Recommended Principles for Updating Privacy Laws

June 26, 2008

Policy Posts are in-depth analyses on current tech policy issues from CDT experts. Sign up to receive the latest Policy Posts here:

Federal privacy laws have historically been successful in helping to protect personal information in the hands of federal government. However, inconsistent implementation and failure to update these laws with current technology have widened gaps in the law. CDT urges legislation to bring privacy laws up to date in order to minimize threats to privacy.

(1) Legislation Needed to Bring Privacy Laws Up to Date

(2) Shortcomings of the Privacy Act of 1974

(3) Shortcomings of the Privacy Impact Assessment Process and Lack of OMB Guidance

(4) Recommendations

---

(1) Legislation Needed to Bring Privacy Laws Up to Date

Federal privacy laws have historically been successful in helping to protect personal information in the hands of federal government. However, inconsistent implementation and failure to update these laws with current technology have widened gaps in the law. CDT urges legislation to bring privacy laws up to date in order to minimize threats to privacy.

Notably, the Privacy Act of 1974 - while generally successful in offering a baseline standard of protection - has for years been criticized for its flaws. The Privacy Protection Study Commission (PPSC), a Commission created by the Privacy Act itself, issued an assessment in July 1977 commenting on problems in the Act that have been echoed ever since.

Another federal privacy law is the E-Government Act of 2002. In particular, Section 208 mandates that privacy considerations be integrated into the design of information systems by requiring agencies to conduct privacy impact assessments (PIAs). These PIAs are supposed to include a description of the project, risk assessment, discussion of potential threats to privacy and ways to mitigate those risks and are conducted before new projects. Some agencies have created excellent processes for completing and publishing PIAs. However, inconsistent and incorrect compliance to PIA, mostly due to lack of OMB guidance, has compromised the value of this process.

CDT urges the drafting legislation that includes the recommended principles outlined here so that the next President has the right tools in place upon taking office to get started immediately on strengthening privacy in federal government.

---

(2) Shortcomings of the Privacy Act of 1974

The gaps in the Privacy Act of 1974 have been noted since shortly after its passage, but failure to update the laws with rapidly advancing data collection technology has widened them further. There are three main areas of concern that have been raised since the 1977 PPSC assessment and most recently, in the GAO report "Alternatives Exist for Enhancing Protection of Personally Identifiable Information" released on June 18, 2008.

Scope of the Act. The most important term in the Act -- "system of records"-- is ill-suited to the current data environment. The term is critical since, as PPSC suggested 30 years ago, the system of records requirement acts as the "on/off' switch for the rest of the Act's provisions.

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," no matter how that data is used or misused. For example, take the controversy over the secret acquisition of airline passenger data by the Department of Homeland Security. Despite the fact that the Department's Privacy Officer admitted to TSA employees acting without appropriate regard for passenger privacy, it was concluded that no violation of the law had occurred since the data did not meet the "system of records" definition in the hands of DHS.

Technological advancements have made the definition narrower over time. Today, data systems are rarely created with specific identifiers as was commonplace in the 1970s. Instead, personnel can search on a range of different types of criteria, skirting the law. A data-mining program like the DHS "ADVISE" project was not covered by the Act, despite its privacy risks, because it did not specifically search on an identifier.

Finally, the Act does not cover private sector data used by the government. 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 or falling under the Act's provision that covers contractors.

Breadth of Routine Use Exemptions. 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. It is so widely used and unchecked today that almost every Privacy Act Notice lists numerous and vague routine uses that confuses both citizens wanting to know what is happening with their data and personnel responsible for it. The Department of Defense lists over 20 routine uses and a link to a set of another 16 "Blanket Routine Uses" included with every Privacy Act Notice it publishes.

Enforcement. GAO has reported for years that the Act has not been properly implemented or enforced. Federal agencies have been inconsistent with publishing system of records notices, determining the "system of records" application, building internal assessment measures regarding data safety, and establishing basic rules on use of information obtained from data resellers. Many agencies have simply lost the personal data of millions of citizens.

---

(3) Shortcomings of the Privacy Impact Assessment Process and Lack of OMB Guidance

Federal agencies have unevenly implemented even the basic requirement of PIAs. The recent OMB Federal Information Security Management Act (FISMA) report indicates the agency performance on PIAs, as rated by their own Inspectors General, range from "excellent" to "failing." This wide variation is due to two factors: 1) Lack of OMB guidance and 2) no uniform reporting standards, as each Inspector General basically develops its own standards for ratings. More troubling is that some agencies simply do not perform PIAs for as many as half of their qualifying technologies. Even those that do prepare in-depth PIAs too often complete them after a project has been developed and approved, defeating the purpose of having PIAs in the first place. PIAs are supposed to inform the decision making process, not ratify it.

Another problem, similar to that of the Privacy Act, is that the PIA requirement does not cover government use of private sector data. OMB guidelines allow exemption from PIAs when the

commercial data used is not "systematically incorporated" into existing databases. PIAs are also not required for data collections and systems involving information of federal employees. Recent data breaches at federal agencies, like the leak of patient information at the Walter Reed Hospital, suggest the government is not adequately protecting information about its own personnel.

While some of the blame clearly falls on agencies, part also falls on the OMB that is responsible for oversight of both the Privacy Act and Section 208 of the E-Government Act. The OMB's lack of leadership has been criticized since 1983, when House Committee on Government Operations pointed out that OMB had not updated its guidance in the first nine years of the Act's passage. Most recently, GAO's "Alternatives Exist for Enhancing Protection of Personally Identifiable Information" reported noted the OMB failed to act on GAO recommendations in 2006 to clarify Section 208 guidelines to apply to commercial data re-sellers.

---

(4) Recommendations

In the past, CDT had called for the creation of a new one-year commission to study privacy laws and offer solutions. However, with the recent release of GAO reports on the laws and numerous Congressional hearings on this subject, the basic work that such a commission would have accomplished has already been completed. There is now a consensus around a set of sound principles that Congress and the Executive Branch can act upon to fill the gaps in privacy law.

- Expanding Privacy Act Coverage - CDT urges an update to the definition of "system of records," which is out of date and too narrow to cover the full range of relevant cases.
- Closing Privacy Act Loopholes - CDT urges legislation that limits the "routine use" exemption by limiting the definition to encompass only uses compatible with the original purpose. Also, we urge clarifying the Act to make its core principles apply to commercial data use.
- Improving Privacy Impact Assessments - CDT urges passage of the E-Government Act Reauthorization Act (S.2327) that creates best practices for PIAs. We also support making PIAs a requirement for commercial data used by government, government-wide rulemaking, and systems of federal employee information. We stress the importance of making sure PIAs start early in the development process of any system or program.
- Creating a Chief Privacy Officer Position at OMB Who Will Run a Separate CPO Council - We urge all large agencies (so called "CFO agencies") to have statutory CPO positions. These privacy officials should be placed outside the CIO office, which is more focused on maintenance and system procurement than information policy, and head a separate CPO Council.
- Increasing and Improving Privacy Reporting Audits - CDT urges OMB to create standardized measurements to evaluate the quality of both the PIA process and PIAs themselves at agencies. We also believe systems of greatest privacy risk should undergo regular audits by IGs or other expert third party audit firms.

Copyright © 2013 by Center for Democracy & Technology.
The content on this website that originates with CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. Details.

Source URL: https://www.cdt.org/policy/recommended-principles-updating-privacy-laws