Statement of
Senator Susan M. Collins

Protecting Personal Information: Is the Federal Government Doing Enough?

Committee on Homeland Security and Governmental Affairs
June 18, 2008

★ ★ ★

We live in a world of unprecedented access to information. Data are being collected and stored in quantities of almost unimaginable size by a wide range of public and private entities. People freely share personal information about themselves on blogs or social networking websites. At the same time, most Americans believe that protecting some degree of personal privacy is a fight worth waging in the digital age.

In 1974, Congress passed the Privacy Act to establish rules for government's use of computerized record-keeping systems. In that same year, President Nixon resigned the Presidency in the wake of the

Watergate scandal. Gasoline cost 55 cents per gallon. And an exciting new gadget – the pocket calculator – was just beginning to appear on store shelves.

Thirty-four years later, six presidents have occupied the Oval Office, the average cost of gasoline exceeds $4 per gallon, and the Blackberrys that the Chairman and I depend on can do more than all but the most sophisticated computers of 1974. Yet with very few modifications, the 1974 Privacy Act has remained the primary law governing the federal government's collection, storage, and use of personal information about its citizens.

Obviously, technology has changed dramatically since the Privacy Act was written. The federal government can now gather, store, and share information more efficiently than was even imagined possible 34

years ago. Yet it is a testament to the original drafters of the Privacy Act that in spite of these significant advances in technology, many of its provisions remain applicable to the technology in use today.

Nonetheless, as the GAO and our other witnesses will testify, current law could be strengthened to improve assurances that personal information is legitimately collected and adequately secured.

We should build on the success of the original laws while ensuring that they are adequate to meet the new challenges of the Digital Age. We can accomplish this by remaining true to the principles of openness, accuracy, transparency, and accountability that underpin the Fair Information Practices, which were developed by the U.S. government and endure as guiding principles for

protecting the privacy and security of personal information.

This hearing will examine several important questions. First, are the rules governing the collection and use of personal information clear to both the officials who have access to it and the public that provides it? System of Records Notices, descriptions of routine uses of information, and other basic tools of the privacy regime are supposed to describe various information systems so that government officials and the public will know when and how personal information can be collected and shared by the government. In many cases, however, these tools are worded so broadly that they provide little clarity as to what rules govern any particular information system.

Second, how can we ensure the security of personal information collected and maintained by the U.S. government? Unfortunately, there are far too many recent examples that demonstrate the need for the federal government to better secure the sensitive information that it collects and maintains.

In 2006, the Department of Veterans Affairs reported that the personal information of approximately 26.5 million veterans was compromised when a laptop containing Department records was stolen. A 2007 study by the Inspector General for Tax Administration found that at least 490 laptops containing sensitive taxpayer data had been lost or stolen between 2003 and 2007. But lost or stolen laptops are not the only security concerns, as in a 2006 data compromise of employee information at the Department of Agriculture that was caused by unauthorized access to the agency's systems.

Beyond the physical- and cyber-security of sensitive data, we must also ask what is the best way to deal with innovative technologies – such as data mining – that seek to use information in entirely new ways. Technology develops so rapidly in this day and age that we will need to be vigilant to ensure that the wheels of progress are not inadvertently running over our basic privacy rights.

And, finally, how can we continue to encourage the sharing of information among government agencies for legitimate purposes while maintaining adequate controls to hold accountable those who might compromise an individual's privacy by misusing their personal information? The recent inappropriate searches by State Department contractors of the passport files of Senators McCain, Obama, and Clinton highlight the need for improvements in this area. Prohibitions against unauthorized use of the passport system did not prevent

these improper inquiries – though audit mechanisms did facilitate prompt administrative action against the contractors responsible. As the government searches for ways to improve the sharing and analysis of the information it collects, we must develop effective security measures and consider whether our laws properly sanction those who use sensitive information for inappropriate purposes.

This hearing is yet another step in a robust dialog now occurring about privacy in this country. A strong privacy regime, built on principles of transparency and accountability, should inspire the confidence of the American people that the federal government is not compromising personal privacy but rather preserving and protecting it.