Statement of

The Honorable Russ Feingold

United States Senator
Wisconsin
April 13, 2005

Statement of Senator Russell D. Feingold
Senate Judiciary Committee Hearing on
"Securing Electronic Personal Data: Striking a Balance
Between Privacy and Commercial and Governmental Use"

April 13, 2005

Mr. Chairman, thank you very much for holding this hearing today. This is an extremely important issue, and one that I am very pleased the Judiciary Committee is taking up.

Recent security breaches at companies like ChoicePoint and Lexis-Nexis, which collect and sell information about individuals, have placed the identities of hundreds of thousands of Americans at risk. Congress needs to understand how and why these security breaches happened, something I hope we can begin to accomplish at today's hearing, and whether a new legal regime is needed. There is no question that data aggregators provide valuable services, allowing consumers to obtain instant credit and police officers to locate suspects. But these companies also gather a great deal of potentially sensitive information about individuals, and in many instances they go largely unregulated.

However, this is about much more than just information security. Until California law required ChoicePoint to notify individuals that their information was compromised and they might be vulnerable to identity theft, many Americans had never heard of this company. As news stories focused on the data broker business, many Americans were surprised to discover that companies are creating digital dossiers about them that contain massive amounts of information, and that these companies sell that information to government and business entities. The revelations about these security breaches highlighted that Americans need a better understanding of what happens to their information in a digital world - and what kind of consequences individuals can face as a result.

In particular, I am concerned about an aspect of the data broker business that has not yet gotten much attention in the wake of these security breaches. The information gathered by these companies is not just sold to individuals and businesses; law enforcement agencies like the FBI also buy or subscribe to information from commercial sources.

While I believe the government should be able to access commercial databases in appropriate circumstances, there are no existing rules or guidelines to ensure this information is used responsibly. Nor are there any restrictions on the use of commercial data for powerful, privacy-intrusive data mining programs. The Privacy Act does not apply because the information is held outside the government and is not gathered solely at government direction.

As a result, there is a great deal we do not know about government use of commercial data, even in clearly appropriate circumstances such as when the agency's goal is simply to locate an individual already suspected of a crime.

We don't know under what circumstances government employees can obtain access to these databases or for what purposes. We don't know how government agencies evaluate the accuracy of the databases to which they subscribe, or how the accuracy level affects government use of the data. We don't know how employees are monitored to ensure they do not abuse their access to these databases, or how those who misuse the information are punished. We don't know how government agencies, particularly those engaged in sensitive national security investigations, ensure that the data brokers cannot track the individuals about whom the government is seeking information, an issue that is particularly important in light of the security problems we are talking about today.

The lack of information about government use of commercial data is even more worrisome in the context of data mining programs. A government law enforcement or intelligence agency searching for patterns of criminal or terrorist activity in vast quantities of public and private information raises serious privacy and civil liberties issues - not to mention questions about the effectiveness of these types of searches. More than two years after Congress first learned about Total Information Awareness, there is still much we do not know about the federal government's other work on data mining.

That is why I am planning to reintroduce in the next few days my Data Mining Reporting Act, which would require all federal agencies to report to Congress on data mining programs used to find a pattern indicating terrorist or other criminal activity and how these programs implicate the civil liberties and privacy of all Americans. The bill does not end funding for any program, does not determine the rules for use of the technology or threaten any ongoing investigation that uses data mining technology. But it would allow Congress to conduct a thorough review of the costs and benefits of the practice of data mining and make considered judgments about which programs should go forward and which should not.

I am glad that this hearing gives us an opportunity to explore both government and commercial reliance on data brokers, and I look forward to working with my colleagues on the Committee to develop legislation to address these issues.