July 18, 2005

TO: Data Privacy and Integrity Advisory Committee
Department of Homeland Security

FROM: Ari Schwartz
Associate Director
Center for Democracy and Technology

RE: Written supplement to oral testimony delivered on June 15, 2005:
Recommended Policies for Use of Private Sector Data

The Center for Democracy and Technology (CDT) is pleased to supplement its oral testimony of June 15, in order to spell out in greater detail the policy framework that DHS needs to develop for government use of personally identifiable information (PII) acquired from the private sector.

The breadth and depth of private sector data currently available to government agencies was not contemplated in 1974, when the Privacy Act created a legal framework for the federal government's collection and use of personal information. However, while there may be a lack of clarity about when the Privacy Act applies to government uses of commercial data, it is clear that the principles found in the Act remain valid and therefore should be followed when the government uses private sector databases of PII for programmatic functions. CDT urges this Committee to recommend that Congress amend the Privacy Act to make it clear that it applies to government use of commercial data. In addition, until Congress acts, we urge this Committee to recommend that DHS apply core Privacy Act principles – including transparency, collection limitation, accuracy, and redress -- as a matter of policy and contract when it accesses or uses commercial PII.

We will offer a short history of specific areas where controversy exists today and suggestions to ensure that DHS follows fair information principles when it uses private parties to search information on the government's behalf.

I. Privacy Act Background

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. The law only applies to databases fitting the statutory definition of "systems of records."

Among other provisions, the Act contains protections that require:

- **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 required 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 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 exempt records from any of the Act's provisions, it must do so by means of a rulemaking proceeding in which it justifies the exemption.

While the 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 a somewhat arcane law with a dated structure and definitions. Also, it is widely acknowledged that the Act is not being as well enforced as it should be 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."[1] In the two years since the GAO's report, OMB has done little to provide the kind of leadership that is needed to help DHS and other agencies enforce the Act.

II. The Privacy Act's Application to Commercial Databases

The Act's limitations are particularly apparent with regard to government use of commercially-compiled personal data. 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** — As noted above, 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, should make no difference: all Privacy Act principles should apply to the data in the private entity's computers that was collected at the behest of the government. 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 have been confusion

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

about this issue, especially because, 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 two 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 for testing purposes. 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,"[2] presumably because data was not regularly searched on the basis of name. This seems to be an overly narrow view of the Privacy Act, especially because the airline passenger data was specifically augmented with commercial to confirm identities of passengers, and sensitive information like Social Security numbers was used in the testing.

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 area of confusion is over whether the Act applies to commercial databases used by the government when the database was not created at the government's behest and the database remains in the control of the contractor and 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.

III. Privacy Impact Assessments

Section 208 of the E-Government Act of 2002 requires agencies to conduct "privacy impact assessments" (PIAs) when developing or procuring information technology that collects, maintains or disseminates information in identifiable form or when a new information collection is initiated on 10 or more people. The purpose of the PIA is to ensure that agencies have taken privacy into account in making technology decisions and instituting new collections and that agencies document their decisions in written assessments available to the public for comment.

---

[2] "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.

DHS has been a leader in the implementation of the PIA concept. DHS makes its PIAs available on the Privacy Office's Web site.[3]

Unfortunately, Section 208 did not specifically address performance of PIAs for government access to private sector data, and the Office of Management and Budget guidelines allow agencies to exempt the government's use of private sector databases from the requirement to conduct PIAs. 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.

Under the E-Gov Act and the OMB guidelines, there is no prohibition against conducting a PIA when the government procures information services from the private sector. DHS can and should perform PIAs when contracting for commercial data.

IV. Recommendations

With a law as complicated as the Privacy Act, it is often difficult to avoid technical debates about how the law should be applied in situations that could not have been envisioned by its drafters 30 years ago. The following recommendations are meant to move beyond narrow debates about construction of the law and into what DHS policy should be to protect the privacy of individuals.

Specifically, CDT urges the Committee to recommend that DHS reaffirm the application of the Privacy Act to commercial data acquired by the government and apply the Privacy Act to grey areas:

1) Reaffirm the application of the Privacy to the collection of data by commercial entities at the behest of the government (contracting out) and when commercial PII is transferred to the government.

2) Make it clear, as a matter of policy, that Subsection (m) of the Act applies to all PII acquired by the government from private sector

[3] http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0511.xml. While DHS' PIAs have been some of the most comprehensive in the federal government, the Privacy Office has been inconsistent in terms of when it completes and releases its PIAs. In some cases, the PIAs have been released on the same day that a system goes live, offering no opportunity for public comment. However, in most cases, the PIAs have been released at about the same time as the SORN, before collection has begun. CDT believes that an even earlier release would be better with the idea that details can be filled in and changed over time.

databases, whether or not the data is searched by name or other personal identifier.

3) Make it clear that the merging of private sector data with an existing system of records requires a new public notice (SORN).

4) When PII remains in the hands of contractors providing services to the government, either

    a. Subsection (m) of the Act should be applied to all PII used by DHS whether or not they were created at the behest of the government or are commercially available for other purposes, or
    b. commercial data services companies should be required by contract to provide the same rights afforded by the Act, including access and correction, and should be subject to consequences for violating those protections, including fines and possible contract termination.

    Covering private sector databases with the Privacy Act is a clean solution to the problem in that the rules are already in place and creating new protections will be a long and more difficult process. However, as an alternative, the Committee may find it preferable to develop new rules that apply the Privacy Act's principles while excluding any requirements that would be unreasonable to impose on the private sector. This would certainly be progress from the situation today. CDT would by happy to work with the Committee in developing these rules.

5) Require PIAs to be completed for all DHS projects that utilize personal information from private sector sources.

IV. Conclusions

Considering the government's increasing reliance on commercial data, and the harms that can occur when the government makes decisions about individuals based on inaccurate or irrelevant data, it is imperative that DHS develop rules for use of commercial data, regardless of whether the data is brought into government computers. While the principles of the Privacy Act remain viable, DHS will have to go beyond narrow interpretations of the Act in order to ensure that adequate privacy protections are built into its projects. There are increasing calls to update the Privacy Act, but, in the meantime, DHS can take administrative steps to apply the Act's principles to all its uses of personal information.