

**STATEMENT OF  
OF THE  
CENTER FOR DEMOCRACY AND TECHNOLOGY  
BEFORE THE VETERANS AFFAIRS AND  
SENATE HOMELAND SECURITY AND GOVERNMENT AFFAIRS  
COMMITTEE**

May 24, 2006

The Center for Democracy and Technology<sup>1</sup> is deeply troubled by the revelation that the Department of Veterans Affairs carelessly allowed the personal data of millions of men and women who've served this country to fall into the hands of a simple burglar. Yet, it is our view that this breach is not the failure of one employee or even one agency. It is symptomatic of a larger failure of data management across the federal government.

Until we bring the aging laws and policies that protect our personal information up to date with modern technology, these catastrophic data "spills" will only get worse.

Attorney General Alberto Gonzalez responded to the breach -- the latest in a series of private and public sector privacy gaffes -- by vowing to closely monitor for any signs of identity theft and to aggressively pursue offenders. This is an appropriate and necessary response, now that the data has been compromised, but it doesn't come close to providing the comprehensive protection for personal information expected when the Privacy Act was passed in 1974.

A growing body of research, supported by years of Government Accountability Office reports, makes clear that it is time to bolster the protections in that law and dramatically improve enforcement.

In 2003, GAO made clear that "the government cannot adequately assure the public that all legislated individual privacy rights are being protected." This report and others made clear that the problem is not with an individual agency but rather an endemic lack of leadership from the White House and its Office of Management and Budget over Privacy Act enforcement. In the absence of strong Administration leadership,<sup>2</sup> individual agencies have been left to fend for themselves in bringing their information practices in line with the Privacy Act.<sup>3</sup>

---

<sup>1</sup> CDT is a non-profit, public interest organization dedicated to preserving and promoting privacy, civil liberties and other democratic values on the Internet and new communications technology. Since its founding in 1994, CDT has tracked government information technology privacy and security policy to ensure that it has been kept up to date. This has included reports and testimony on the Privacy Act, the privacy provisions of the E-Government Act and the Federal Information Security Management Act.

<sup>2</sup> GAO, Privacy Act: OMB Leadership Needed to Improve Agency Compliance, GAO-03-304 (Washington, D.C.; June 30, 2003).

<sup>3</sup> CDT has championed the return of the Chief Privacy Counselor, or similar position, to OMB. At the end of the Clinton Administration, Chief Privacy Counselor Peter Swire produced regular guidance to agencies that, while not comprehensive, at least moved many agencies toward positive progress on important privacy matters.

CDT's discussions with agency privacy officers support the GAO findings. One chief privacy officer for a key agency told us that half of the agency's Privacy Act systems of records -- the databases most likely to have sensitive information on Americans -- were simply missing.

To address these serious concerns, GAO correctly recommends that agencies be given better guidance and follow best practices. The Office of Management and Budget's Privacy Act guidance was written in 1975 and has never been comprehensively updated.<sup>4</sup> Technology has evolved enough in the past three years, let alone the past 30, to warrant a thorough rewrite of that guidance. Such a rewrite alone would send a clear message to agency heads and privacy officers that they will be held responsible for the sensitive data in their care.

Although renewed leadership on Privacy Act compliance would be an important first step, it's also the case that the law itself is in need of renovation, given the technological revolution that has taken place in the decades since its passage. Congress must patch the holes in the aging laws intended to protect the personal information that Americans entrust to the government before more massive data breaches occur.

Because of the rash of high-profile data breaches in the private sector, Congress has focused its legislative efforts on establishing data breach rules for the private sector and has not given the same attention to the serious privacy and security problems in government agencies that collect and maintain databases of personal data on Americans. Indeed, only one of the data-breach bills under consideration even begins to address the federal government's use of personal information. The measure, S.1789, "The Personal Data Privacy and Security Act" sponsored by Senators Arlen Specter (R-Pa.) and Patrick Leahy (D-Vt.) would, among other things, require greater oversight over the government's use of personal data and would limit the government's ability to augment its data with additional information purchased from private-sector companies like ChoicePoint. Today, many government agencies are using this commercial data in ways that violate the spirit of the Privacy Act, but not the letter of the law. These practices have encouraged an atmosphere that suggests that the law is not as relevant as it was at the time that it was passed.

Enacting those provisions would be a valuable step toward safeguarding our personal data, but Congress should go further and enact comprehensive legislation to bring Privacy Act into the 21st century. The law, written during the age of the mainframe computer, must be updated to respond to new technologies. Today, a smart phone can hold as much data as computers that occupied an entire room in 1974. Congress can start by updating the basic definitions of the Act and limiting the routine exemptions on the data.

---

<sup>4</sup> OMB, "Privacy Act Implementation: Guidelines and Responsibilities," Federal Register, Volume 40, Number 132, Part III, pp. 28948-28978 (Washington, D.C.: July 9, 1975). There has been irregular guidance such as that issued on May 22, 2006 (the day of the public announcement of the breach).

As early as 1977, a Congressional commission found that the Act's central definition — "systems of records" — was already outdated. Particularly on the Internet, where multiple databases can be linked, searched, copied and reconfigured, the concept simply does not work.<sup>5</sup> Moreover, privacy advocates and policy-makers have long complained that the "routine use" exemption is being used in ways going far beyond its original intent. That definition also needs to be reconsidered.

Congress may also want to review the effectiveness and applicability of sections of the Taxpayer Browsing Protection Act of 1997, which was passed after abuses by IRS employees, including improper removal of taxpayer records from the agency, were revealed.<sup>6</sup>

Americans entrust the federal government with significant amounts of our personal information in order to deliver benefits and services. Updating privacy oversight, policy and law in this area is the first necessary step to ensuring that this information is not simply left vulnerable to common thieves.

---

<sup>5</sup> Privacy Protection Study Commission, *Personal Privacy in an Information Society*, July 1977. An electronic version is available at <http://www.epic.org/privacy/ppsc1977report/>

<sup>6</sup> PL 105-35