far as 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.[23] Other agencies have also failed to fulfill their government-wide responsibilities. The Department of Justice, which had published an official case law guide to the Act every two years since the late 1980s, has not done so for the past four years.[24]

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

Recent revelations about problems in the State Department's handling of passport files highlight longstanding and government-wide weaknesses in protecting the privacy and security of personal information in the hands of the government. We urge the Congress and the Executive Branch to begin this year to implement a series of long overdue reforms:

1) Update Privacy Protections for Passport Records — As mentioned earlier, using the Taxpayer Browser Protection Act as a model, Congress should strengthen protections

---

[22] GAO-03-304.

[23] House Report No. 98-455.

[24] 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.

for passport records and penalties for misuse. This includes increased oversight and specific penalties for the agency for failure to set and meet specific privacy goals.

2) Increase Oversight of Privacy at the State Department — Passport browsing is not the only privacy problem at the State Department. The Department should be held accountable through its information technology budget for failing to protect the privacy of all individuals.

3) Review Privacy Act Coverage and Close Loopholes — CDT agrees with GAO's basic assertion that Privacy Act definitions are out of date. We believe that these issues must be addressed in legislation.

4) Improve Privacy Impact Assessments Across the Government — CDT supports the creation of best practices for PIAs. 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.

5) Creating a Chief Privacy Officer Position at OMB Who Will Run a Separate CPO Council — To ensure that agencies have greater consistency on privacy and leadership is taken, CDT would like to see a 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 a similar structure to the CIO and CFO Councils.

6) Increase and Improve 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 agencies should

be required to ensure 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.

Conclusion

The violations of the employees who have been browsing passport records are certainly egregious and Congress must address this specific practice. Yet, the State Department and Congress would be treating the symptom of a larger problem if it only took this opportunity to address the problems around this one sensitive database. The failure to protect information in the federal government is far more widespread. The State Department has clearly been a failing agency across the board in this regard and there are several other failing agencies as well. To prevent another serious breach of public trust in this way, Congress will need to address the roots of the problem by updating privacy laws, oversight and leadership.