Statement of

The Honorable Patrick Leahy

United States Senator
Vermont
October 27, 2005

Statement Of Senator Patrick Leahy
On The Personal Data Privacy and Security Act (Specter-Leahy)
Executive Business Meeting
Committee On The Judiciary
October 27, 2005

We have been working hard for some time to finalize the Personal Data Privacy and Security Act. I appreciate the Chairman's dedication to solving these challenging problems. We have worked closely with the members of the Committee, as well as a wide variety of stakeholders and experts to address their concerns, and have made substantial revisions. I especially thank Senator Feinstein for her dedication and resolve to address these difficult issues and in helping us reach a consensus bill. Passing this bill out of committee is long overdue.

I am pleased with some of the bill's developments. We refined the bill to focus on companies that maintain vast treasure troves of sensitive personal information. We protect information like Social Security numbers, mothers' maiden names, full dates of birth, and biometrics, such as fingerprints, DNA and iris scans. These changes cannot come soon enough. Just last week came the announcement that a company that aims to encourage people to use their fingerprints instead of credit cards is planning to buy the assets of CardSystems Solutions, the firm where more than 40 million credit card accounts were compromised. Today it's about losing credit card numbers, but tomorrow, the breaches could be even more invasive. There is no doubt that we need to continue our vigilance in securing this information.

Our bill requires companies that lose our sensitive information, or who are victims of hacking crimes, to tell us about it. We include numerous precautions to ensure effective individual notice where it is necessary, while avoiding over-notification.

We not only offer remedies to help individuals after they have been harmed. We also address the underlying problem of lax security and lack of accountability with baseline good security practices to make sure that these breaches do not happen in the first place.

We also address the challenges of the exploding market for sale of individuals' profiles and sensitive data. We have established a minimal framework that allows individuals to see the sensitive personal information that data brokers are selling about them, and where they can demonstrate inaccuracies, to correct those. We narrowly tailor the type of companies that must follow these rules to those that are truly trafficking in sensitive data, exempting certain fraud

tools, proprietary information, or less-sensitive marketing data. We also included important protections to make sure that individuals with fraudulent intent cannot abuse the system.

Finally, we address the important data security and privacy challenges raised by government use of commercial data. Our bill makes sure that data brokers doing business with the government have good security, and that the government's use of these commercial services is effective, based on accurate data, and includes appropriate protections against abuse and misuse.

But these benefits came at a great price. I am extremely disappointed about the scope of preemption in this bill. States have long been the laboratories for good consumer protections. My home State of Vermont was among the first - if not the first - to require individual consent before sharing financial information with third parties, and to require a person or business to obtain consent from individuals before reviewing their credit reports. If the states had been preempted on some of these data protections earlier, we would not have had a California notice bill and might never have heard about many of these breaches. I am especially concerned about the data security section, where we have preempted such a broad field while only providing limited requirements in return.

I am also disappointed that we have removed the protections for Social Security numbers and the government's use of commercial data to set up programs to screen Americans. We saw the problems with lack of accurate data and good procedures in the airline screening program. Just the other day, there was a report about a 62-year-old nun routinely detained for hours at the airport because a terrorist list could not distinguish between her and a male terrorist using the same last name.

We also had to sacrifice additional funding to help law enforcement agencies fight these crimes, particularly in the wake of other heightened demands on federal resources after Katrina.

But the package of reforms we present today to the Committee for consideration is important, and it is overdue. Technology has been swiftly advancing on several fronts in ways that present new challenges to the personal privacy and data security that we all used to take for granted. Guidance and guidelines to protect Americans' privacy have not kept pace. This effort helps remedy that neglect.