Testimony of

Dr. James Jay Carafano

Assistant Director, Kathryn and Shelby Cullom Davis Institute for International Studies; Senior Research Fellow, Douglas and Sarah Allison Center for Foreign Policy Studies
Heritage Foundation
January 10, 2007

STATEMENT OF

DR. JAMES JAY CARAFANO

SENIOR RESEARCH FELLOW
THE HERITAGE FOUNDATION

BEFORE THE SENATE JUDICIARY COMMITTEE

PROMOTING SECURITY AND CIVIL LIBERTIES:
THE ROLE OF DATA MINING IN COMBATTING TERRORISM

JANUARY 10, 2007

Mr. Chairman and other distinguished Members, I am honored to testify before you today.1 In my testimony, I would like to: 1) describe the nature of the challenge facing Congress; 2) offer a set of principles for both enhancing counterterrorism programs and protecting civil liberties; and 3) suggest how these principles should be applied to the employment of data mining technologies.

Between Liberty and Order

Even though I appreciate the opportunity to testify before the committee, I must state at the outset that I reject the premise of this hearing. It is wrong to conceptualize the government's task as an effort to "balance" preventing terrorist attacks and protecting the liberties of individual citizens. Such a paradigm implies making trade-offs. Indeed, the late Supreme Court Justice William Rehnquist suggested that in time of war compromises had to be made. He wrote:

In any civilized society the most important task is achieving a proper balance between freedom and order. In wartime, reason and history both suggest that this balance shifts in favor of order--in favor of the government's ability to deal with conditions that threaten the national well-being.2

Yet in a long war, where societies must remain secure, free, and prosperous in order to compete and thrive, shifting the balance between liberty and order is fraught with danger.3 This is particularly true when facing a protracted terrorist threat. One clear advantage for any country facing a determined enemy is a strong civil society. A resilient populace can better resist the fear,

doubt, and despair that terrorists try to sow. Paradoxically one of the great fears of fighting terrorism is that civil society will become the first casualty--that efforts to add security and forestall attacks will undermine the liberties that make societies free and strong to begin with. To frame the fight against terrorism as a choice between safety and freedom offers a false choice. The most effective way to wage a war on terrorism is to adopt policies that secure both safety and freedom equally well.

Freedom from Fear

There has, however, been a concerted effort since September 11 to make the case that enhancing security and protecting freedoms are mutually exclusive. There are three factors animating fears about anti-terrorism campaigns.

? First, critics frequently decry the expansion of executive authority in its own right. They generically equate the potential for abuse of executive branch authority with the existence of actual abuse. They argue that the growth in presidential power is a threat, whether or not that power has, in fact, been misused. These critics come from a long tradition of limited government, which fears any expansion of executive authority.

? The second kind of criticism is stimulated by the "Luddite response"--a fear of technology. As the government begins to explore ways of taking advantage of the information age's superior capacity to manage data through new information technologies, there are rising concerns that it will use these means intrude into our personnel lives. Information equals power. With great efficiency comes more effective use of power. And with more power comes more abuse.

? A third theme underlying criticism is more blatantly political. Take, for example, the passage of the first major post-9/11 anti-terrorism law in the Unites States, popularly called the Patriot Act. The Patriot Act, regardless of its true merits or laws, has been a cause célèbre for raising money and energizing constituencies that are predisposed to be critical of the Bush Administration's response to terrorism. Brand labeling has become a part of the political process.4

One key task of understanding how well government policies affirm the dual priorities of liberty and order is distinguishing real conflicts in achieving both from merely rhetorical arguments that are more concerned with advancing ideological and political agendas than adopting security measures to keep people safe, free, and prosperous.

The Reality of Terrorism

Simply arguing against adding security out of the fear that it might encroach on individual liberties might be prudent if there were no real threats to be addressed. That, however, is not the case. The sad truth is that terrorism remains a potent threat to international security. All we know for sure is that no one can say with much certainty how many terrorists with aspirations of waging transnational war there are, where they are, and what they are planning. Virtually every terrorism expert in and out of the government believes there is a significant risk of more attacks.

In addition, we know that an efficacious defense against terrorism will not be accomplished by military power alone. Rather, effective law enforcement and intelligence gathering are essential

instruments. Equally important, this is policing of a different form--preventative rather than reactive.

An understanding of the nature of the terrorist threat helps to explain why the traditional law enforcement paradigm needs to be modified and why government can't avoid its obligation to advance both liberty and order. The traditional law enforcement model is highly protective of civil liberty in preference to physical security. All lawyers have heard some form of the maxim "It is better that ten guilty persons go free than that one innocent person be mistakenly punished."5 This embodies a fundamentally moral judgment that when it comes to enforcing criminal law. This dictum, however, does not suffice when considering matters of national security in which the state has a dual responsibility to protect both the individual and the people.

Principles for Preserving Security and Civil Liberties

Although a large portion of the debate about new law enforcement and intelligence measures focuses on perceived intrusions on human liberties, we should keep in mind that good governance weighs heavily on both sides of the debate. Thus, as we assess questions of civil liberty and human rights, we cannot lose sight of the dual purpose of government--protecting personal and national security. So how do we square the circle?

What we need for the war on terrorism is a set of principles that work for this long war, principles that are consistent with good governance that give us the tools we need to get the terrorists before they get us. The "?rst" principles that I have advocated for include:

? No fundamental liberty guaranteed by the laws of a sovereign state can be breached or infringed upon. This should include the protection of human rights guaranteed by international treaties, which when ratified by the state have the force of national law.

? Any new intrusion must be justi?ed by a demonstration of its effectiveness in diminishing the threat. If the new system works poorly by, for example, creating a large number of false positives, it is suspect. Conversely, if there is a close "?t" between the technology and the threat (that is, if it is accurate and useful in predicting or thwarting terrorism), the technology should be more willingly embraced.

? The full extent and nature of the intrusion worked by the system must be understood and appropriately limited. Not all intrusions are justified simply because they are effective. Strip searches at airports would prevent people from boarding planes with weapons, but at too high a cost.

? Whatever the justification for the intrusion, if there are less intrusive means of achieving the same end (at a reasonably comparable cost), the less intrusive means ought to be preferred. There is no reason to erode Americans' privacy when equivalent results can be achieved without doing so.

Any new system developed and implemented must be designed to be tolerable in the long term. The War on Terrorism is one with no immediately foreseeable end. Thus, excessive intrusions may not be justi?ed as emergency measures that will lapse upon the termination of hostilities.

Policymakers must be restrained in their actions; Americans might have to live with their consequences for a long time.

Rules for New Technologies

Because technology is going to be an important part of any set of counterterrorism tools, and because our lives in the information age are so dependent on many of the systems and databases in which these technologies will look for information about terrorists, we also need a set of rules to guide how we implement the basic principles of long-war fighting in the electronic world. This is what these principles should look like:

? No new system should alter or contravene existing legal restrictions on the government's ability to access data about private individuals. Any new system should mirror and implement existing legal limitations on domestic or foreign activity.

? Development of new technology is not a basis for authorizing new government powers or new government capabilities. Any such expansion should be independently justi?ed.

? No new system that materially affects citizens' privacy should be developed without specific authorization by the people's representatives and without provisions for oversight of the system's operation.

? Any new system should be, to the maximum extent practical, tamper proof. To the extent the prevention of abuse is impossible, any new system should have built-in safeguards to ensure that abuse is both evident and traceable.

? Any new system should, to the maximum extent practical, be developed in a manner that incorporates technological improvements in the protection of civil liberties.

Finally, no new system should be implemented without this full panoply of protections against its abuse.

Application to Employing Data Mining Technologies

First, we must always protect liberties guaranteed by the Constitution. From a practical perspective, there are two distinct types of constitutional violations to be avoided. It should go without stating, but we must never countenance intentional or systemic constitutional violations. In other words, we should design every data-mining system so that, if properly used, it will never violate constitutional rights.

Nevertheless, even an information system that is properly designed using state-of-the-art technologies and privacy safeguards can carry the potential for misuse and abuse. Our goal in the second instance must be to remain vigilant to prevent, identify, and appropriately punish such violations. Inadvertent or negligent violations should be punishable by civil penalties. Intentional violations should be punishable by both civil and criminal penalties.

Second, any imposition on a valid privacy interest by a data-mining program must be justified by the severity of the threat. Standards should be developed for assessing and comparing the relative

severity of various threats. Federal departments and agencies should adopt and implement these standards widely and uniformly. Standardization poses the risk of a widespread over-estimate or under-estimate of a particular threat's severity, but the alternative is a flying-by-the-seat-of-the-pants approach that cannot be properly vetted or tested.

Similarly, any new intrusion must be justified by a demonstration of the data-mining program's effectiveness in diminishing the terrorist threat. If the new program works poorly by, for example, creating a large number of false positives, it should be considered suspect. Conversely, if there is a close "fit" between the technology and the threat (that is, for example, if it is accurate and useful in predicting or thwarting terrorism), the technology should be more willingly embraced.

Third, we must understand and limit the imposition on privacy interests. The full extent and nature of the intrusion worked by the system must be understood and appropriately limited. Intrusions should not be justified simply because they are effective.

Fourth, we must strive to develop methods and systems for data mining that are--of the reasonable and feasible alternatives--the least intrusive upon privacy rights. There is no reason to erode Americans' privacy when equivalent results can be achieved without doing so.

Moving Forward

There is clearly a roll for Congress in advancing the use of data mining and other information technologies and ensuring they are employed in an appropriate manner. Establishing federal guidelines for the use of these technologies is one way to address the issue. Such guidelines would begin by defining what programs should come under the scope of data-mining programs. The guidelines should also include the following elements:

? Every deployment of federal data-mining tech¬nology should require authorization by Congress;

? Agencies should institute internal guidelines for using data analysis technologies, and all systems should be structured to meet existing legal limitations on access to third-party data;

? A Senate-confirmed official should authorize any use of data-mining technology to exam¬ine terrorist patterns, and the system used should allow only for the initial query of gov¬ernment databases and disaggregate personally identifying information from the pattern analysis results;

? To protect individual privacy, any disclosure of a person's identity should require a judge's approval;

? A statute or regulation should require that the only consequence of being identified through pattern analysis is further investigation;

? A robust legal mechanism should be created to correct false positive identifications;

? To prevent abuse, accountability and oversight should be strengthened by including internal policy controls, training, executive and legisla¬tive oversight, and civil and criminal penalties for abuse; and

? The federal government's use of data-mining technology should be strictly limited to national security-related inves¬tigations.6

Congress should also require agencies to report on their intent to establish data-mining programs and require annual reports on their implementation, as well as their compliance with federal guidelines.

Thank you for the opportunity to testify on this important subject.

1. The title and affiliation are for identification purposes only. Staff of The Heritage Foundation testify as individuals. The views expressed are our own and do not reflect an institutional position for The Heritage Foundation or its board of trustees. The Heritage Foundation is a public policy, research, and educational organization. It is privately supported, receives no funds from government at any level, and performs no government or other contract work. The Heritage Foundation is the most broadly supported think tank in the United States. During the past two years, it had approximately 275,000 individual, foundation, and corporate supporters representing every State in the nation. Its 2005 contributions came from the following sources: individuals (63%), foundations (21%), corporations (4%), investment income (9%), publication sales and other sources (3%).

2. William Rehnquist, All the Laws But One: Civil Liberties in Wartime (New York: Knopf, 1998), p. 222.

3. See Chapter 3, "Between Liberty and Order," in James Jay Carafano and Paul Rosenzweig, Winning the Long War: Lessons from the Cold War for Defeating Terrorism and Preserving Freedom (Washington, D.C.: The Heritage Foundation, 2005), pp.79-97.

4. See MoveOn.org, "The Administration Is Using Fear as a Political Tool," The New York Times, November 25, 2003, p. A1. Their Web site offers a full-page ad reprinting excerpts of speeches by former Vice President Al Gore. It is no coincidence that many Democratic presidential aspirants garnered great applause with the "novel" suggestion that, if elected, they would ?re Attorney General John Ashcroft. See Carl Matzelle, "Gephardt Talks the Talk Steelworkers Want to Hear," Cleveland Plain Dealer, December 7, 2003, p. A24 (includes a promise to ?re Ashcroft "within [the] ?rst ?ve seconds" of new Administration); and Greg Pierce, "Inside Politics," The Washington Times, September 23, 2003, p. A6 (noting the "frenzy" of "Ashcroft bashing"). To the extent that criticism of the Patriot Act and related activities is purely political, the debate about these truly difficult questions is diminished. Thoughtful criticism recognizes both the new realities of the post-9/11 world and the potential for bene?t and abuse in governmental activity.

5. Furman v. Georgia, 408 U.S. 238, 367, n.158 (1972).

6. Paul Rosenzweig, "Proposals for Implementing the Terrorism Information Awareness System," Heritage Foundation Legal Memorandum No. 8, August 7, 2003, at www.heritage.org/Research/HomelandDefense/lm8.cfm.