Protecting Personal Information: Is the Federal Government Doing Enough?
Homeland Security and Governmental Affairs Chairman Joe Lieberman
June 18, 2008

Good morning and welcome to our hearing today on federal efforts to protect personal privacy. I want to welcome our distinguished panel and also commend the Government Accountability Office for its excellent work on this issue, as reflected in their report being released today on the federal government's privacy efforts. I also want to thank my colleague, Senator Akaka, who has taken a particular interest in government privacy issues and encouraged Senator Collins and me to convene today's hearing.

We live in an "information age," and the explosion of new technologies to gather, share, and store huge quantities of information has made possible huge advances in every aspect of our lives, including more efficient and effective government programs. But these same technologies have also dramatically altered the privacy landscape. It is easier than ever for government and private entities to acquire large amounts of personal information about people – information that can cause harm to those people if it is improperly used or disclosed.

For the individual, loss of privacy can lead to crimes such as identify theft or stalking. The dissemination or misuse of certain private data can also result in other harms such as loss of employment, discrimination, or unwarranted harassment or surveillance. Certainly, it is essential for government to collect and use personal information – for example to provide security, conduct law enforcement, or administer benefits. But we must strive to ensure that we tread carefully when dealing with the personal information of individuals and that we properly balance our many policy goals against potential incursions on privacy.

Congress constructed a foundation for respecting individual privacy within the federal government in the landmark Privacy Act of 1974 which seeks to prohibit unauthorized

disclosure of personal information, ensure the accuracy and relevance of information collected by the government, and provide individuals with access to their information and a means of redress for errors. Six years ago, that law was buttressed by the Electronic Government Act of 2002, which I introduced and had the privilege of guiding through this Committee on its way to becoming law. The E-Government Act requires that agencies analyze in advance the potential privacy impacts of new information systems and data collections, and minimize those potential risks. But we know there is more to do.

New technologies and data practices have overtaken some of the core definitions of the Privacy Act. For instance, the Act simply could not foresee the government's use of private data brokers with access to extensive personal information about individuals, and we need to ensure this practice does not become a serious end-run around the protections of the Privacy Act.

New policy demands – including some of the homeland security efforts that are of vital concern to this Committee – call for sharing information among a wider array of agencies. Security concerns combined with new technologies, such as biometrics, are also driving the collection of new types of personal information. Americans may have justifiable concerns about sharing their personal information when the government is collecting and storing their fingerprints, retinal scans, even their DNA. We need to look closely to see how these new programs and practices intersect with existing privacy law, and what adjustments may be necessary.

This Committee has recognized the need for dedicating officials and resources to address privacy concerns within government, particularly as we tackle challenging new missions such as homeland security. When we created the Department of Homeland Security, we mandated the establishment of a Chief Privacy Officer within the department to address what we knew would be challenging questions as to how to integrate privacy considerations – including

implementation of government privacy law – into the critical mission of homeland security. I am pleased that the second individual to hold that position, Mr. Teufel, is one of our witnesses today. We also created an expanded network of privacy officials as part of the two laws enacting recommendations of the 9/11 Commission.

But the question remains whether we have adequate leadership and resources devoted to privacy at the government-wide level. In 2003, in response to a request from this committee, GAO concluded that OMB needed to assert more leadership on privacy to ensure that agencies fulfilled the mandates of the Privacy Act and other government privacy law. In fact, there is no one in OMB, no office in the federal government, no high-level official, not even a political appointee or member of the Senior Executive Service, whose job it is to focus full-time on government-wide privacy policy. This stands in stark contrast to many other countries, including those in the European Union, which have elevated privacy policy to the highest levels of government. This absence of leadership is a message we will hear loud and clear today.

I look forward to the testimony and to working together to ensure that our privacy laws continue to provide appropriate and meaningful protections for our citizens. Senator Collins?

-30-