Center for Democracy & Technology Transition Memo
Theme: Balancing Security and Liberty
Issue: Updating the Privacy Act

✶**Issue/Problem.** The Privacy Act of 1974—the main federal law that protects the privacy of personally identifiable information in records maintained by the federal government—is seriously out of date.

✶**Policy History.** The Privacy Act was written three and a half decades ago, before the Internet even existed and before the government had available to it databases of personal information complied by private data brokers. The Act's central definitions are based on the old model of centralized, name-indexed databases and mainframe computers. The Act needs to be updated to reflect the distributed nature of modern government information systems and the realities of the ways that information is now searched, retrieved and analyzed.

Gaps in the Privacy Act were first noted soon after its passage, but the failure to update the law to keep pace with rapidly advancing technologies has exacerbated the Act's limitations. Three main areas of concern have been raised, most recently in a GAO report that concluded that existing privacy laws do not consistently protect personally identifiable information collected and used by the federal government.[1]

(1) The most important term in the Privacy Act—"system of records"—is not well matched to the current information environment. The definition of "system of records" serves as the "on/off" switch for the rest of the Act's protections; if data does not fall under the definition, then the Privacy Act does not protect it, no matter how it is used or misused. Most significantly, the definition excludes data that is not regularly retrieved using a personal identifier such as a name.[2] Technological advancements have far out-stripped this view of how of data is used. Today, in contrast to the 1970s, data systems do not need to use specific identifiers. Instead, personnel can search on a range of different types of criteria. Thus, for example, a database containing information on millions of persons that is data-mined based on travel histories is not covered by the Act if the list is not searched by name.[3] Likewise, the DHS "ADVISE" project, another data-mining program, was considered to be out of the Act's scope, despite its privacy risks, because it did not specifically search on an identifier.

---

[1] "Alternatives Exist for Enhancing Protection of Personally Identifiable Information," GAO-08-536 (June 18, 2008), http://www.gao.gov/new.items/d08536.pdf.
[2] The definition excludes data 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," 5 U.S.C. § 552a(a)(5).
[3] The DHS Privacy Office found that, because of the out-dated definition of "system of records," no laws were broken when an airline gave DHS a comprehensive list of their passengers, even though employees "acted without appropriate regard for individual privacy interests or the spirit of the Privacy Act." Department of Homeland Security Privacy Office, "Report to the Public on Events Surrounding jetBlue Data Transfer: Findings and Recommendations," February 20, 2004, page 9, http://www.cdt.org/privacy/20040220dhsreport.pdf.

(2) Another problem with the Act is that it does not apply when the government contracts to use private sector data, as it often does. In 1974, Congress did not envision that private data service companies would amass enormous databases that government agencies could subscribe to and search without ever bringing the data into a federal database. (When the government subscribes to already-existing commercial databases, the Act's provision covering contractors does not apply.)

(3) Many agencies exploit the "routine use" exemption in the Act, which was intended to allow agencies to share information in limited circumstances based on the frequency and administrative burden of the project. Today, this exemption is so widely used that almost every Privacy Act Notice lists numerous and vague routine uses. For example, the Department of Defense lists over 20 routine uses and links to a set of 16 more "Blanket Routine Uses" in every Privacy Act Notice it publishes. This abuse of what was supposed to be a narrow exception confuses both citizens wanting to know what is happening with their data and personnel responsible for it. The Bush Administration has been more aggressive than any other in invoking the Act's other exceptions and exemptions.

The defects in the Privacy Act itself have been compounded by lack of enforcement and carelessness toward records management, especially in the Bush Administration. The GAO has reported for years that the Act has not been properly implemented or enforced. Federal agencies have been inconsistent in publishing system of records notices, in applying the "system of records" definition, in defining internal measures of data security, and in establishing basic rules on use of information obtained from data resellers. Many agencies have simply lost the personal data of millions of citizens.

✶**What the Obama Administration Should Do.** Recent GAO reports and numerous Congressional hearings have produced a consensus around a set of reforms that the Obama administration can adopt in order to fill the gaps in privacy law. Immediately, President Obama can create a Chief Privacy Officer for the Executive Branch, instruct agencies to use Privacy Act exemptions sparingly, and conduct Privacy Impact Assessments when subscribing to commercial databases. More long-term, President Obama should advocate for legislation that will strengthen the Privacy Act.

1) President Obama should appoint a senior White House official as Chief Privacy Officer (CPO), to be an advocate for privacy within the Executive Branch. The CPO should chair a CPO Council consisting of the Chief Privacy Officers of each agency, in a structure similar to that of the Chief Information Officer Council. At the agency level, privacy officials should be placed outside the CIO office, which is more focused on maintenance and system procurement than information policy.

2) Immediately upon taking office, President Obama should direct Executive Branch agencies to use Privacy Act exceptions sparingly and to conduct Privacy Impact Assessments for uses of commercial data.

3) Also, President Obama should immediately direct the OMB to issue guidance to all agencies that will strengthen implementation of the current Privacy Act, increase the

quality and timeliness of Privacy Impact Assessments, require regular audits of the largest and most sensitive databases, and establish best practices and standards.

4) President Obama should propose and promote legislation that updates and strengthens the Privacy Act, limiting the "routine use" exemption and covering government use of commercial data.

✶For More Information.

CDT issue expert: Ari Schwartz, ari@cdt.org, 202-637-9800 x107

Resources:

- CDT Testimony on the Privacy Act and Related Issues (June 2008) http://cdt.org/testimony/20080618schwartz.pdf

November 13, 2008