Testimony of

The Honorable Robert Barr

Chief Executive Officer
Liberty Strategies, LLC
January 10, 2007

Testimony concerning the Privacy Implications of Government Data Mining Programs by Robert Barr
Chief Executive Officer
Liberty Strategies, LLC

Thank you for inviting me to this first oversight hearing of the Senate Judiciary Committee in the 110th Congress. I am extremely pleased that Congress is finally asking hard questions about the impact of the administration's security policies on Americans' privacy and civil liberties. This dialogue is long overdue.

As a former member of Congress, I have been disappointed to see the Congress shirk its responsibility to the American people and sit silently by while the Constitution is gutted of meaning.

As chairman of Patriots to Restore Checks and Balances, an alliance of individuals and organizations - conservatives and liberals - committed to upholding the Constitution, I have worked with many Republicans and Democrats to do what is right for the American people. I appreciate the opportunity to talk today about the constitutional questions raised by the federal government's data-mining practices.

It is unconscionable that ordinary Americans' jobs and finances - their entire lives - are at risk because they do not know what information the government is collecting about them; or what it is doing with that private information; or who government is sharing the information with. And if that information is wrong, they have no way of knowing about it, no way of seeing it, and no way of correcting it.

Data mining presents many serious threats to the First, Second, Fourth and Fifth Amendments to the Constitution. That is nearly half of the Bill or Rights! Where will this end? With the repeal of the Constitution so that the White House won't have to worry about those inconvenient and troublesome laws any more?

The federal government constantly is taking in huge amounts of information on Americans from many sources; some of these databases are known, some are not; some may be lawful, others not. Every month there is a new revelation. Last week we learned that the administration wants to open our mail at its discretion, in addition to listening to our phone calls and reading our e-mails without court order.

Just weeks earlier the Department of Homeland Security admitted that its Secure Flight program to screen domestic air passengers violated the Privacy Act. Just prior to that, we learned that Customs and Border Patrol was using the Automated Targeting System, designed initially for cargo security, to assign a terror risk score to travelers entering the United States. Anyone in this room who has traveled abroad in recent years is likely in this system. And their records will be kept for 40 years.

States will soon begin to implement the Real ID law, creating a national registry of tens of millions of drivers. Accessible to officials across the nation, this database, currently being finalized for implementation in 2008, is almost certain to contain individuals' fingerprints, photo, Social Security number, immigration status and more (possibly including other biometric data and an RFID chip).

We learned recently the FBI has been using "national security letters" to excess; in one example, using this easy way to demand access to private data, to collect information on nearly 300,000 people who did nothing more suspicious than that they spent the Christmas holiday in Las Vegas. Who knows how many other instances of mass data collection have occurred in the past few years, all in the name of national security? The government is re-analyzing perfectly lawful behavior through unproven data-mining programs and bringing vast numbers of innocent Americans under suspicion.

Adding insult to injury, there is no scientific proof that data-mining to identify terrorists even works. No scientist has ever demonstrated that the government can predict who will commit an act of terror at some future time. Yet, the government spends tens of billions of taxpayers' dollars on data-mining programs each year --collecting, manipulating, retaining and disseminating the most personal and private information on unknowing American citizens and others.

Chilling effects on ordinary Americans necessarily follow. For example, an individual decides to learn Arabic to help their country fight terrorism. They travel to an Arabic speaking nation such as Egypt, which maintains close and cooperative ties with the U.S., to study the language, but when they come home and apply for a job with the federal government, they can't pass the background check because a database, perhaps the Automated Targeting System, shows that they traveled to Egypt. This just isn't right, and it may very well be counter-productive. Data-mining, therefore, has the propensity to make us more vulnerable, not safer.

Data-mining undermines the First Amendment guarantees for freedom of association. Using link-analysis data mining, a person can easily be found guilty by association. This means that anyone who comes into contact - even incidental contact - with a person whose name appears on some list as a terrorist suspect, become a suspect themselves. Once a person is linked to a terrorist, it is virtually impossible to clear his or her name - if they even know they have come under suspicion.

The First Amendment also implies a right to travel and to move freely throughout society. However, when the simple fact of traveling puts people under suspicion, then they may very well curtail or stop traveling for business and other purposes to avoid the hassle of extra scrutiny at the airport or being put on a "watch list."

Concerns about data-mining relate to other of our rights guaranteed by the Bill of Rights. For example, I am deeply concerned about data mining threatening the Second Amendment right to bear arms. Although the government is prohibited by law from creating a national registry of gun owners, it can purchase records from data brokers that in a sense provide this information. This is also a problem under the Real ID Act, which will contain all sorts of data the average applicant for, or holder of, a state drivers license, possibly including information on firearms records. The government will claim it isn't creating a "registry," it is just analyzing data, and they will have circumvented the registry prohibition. Perhaps the nation's farmers who buy nitrate-rich fertilizer will also end up in the data mining programs and come under suspicion without reason.

Data mining is also entirely incompatible with the Fourth Amendment prohibition on unreasonable search and seizure. Our justice system and ability to prosecute suspects is based on crimes that have been committed or planned. It is absurd for the government to use databases to predict individuals' future acts. We do not live in the Hollywood movie scenario depicted in Minority Report, where law enforcement halts "pre-crimes" before they happen, yet the practice of government data-mining, which collects personal information on citizens and other persons often without any suspicion or evidence they have done anything wrong, grows exponentially; a practice undermining the very rights supposed to be protected by the Fourth Amendment.

The Fifth Amendment's Due Process Clause requires that the government tell Americans what personal information is collected about us, how it is being used, and to provide a right to challenge and correct erroneous information that wrongly could be used to deny us our rights and privileges. Yet, none of these shadowy data mining programs provides such a process.

I urge this committee and Congress to consider seriously strict laws to regulate data-mining by government and private industry, and provide oversight concerning their government contracts, so that government agencies are not able to evade federal laws that provide at least some protection against abuse; laws such as the Privacy Act and the Freedom of Information Act. The point here is not to unduly restrict or prohibit the accumulation or analysis of commercially-relevant data for legitimate business purposes. Rather the goal should be to ensure the process possesses a necessary degree of transparency, that it provides essential privacy protection for the consumer, and that such databases are not a tool whereby government can circumvent the law or the requirements of the Bill of Rights.
Funding for the Total Information Awareness system and other discredited programs may have been cut off because of privacy concerns, but other heads of the beast have sprung up in its place with new names. These programs have no greater safeguards for Americans' privacy and should also be ended.

Finally, I urge the committee to re-introduce and pass the Personal Data Privacy and Security Act and the Federal Agency Data-Mining Reporting Act in the 110th Congress.

Thank you again for having me here today. I look forward to working with the committee over the next two years on these important issues.