

Veterans Data Breach Highlights Inadequate Privacy Protections

May 31, 2006

Tags: Array

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

The revelation that the Department of Veterans Affairs allowed the personal data of millions of men and women who've served this country to fall into the hands of a simple burglar was troubling, but sadly not surprising to those who have tracked the failure of our aging privacy laws to protect citizens' personal information in the digital age.

[\(1\) Veterans Data Breach Highlights Inadequate Privacy Protections](#)

[\(2\) Privacy Act of 1974 Must Be Enforced, Updated](#)

[\(3\) Citizens Should Take Steps to Protect Personal Information](#)

(1) Veterans Data Breach Highlights Inadequate Privacy Protections

The revelation that the Department of Veterans Affairs allowed the personal data of millions of men and women who've served this country to fall into the hands of a simple burglar was troubling, but sadly not surprising to those who have tracked the failure of our aging privacy laws to protect citizens' personal information in the digital age.

Lawmakers have been slow to acknowledge that the growing frequency and severity of data "spills" in the public and private sectors is symptomatic of an outdated legal regime -- developed before the widespread use of the Internet -- that is dangerously ill equipped to protect Americans from modern privacy threats.

Attorney General Alberto Gonzales responded to this latest breach 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, individual agencies have been left to fend for themselves in bringing their information practices in line with the Privacy Act.

The Veterans Administration breach bears interesting parallels to those first reported in 2005 involving data brokers ChoicePoint and Lexis-Nexis. That case triggered firestorm of bad press for the companies involved, renewed public interest in the practice of buying and selling personal information and legislative proposals intended to address the problem.

In the aftermath of those highly publicized incidents, many still failed to make the connection

between the breaches and the laws -- or lack thereof -- designed to protect the personal information that Americans increasingly relinquish to companies as a cost of doing business.

The policy of addressing these data security failures as unfortunate but isolated incidents is no longer viable. In both the government and commercial contexts, the laws that protect Americans' personal information haven't been substantially updated since the widespread adoption of the Internet. Until those laws are updated to reflect the massive data storage, collection and distribution capabilities of Internet and database technology, more and larger data spills will be inevitable.

(2) Privacy Act of 1974 Must Be Enforced, Updated

To address the concerns raised in its reports on government privacy practices, 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. 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.

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 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 another valuable step toward safeguarding Americans personal data against government misuse, but Congress should go further still, by enacting comprehensive legislation to bring Privacy Act into the 21st century. Improved guidance, and fringe regulatory changes can only go so far. The Privacy Act itself, 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.

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. 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.

(3) Citizens Should Take Steps to Protect Personal Information

There is virtually nothing that individuals can do to prevent their personal data from being exposed in breaches like those experienced by the Veterans Administration, ChoicePoint and Lexis-Nexis. In the case of the Veterans Administration, veterans themselves had little say in what information was stored about them and how it was handled.

But there are steps that individuals can take -- both under normal circumstances, and in the wake of a data breach -- to minimize the damage caused by having their information improperly exposed.

Every adult, regardless of whether they believe their information has been improperly exposed, should closely follow their bank and credit activity, including performing regular credit checks with the three major credit reporting agencies. Federal law requires those companies to provide one free credit check a year.

Individuals who believe their personal data has been compromised should contact one of the three reporting agencies and request that fraud alerts be added to their credit reports. Seven states now allow consumers to go a step further by requesting that a "credit freeze" be placed on their report. Consumers should close accounts that have been tampered with or opened fraudulently and alert local police if they detect evidence of identity theft. Victims should also file complaints with the Federal Trade Commission online or by calling (877) ID-THEFT (438-4338).

- [Information for Veterans](#) [1]
- [Theft Prevention Tips](#) [2]
- [FTC Tips](#) [3]

-

- [The Privacy Act](#)
- [Open Government](#)

Copyright © 2013 by Center for Democracy & Technology. CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. [Details](#).

Source URL: <https://cdt.org/policy/veterans-data-breach-highlights-inadequate-privacy-protections>

Links:

[1] <http://www.firstgov.gov/veteransinfo.shtml>

[2] <http://www.consumer.gov/idtheftID>

[3] <http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm>