Statement of

The Honorable Edward Kennedy

United States Senator
Massachusetts
January 10, 2007

Statement of Senator Edward M. Kennedy
Senate Judiciary Committee Hearing on "Balancing Privacy and Security: The Privacy Implications of Government Data Mining Programs"
January 10, 2007

Mr. Chairman, I commend you for holding this hearing and for your dedication to ensuring that our citizens' privacy and civil liberties are not unnecessarily or unjustifiably violated in the battle against terrorism.

Terrorism is the greatest challenge we face today as a nation. We all agree on the need for strong powers to investigate terrorism, prevent future attacks, and improve information-sharing by federal, state and local law enforcement. But legitimate concerns about the terrorist threat should not be misused as an excuse to grant extraordinary and unchecked powers to the President.

Modern technology holds great promise for meeting all the challenges we face, but we can't afford to overlook the new encroachments on privacy and our civil liberties that such technology now makes possible. We must not sacrifice core American values in our battle against terrorism, for there can be no victory at the cost of these ideals.

It is the duty of Congress to ensure that the proper balance is achieved between realizing the promise of technology and safeguarding civil liberties and the right to privacy. The Bush Administration is not entitled - nor should it expect - a blank check when it comes to fighting terrorism. We don't question the sincerity of the Administration in wanting to protect the American people against new terrorist attacks. But it is our responsibility to conduct meaningful oversight over the judgments and methods involved.

For these reasons, last Congress I urged my colleagues to adopt an amendment that would have required the Administration to tell Congress what the National Security Agency is doing. My amendment would have merely required that the NSA report to Congress on the legal standards used for electronic surveillance within 60 days after the enactment of this bill. My amendment was identical to a requirement sponsored by one of the Committee's witnesses' today, former Representative Bob Barr, and adopted with unanimous bipartisan support in the 106th Congress. Now, a few years later, the Congress and the American people are still entitled to know what standards the NSA is observing in conducting electronic surveillance.

As part of the 2000 Intelligence Authorization Act, the Congress mandated that the National Security Agency report on the legal standards that it was using to conduct surveillance on U.S. soil. At that time, many in Congress were concerned about rumors that the NSA was engaging in

broad eavesdropping, and language requiring the Attorney General and the Director of National Intelligence to report on the standards used for electronic surveillance was adopted - without a single objection in either the House or the Senate. Based on public reports now, the NSA had not begun its so-called "Terrorist Surveillance Program" at the time that it provided its report to Congress on the legal standards being used. The Administration owes us a current answer on how they define the playing field. Unfortunately, the Committee did not adopt my amendment last year but now we have another opportunity to press ahead and today's hearing is a good start.

The Administration has repeatedly betrayed the public trust with its broad interpretation of Executive power and authority. This President thinks it's permissible to listen in on our phone conversations and read our mail - without any Congressional or judicial oversight. At the time the Foreign Intelligence Surveillance Act was enacted in 1978, the President and Congress concluded that our national security laws are toughest when they are clear and meet the test of common sense. Without such guidance, the actions of national security officials and law enforcement officials will be subject to frequent challenge in the courts.

Today, however, we face the unsettling prospect that there are no clear rules for the government's national security actions or data collection.

Our common concern for national security can best be met when the President and Congress work together to approve the means he uses to keep us safe. But instead of uniting us to strengthen our national security, the Administration has taken its own controversial and divisive course. Instead of working with Congress to improve our laws, the President has chosen to ignore them and ride roughshod over basic constitutional principles.

Already, the Administration has had to terminate its data mining programs, after details of their operation came to light. The Pentagon's Terrorism Information Awareness program, formerly known as the Total Information Awareness program, was dropped in the face of legislation aimed at ending the program. The Transportation Security Administration's passenger prescreening program was stopped after lawsuits were filed by passengers challenging the sharing of their personal information between commercial airlines and the TSA. Another concern was TSA's stated intention to use the information it collected for purposes other than fighting terrorism, such as to identify individuals with outstanding warrants or expired visas.

Data mining is a developing technology that may prove effective in fighting terrorism without unduly compromising privacy and civil liberties. But we need more information. It's time for the Administration to give us an accounting of all its data mining programs currently in existence. We need to know the answers to many questions about these programs. Are they effective? Are the costs - in terms of dollars and privacy - worth it? Where is the data coming from? Who is collecting it? Is the data captured accurate and complete? For what purposes is the information used? Who has access to it? What safeguards are in place to ensure that the desire for information does not trample upon our basic rights? Are there safeguards to ensure that groups, such as Arab Americans or Muslims, are not targeted unfairly? Are these safeguards effective? We have a long list of questions and today's hearing is a welcome start to obtaining meaningful answers.

As we look forward to further debate on this important topic during the 110th Congress, I'd like to remind my colleagues that the Administration is required to submit a report to Congress on its current data-mining activities by March 9, 2007. When we reauthorized the PATRIOT Act, Congress established a requirement for the Attorney General to report to Congress regarding the Department of Justice's use or development of data mining technologies - within one year of the date of the enactment of the reauthorized PATRIOT Act. I expect that the Administration will meet the statutory deadline so that we will finally have more detailed information on their current practices and procedures.

I look forward to today's testimony and to new and more vigorous oversight by the Judiciary Committee under the leadership of Chairman Leahy. Across party lines, many of us stand ready to improve our surveillance laws to serve our country's best interests. It would be wrong for Congress to continue to rubber stamp programs that will change the law in far-reaching ways and produce devastating losses of basic constitutional freedoms and protections. Now more than ever, we must be vigilant in our defense of safeguards that limit the President's power to collect and store vast amounts of information on Americans.