

STATEMENT OF CHAIRMAN DANIEL K. AKAKA

State of Federal Privacy and Data Security Law: Lagging Behind the Times?

Hearing Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, Senate Committee on Homeland Security and Governmental Affairs

I call this hearing of the Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia to order. I want to welcome our witnesses. Aloha and thank you for being here.

Today, the Subcommittee will examine the foundation for our federal privacy and data security laws. Unfortunately, key pieces of this foundation have serious cracks that need to be fixed.

The Privacy Act, a cornerstone of federal privacy protection, was enacted in 1974 to respond to the increasing ease of collecting and storing personal information in computer databases. It governs how the federal government gathers, shares, and protects Americans' personal information.

Despite dramatic technological change over the last four decades, much of the Privacy Act remains stuck in the 1970s. Many of the definitions in the Act are simply out of date and do not make sense in the current data environment. As a result, the Act is difficult to interpret and apply, and it provides inconsistent protection to the massive amount of personal information in the hands of the government. I want to highlight a few specific concerns.

Earlier this year, the Supreme Court restricted Privacy Act remedies. In Federal Aviation Administration v. Cooper, the Social Security Administration violated the Privacy Act by sharing the plaintiff's HIV status with other federal agencies. The Court concluded that he could not be compensated for emotional distress, because Privacy Act damages are limited to economic harm. By many experts' accounts, this decision rendered the Act toothless, and scholars across the political spectrum have called for Congress to amend the Privacy Act to fix this decision.

Additionally, agencies frequently use private sector databases for law enforcement and other purposes that affect individuals' rights. This is not covered by federal privacy laws, which creates a loophole that allows agencies to avoid privacy requirements. We should require privacy impact assessments on agencies' use of commercial sources of Americans' private information. This would provide basic transparency of agencies' use of commercial databases, so that individuals have appropriate protections such as access, notice, correction, and purpose limitations.

Strong executive branch leadership is also essential to effectively enforcing the privacy protections we do have. Over time, Congress has statutorily required Chief Privacy Officers in many agencies across the federal government, and the Office of Management and Budget (OMB) mandated in 1999 that all agencies designate a senior privacy official to assume responsibility for privacy policy. My Privacy Officer With Enhanced Rights (POWER) Act – included in the Implementing Recommendations of the

9/11 Commission Act of 2007 – strengthened the authorities of the DHS Chief Privacy Officer, with positive results.

Despite OMB's mandate to oversee privacy policies government-wide, it has not named a chief privacy official since the Clinton Administration. As a result, responsibility for protecting privacy is fragmented and agencies' compliance with privacy requirements is inconsistent.

Widespread agency data breaches, and inconsistent responses when they occur, are symptoms of this problem. We all remember the massive data breach at the Department of Veterans Affairs in May 2006, where the personal information of more than 26 million veterans and active duty members of the military was exposed. After that breach, OMB issued guidance in 2007 requiring agencies to strengthen safeguards for personal information and implement data breach notification policies. But implementation of the guidance has been uneven, and the number of federal data breaches has only grown.

Recently, a contractor to the Federal Retirement Thrift Investment Board was the subject of a cyber attack that compromised the personal information of over 123,000 participants in the Thrift Savings Plan. This included 43 current and former Members of Congress. I was concerned to learn that the Board had not followed the 2007 OMB guidance and did not have a data breach notification policy in place when they learned of the breach. I am working with the Government Accountability Office (GAO) to determine how many other agencies have not followed this guidance and determine whether there is sufficient oversight of agencies that have complied.

This builds on the substantial work GAO has completed in response to my nine previous requests on privacy and data security. I have also worked closely with GAO in drafting my Privacy Act Modernization for the Information Age Act (S. 1732), which would make the OMB guidance mandatory for agencies and fix many of the other cracks in the privacy and data security foundation.

Promoting privacy and civil liberties has been a priority during my tenure in the U.S. Senate, and I will continue focusing on this issue until the end of the year. I hope my colleagues will join me in two current efforts to address the problems raised at this hearing: S. 1732 and my amendment to the Cybersecurity Act of 2012 (S. 3414), which we are currently considering on the Senate floor. Protecting Americans' privacy is a bipartisan issue that I hope my colleagues will continue to advance in the years to come.

-END-