Statement of

The Honorable Patrick Leahy

United States Senator
Vermont
April 13, 2005

STATEMENT OF SENATOR PATRICK LEAHY,
RANKING MEMBER, COMMITTEE ON THE JUDICIARY
HEARING ON "SECURING ELECTRONIC PERSONAL DATA: STRIKING A BALANCE
BETWEEN PRIVACY AND COMMERCIAL AND GOVERNMENTAL USE"
APRIL 13, 2005

I am pleased the Committee is turning its attention today to the challenges we face in securing electronic personal data in a digital era. Earlier this year I wrote to the Chairman and requested this hearing, and I appreciate his receptiveness, interest and prompt agreement.

I welcome the witnesses here today and look forward to their testimony. Our colleague, Senator Feinstein, has been a leader on these important issues and I look forward to hearing of her efforts to date, and Senator Schumer and other members of our Committee, as well as Senator Nelson on Commerce, have also followed these issues closely and have insights to offer. I am also pleased to see here today my old friend and fellow Vermonter, Bill Sorrell, who is the Attorney General of Vermont and now is president of the National Association of Attorneys General.

Personal Information, A Hot New Commodity

In the past few months, we have become aware of a string of major security breaches involving large firms such as ChoicePoint, Bank of America and Seisint, a LexisNexis subsidiary. These incidents demonstrate the susceptibility of our most personal data to relatively unsophisticated scams and logistical mishaps, and they raise broader concerns about the misappropriation of personal information and identity theft. The ChoicePoint breach was especially troubling for its highlight of a dangerous vulnerability in the information economy - the inadequate screening of the customers who are buying this personal information. ChoicePoint's bread-and-butter business includes identity verification and screening to help corporate America "know its customers." Yet the company failed to know its own customers and sold personal information on at least 145,000 Americans to criminals posing as legitimate companies.

Advanced technologies, combined with the realties of the post-9/11 digital era, have created strong incentives, opportunities and a robust market for collecting and selling personal information about each and every American. Today, all types of corporate and governmental entities routinely traffic in billions of digitized personal records about Americans. The sudden rise of giant data brokers has brought much of this information together for centralized access. We rely on this data to facilitate financial transactions, provide services, prevent fraud, screen employees, investigate crimes, and find loved ones. In today's security-saturated environment, our own government is using it to "know its residents."

These advances have improved our lives and made us safer. But in this era where personal information has become a key commodity, the personal information of Americans has become a treasure trove, valuable and vulnerable, and our privacy and security laws have not kept pace.

Increasingly, those who trade in digital dossiers have no direct relationship with the individuals and faces behind the numbers or letters that identify them, so the normal market discipline of disgruntled consumers does not necessarily save the companies from themselves. Even where there is a direct relationship, individuals often have no idea what companies are doing with their personal data or even what kinds of information is being collected about them. What are these companies doing with this information, who do they sell it to, and why? How is it protected? What are the

benefits for Americans whose information has become a new commodity? These are all questions that too often go unanswered, with unfortunate, and sometimes tragic, results.

An example of tragic consequences from the misuse of personal data is the case of Amy Boyer. In 1999, a man who had been obsessed with her since high school bought Amy's Social Security number, work address and other information from data broker Docusearch for $154. He used the information to track her down and one day came up to her as she was leaving work and fatally shot her, just before killing himself.

In this information-driven age, the use of personal data has significant consequences for every American. People have been refused jobs because a database search has wrongly reported that they have a criminal history. For others caught up in the endless cycle of watching their credit unravel, undoing the damage caused by security breaches and identity theft becomes life-consuming. Last year, 9.3 million Americans fell victim to identity theft, resulting in losses of more than $52 billion to individuals and corporations. And on average, it took 28 hours to sort out the subsequent problems, and much, much longer for many victims.

Sophisticated Scams In The Digital Age

While dumpster-diving is still a popular method of data theft, increasingly the focus is on a new low-hanging fruit: insecure, where one good "hit" nets troves of information. Insecure databases are now low-hanging fruit for hackers looking to steal identities or otherwise misuse data for financial gain. This is especially true as more and more of Americans' personal information is being processed abroad. Just this past weekend, it was reported that individuals working for an Indian data processor stole personal information of Citibank customers and transferred $350,000 to fake accounts. Last year was the report that a Pakistani transcriber of medical files from a San Francisco hospital threatened to post that information on the Internet unless she received back pay.

In yet another strain of cyber crime and high-tech law-breaking, we are seeing a rise in organized rings that target personal data to sell in online, virtual bazaars. These are not your run-of-the-mill criminals. They increasingly have sophisticated computing skills and steal data using a full suite of malicious software, or "malware," such as Trojan horses, keystroke logging, spyware, and phishing, which I recently introduced a bill (S.472) to combat.

A recent investigation by the U.S. Secret Service revealed that one criminal group with some 4,000 members - Shadowcrew -- traded more than one million stolen credit-card numbers, resulting in financial losses of more than $4 million. These are challenging scams to penetrate, and I appreciate and applaud all the work that the Secret Service and other federal agencies have been doing to crack these cases. Just recently, the Senate Sergeant of Arms posted guidance on identity theft on the Senate website.

State and local law enforcement have also worked tirelessly to combat cyber challenges. I know in Vermont, the U.S. Small Business Administration will be hosting a forum to protect small businesses from the impact of scams and identity theft.

Identity theft is a major problem, but when the government is the purchaser of personal data, citizen inconveniences have also arisen, and the stakes can be far higher. We have all heard stories from everyday individuals, as well as colleagues like Senator Kennedy, about the airline passenger screening programs that use incomplete or bad data to peg innocent individuals for delay or denied boarding.

Protecting National Security As Well As Financial Security

Weaknesses in the data industry can also jeopardize our law enforcement and homeland security efforts. Government contractors providing critical data and processing tools must get it right. Protecting our borders requires that we prevent security breaches, especially as we outsource data abroad, that would allow a potential terrorist to steal Social Security and account numbers and masquerade as law-abiding residents, or simply fund their criminal enterprises. We also need to know that data brokers are safeguarding the secrecy of law enforcement investigations and operations where necessary. For example, we need to ensure that there are no technological weaknesses in the data brokers' systems that are supposed to prevent their employees from viewing FBI data searches and suspects the Bureau is investigating.

Our hearing today is not about shutting down these data brokers or abandoning their services. It is about shedding a little sunshine on current practices and weaknesses, and establishing a sound legal framework to ensure that privacy, security and civil liberties will not be pushed aside in this new and evolving age.

Today will be an opportunity to address these concerns as we hear from some of the industry's leaders, ChoicePoint, Acxiom and LexisNexis. These companies play a legitimate and valuable role in the information economy. Their data services facilitate important commercial transactions, improve hiring decisions, deter fraud, assist law enforcement and enhance homeland security. But as with any other significant beneficial industry, the information industry is subject to mistakes, abuse, and unintended consequences that can flourish absent transparency, oversight and proper boundaries.

Although we are focusing today on several leading data brokers, many other companies that traffic in personal data use much lower standards than the companies that have agreed to come under the spotlight today. For example, Docusearch, the company that sold Amy Boyer's personal information to her killer, has said it has no duty to check its customers' backgrounds. This past December, CNN interviewed the founder of Abika, an Internet-based company that performs some three million background searches annually and creates psychological profiles. He said, "I don't even believe in privacy too much . . . why do we need privacy? That's the question . . . why do people need privacy?"

That kind of sentiment is outrageous and is not one that should be tolerated in the data industry. But I will answer the question. One of the most fundamental liberties of being an American is the right to be let alone, and when you invade someone's privacy or treat it glibly, you trample on that liberty. That's why we need privacy, and that's why we should vigilantly protect it.

A Role For Congress

Congress has a role in protecting Americans' privacy, but we need to do it right. Senator Specter and I, as well as many others on the Committee, have been examining these issues closely to ensure a carefully balanced environment that can evaluate the adequacy of current boundaries and behaviors in the realm of data brokering.

We need to consider rules that will guarantee Americans the right to see what information has been collected about them and to make corrections where necessary. We need to consider rules that will ensure Americans are notified when there has been a security breach involving their digitized personal information. We also need to create baseline expectations for data security programs and practices, and penalize government contractors that don't comply. We also need to look at how to protect increasingly public, yet vulnerable, sensitive data such as Social Security numbers, which are the keys to unlocking so much of our financial and personal lives. A computer glitch at another payroll company, PayMaxx, allowed any of its customers to see thousands of W-2s of other company clients, including social security numbers and salaries. Just this past week, it was reported that "Automatic Data Processing," a company that provides payroll and benefits to corporations, mailed out postcards to 1000 workers with their Social Security numbers brazenly visible for anyone to see. Worse still, they described in detail how those Social Security numbers could be used to access employee benefits online. This should not happen. We must have a national dialogue on when and how Social Security numbers can be properly used.

Finally, we need to take a closer look at how the government is using commercial data, and whether those uses properly balance privacy and civil liberty concerns. Recently a ChoicePoint executive was quoted as saying, "We do act as an intelligence agency, gathering data, applying analytics." These partnerships between governments and private data brokers create new challenges for maintaining privacy standards over sensitive information involving each and every American.

With such powerful information-age tools comes heightened responsibility. As the 9/11 Commission noted, "...we must find ways of reconciling security and liberty, since the success of one helps protect the other." No doubt, the information industry can enhance law enforcement and homeland security efforts. But as the Commission also recognized, "while protecting our homeland, Americans should be mindful of threats to vital personal and civil liberties. This balancing act is no easy task, but we must constantly strive to keep it right." We can "keep it right" by putting mechanisms in place to ensure appropriate checks and balances and congressional oversight.

We have many issues to consider on this front. Today's hearing will begin that process by shedding much-needed light on a rapidly growing industry and its practices of handling the most personal information of each and every American.