February 15, 2013 at 9:00am
Congressional Hearing of the
Subcommittee on Oversight and Management Efficiency of the
Committee on Homeland Security of the
United States House of Representatives
311 Cannon House Office Building
Washington, DC 20515
Testimony of
James S. Gilmore, III
(Governor of Virginia, 1998-2002)
President & CEO,
The Free Congress Foundation
&
Former Chairman,
Advisory Panel to Assess the Capabilities for Domestic
Response to Terrorism Involving Weapons of Mass Destruction (1999-2003)
www.rand.org/nrsd/terrpanel

Topic: Ten Year Anniversary of The Department of Homeland Security (DHS): How Wisely is DHS Spending Taxpayer Dollars?

Introduction

Chairman Duncan, it is honor to be here today. I commend you and House Homeland Security Chairman Mike McCaul for holding these hearings on reviewing American Homeland Security policy as an institution for the 21st century and checking how wisely we are spending our taxpayer dollars. Communicating with the American public about the realities of terrorism and how well our country is prepared is essential to maintaining our liberty.

Since it is Abraham Lincoln's 214th birthday this week I think it is fitting to start my testimony with a quote from a great American leader: "America will never be destroyed from the outside. If we falter and lose our freedoms, it will be because we destroyed ourselves."

I was invited to testify due to my experience as the former Chairman of the Advisory Panel to Assess the Capabilities for Domestic Response to Terrorism Involving Weapons of Mass Destruction, also known as the "Gilmore Commission." From 1999 to 2003, the commission produced five reports on the state of our nation's ability to respond to terrorist attacks.

Of its 164 recommendations, 146 have been adopted in whole or in part. The commission thoroughly analyzed how the country achieved the goal of national security, as well as how our preparedness related to citizens' privacy and the role of the military. As I have said before, the agency with the most guns should not always be relied on in a crisis; we need to be prepared physically and emotionally when the attack comes and that is how we keep our freedom and security intact for future generations of Americans.

An assessment of the effectiveness of the DHS can only be made with reference to the strategic plan the department seeks to implement. The first question must always be whether the DHS budget and spending implements the national plan.

Our commission realized that small local communities are both the most vulnerable and the most difficult to secure, due to the higher need for private sector involvement. The commission indentified the "New Normal" and recommended that all communities adopt this plan. This program developed a plan of preparedness which could be carried out by the mayor or local homeland security officials. We outlined the following topics to help start the process for localities:

- Response/Containment
- Intelligence/Situational Awareness
- Transportation/Logistics
- Public Health/Medical
- Legal/Intergovernmental
- Public Safety/Information
- Infrastructure/Economic
- Community/Citizen

On a larger scale, the Congress and the Executive Branch should focus on the following in creating a National Plan:

- State, Local, and Private Sector Empowerment
- Intelligence
- Information Sharing
- Training, Exercising, Equipping, and Related Standards
- Enhanced Critical Infrastructure Protection
- Research and Development, and Related Standards
- Role of the Military

The influence of drugs and other illegal substances are a major threat to American National Security. The availability of narcotic poisons to our population is a key element that is weakening our communities. The routes used to traffick drugs can be used by Al Qaeda to bring terrorists and Weapons of Mass Destruction into our country. In addition to the external threat we must be sensitive to the damaging role of overreaction to our civil freedoms. Thu, we must be aware of the policy actions we have taken with The PATRIOT ACT and the National Defense Authorization Act (NDAA). We must always consider the ***role of the military*** during a major event like Sept. 11th as we decide on our future homeland policy.

One-Sentence Summary

The Gilmore Commission reports discuss preparedness - including strategies, institutions, threats, capabilities, and lessons from other nations.

Main Points

Point 1: We should plan strategically, especially at the state and local levels.

In a free society like our own, there is no way to completely eliminate the threat of terrorism. We have unlimited vulnerabilities, and the multitude of activities and motivations makes it difficult to assess terrorism threats. It is also difficult to assess whether our actions are reducing the threats.

The only solution is to be prepared to mitigate the results of the worst-case scenario, especially at the state and local levels. We should also make a special point to plan strategically and look forward to preemptively recognize threats and manage risks.

The only way we will achieve preparedness is through true cooperation of various government entities. But federal, state, and local governments do not coordinated strategically. In many cases, they have different agendas and clashing organization systems. They are not sharing enough information or intelligence, especially about potential threats. As a result, we are less prepared than we should be.

The federal government should provide a clear definition of preparedness and a strategic plan. Furthermore, states and local governments should be empowered to implement the plan.

Point 2: We should use a risk management strategy for prevention.

Risk management means reducing threats and vulnerabilities. A prevention strategy based on risk management might consist of:

1. Reducing threats: Dismantling terrorist groups and denying them weapons.
2. Reducing vulnerabilities, day-to-day: "Building the fortress" against terrorism.
3. Reducing vulnerabilities, in the event of an immediate threat: Taking steps to protect against specific attacks.

What About Prevention?

The fifth Gilmore Commission Report is an excellent source for the prevention community. It explains why the prevention cube is needed:

“Since there is no way to prevent all attacks, a risk management strategy is needed. The way to manage risks effectively is to collaborate and share information, especially about threats. This is the heart of the prevention process.”

Therefore, a true evaluation would include DHS’s role and partnership with other key national security organizations, including the Department of Defense (DOD), the Federal Bureau of Investigation (FBI), the National Intelligence establishment, and local and state law enforcement authorities.

Source: https://www.preventivestrategies.net/public/spd.cfm?spi=prevention_library_book3

Spending Taxpayer Dollars

The drumbeat of terrorism news never ends in our media society. But we must accept that we cannot be completely safe in a free and open society like America. One thing that I am most proud of is the emphasis the Gilmore Commission placed on for protecting civil liberties as our security consciousness is heightened. We must keep our security AND our liberty intact. There is nothing worth gaining that will come as a result of sacrificing our protection of basic freedoms. Right now, we are achieving much while holding true to our values; however, considerable room for improvement exists.

The current budget for the Department of Homeland Security (DHS) is $60 Billion Annually. That is up $20 billion since 2004. According to an article published in the New Yorker magazine, Lockheed Martin alone receives $30 Billion annually in defense contracts. Does that mean we aren't even close to spending enough on Homeland Security for our vast country? In my opinion, our defense spending is appropriate based on our current national strategy. Can we do better? The answer is a definite yes.

In its fifth and final report in December 2003, our commission repeated its prior emphasis that civil liberties must be a critical element in the consideration of any program to combat terrorism. The commission believed firmly in the principle that Benjamin Franklin spoke of more than 250 years ago: "They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety."

In that final report, in fact, the commission included a treatise about the importance of this issue and ways that the nation might go about achieving that result. I have included that document as an attachment to my written statement and ask that the subcommittee includes it in the record of this hearing. We believe that it is still applicable today.

Though the nation's preparedness in the event of a terrorist attack on our shores was not a primary concern of the federal government, among some government sectors (and some in the news media) there was a growing anxiety about the numerous terrorist attacks occurring all over the world in the 1990s - ie the U.S. embassy bombings in Kenya, the bombing of the USS Cole, and the reports of terrorist training camps in Afghanistan.

An example of the coverage prior to Sept. 11th is found here. The Washington Post reported on the commission on Dec. 15, 2000:

> **Panel Calls for Creating Counterterrorism Agency**
> Friday, December 15, 2000; Page A08
> By David A. Vise
> Washington Post Staff Writer
> A federal panel warned yesterday that the United States is vulnerable to terrorists wielding weapons of mass destruction, calling for the creation of a new counterterrorism agency and the loosening of restrictions on CIA agents that prevent them from recruiting confidential informants who have committed human rights abuses.

> The panel, chaired by Virginia Gov. James S. Gilmore III, urges President-elect Bush to bolster U.S. preparedness against terrorist threats within one year.
> "The United States has no coherent, functional national strategy for combating terrorism," Gilmore said. "The terrorist threat is real, and it is serious."

The commission met with Vice President Cheney at the White House in May 2001 to deliver our recommendations to him personally. One of those recommendations was to create an Office of Homeland Security (OHS) inside the White House within one year. It was created a few days after Sept. 11, 2001.

The charge to the nation's new director of homeland security, Gov. Tom Ridge (R-PA), was to develop and coordinate a comprehensive national strategy to strengthen the United States against terrorist threats or attacks. In the words of President George W. Bush, Mr. Ridge had the “strength, experience, personal commitment and authority to accomplish this critical mission.”

Following the attacks on September 11th, more congressional pressure came to bear on the issue and, against the Gilmore Commission’s recommendations, Congress promoted the OHS to a cabinet-level agency and it became the Department of Homeland Security. Although our Commission did not recommend the creation of DHS, now that it is the main organ for homeland security, we wish to be helpful and constructive to its mission.

Keep in mind, however: a recent New York Times article stated that “of the more than 160,000 homicides in the country since Sept. 11, 2001, just 14 were carried out by Al Qaeda sympathizers in the name of jihad.” Does that mean we can save more taxpayer dollars and dismantle the DHS? Of course not, but we need to understand what are we asking the DHS to do and how can the agency should carry out its mission.

Culture of Preparedness

Members of Congress will always have a bipartisan fear of being labeled soft on terrorism. Lobbyists will continue to fight for their clients and obtain lucrative domestic security contracts, but we need to have a national strategy that communicates to all Americans that we are never completely safe. Ten years later we are safer and more prepared, but are we spending the peoples’ money wisely?

America was caught off guard on Sept. 11th, but propelled by public anxiety, there were stunning advances in surveillance technology. Along with the technological increase came an influx of taxpayer dollars into homeland security — nearly $690 billion over a decade, by one estimate, not including the cost of the wars in Iraq and Afghanistan. (source NY Times)

The current debate on budget sequestration and a sense that major attacks on the United States are unlikely may embolden many Republicans and Democrats to look at our enormous counterterrorism bureaucracy and ask themselves, “is the era of the open checkbook over?”

We all know that the Obama administration is facing a decision over whether or not to scale back security spending. The most obvious solution may be to eliminate the least productive

programs. As always, budget determination must be advised by reference to a national strategy.

What we require is a more systematic, well-considered approach to security than the current DHS supplies. More important than the survival of DHS as an organization is to ensure that the majority of Americans understand that we are prone to attack by extremist organizations. This awareness will hopefully mean that when we are hit again, we don't ramp up our security culture and destroy our freedoms with "overreaction."

The experts here from the GAO, CRS, and CSIS have already outlined the way forward in handling the abuse of taxpayers dollars. Last year, when I testified on this topic I singled out a few items to consider as objectives to save taxpayer dollars. I noted that the Department of Homeland Security (DHS) isn't the only agency with duplication problems. This is a government- wide problem – but four Government Accountability Office (GAO) report items stand out:

Homeland Security Grants The Department of Homeland Security needs better project information and coordination among four overlapping grant programs (current reform is underway with grant consolidation).

Information Technology Investment Management The Office of Management and Budget, and the Departments of Defense and Energy need to address potentially duplicative information technology investments to avoid investing in unnecessary systems.

Passenger Aviation Security Fees Options for adjusting the passenger aviation security fee could further offset billions of dollars in civil aviation security costs.

Domestic Disaster Assistance The Federal Emergency Management Agency could reduce the costs to the federal government related to major disasters declared by the President by updating the principal indicator on which disaster funding decisions are based and better measuring a state's capacity to respond without federal assistance, and by a clearer policy justification for engaging federal assistance or not doing so.

No matter how much money Washington spends, it will never be enough. In 2006, I found myself in the private sector and began the process for creating a blueprint based on my experience with the commission. One major goal the commission was to include localities in the national response. Mayors need to be ready at the local level since all response is local. I recommend that we adopt a blueprint for the private sector.

National Blueprint for Secure Communities (the first 72 hours are critical)

Today, many American communities simply don't have the assets or financial resources to be fully prepared during the first 72 hours of crisis. Whether the threat comes from a natural disaster or a terrorist attack, many of our cities and towns are at risk. According to the Department of Homeland Security, America's vulnerability is a cause "for significant national concern." In addressing this concern, our communities must find ways to augment their existing public sector resources by leveraging the assets and capabilities of citizens, businesses and community organizations during the initial hours or days until help and

reinforcement arrive. The National Blueprint for Secure Communities is intended to help fill this void.

First response is always a local response. During the first 72 hours of a crisis, the quality of first response will be measured in lives saved, property preserved, and the speed of community recovery. As a society, our confidence in our ability to respond to a disaster, whether natural or man-made, will profoundly affect how we approach the challenges of preserving a free society in an age of terrorism.

The goal should be to seek community input through committees, the Internet, and the Congress. The committees must be comprised of first responders, community leaders, private sector representatives, local, state and national officials.

The subcommittees can be organized as such:

Response/Containment
Intelligence/Situational Awareness
Transportation/Logistics
Public Health/Medical
Legal/Intergovernmental
Public Safety/Information
Infrastructure/Economic
Community/Citizen

Instead of waiting for a plan - each community can prepare right now and create a 10 point plan for their city to be responsive to any disaster. From the federal point of view, states and localities will always be under pressure to reach for federal grants and appropriations to fill local budget gaps. Federal spending must be made in accordance with a national strategic plan.

History of Gilmore Commission Before & After 9/11

After the fall of the Berlin Wall, Americans and most of the civilized world looked ahead to the future with little fear – especially of global war. A transcript of a Jan. 26, 1996 Bill Clinton presidential radio address delivered on a Saturday morning following his recently delivered state of the union address sums up where he and most of Americans were focused - Domestic Policy:

“These are the seven challenges I set forth Tuesday night -- to strengthen our families, to renew our schools and expand educational opportunity, to help every American who's willing to work for it achieve economic security, to take our streets back from crime, to protect our environment, to reinvent our government so that it serves better and costs less, and to keep America the leading force for peace and freedom throughout the world. We will meet these challenges, not through big government. The era of big government is over, but we can't go back to a time when our citizens were just left to fend for themselves.” Little did we know then that by 2003 a Republican president would sign a bipartisan bill creating another government cabinet agency called the “Department of Homeland Security.”

History of the Gilmore Commission:

From 1999 to 2003, I was proud to serve as Chairman of the Congressional Advisory Panel to Assess the Capabilities for Domestic Response to Terrorism Involving Weapons Mass Destruction - the shortened name became known as The Gilmore Commission." To sum up what we did in those five years prior and after 9/11 is this: Our Commission was focused on local responders. One Gilmore Commission member, Ray Downey, served as a representative from the New York City Fire Department. Ray, unfortunately, died serving the people of his city and nation while responding and saving lives on September 11, 2001.

Congressional Mandate for the Gilmore Commission

The Advisory Panel was established by Section 1405 of the National Defense Authorization Act for Fiscal Year 1999, Public Law 105–261 (H.R. 3616, 105th Congress, 2nd Session) (October 17, 1998). That Act directed the Advisory Panel to accomplish several specific tasks.

It said: The panel shall--

1. Assess Federal agency efforts to enhance domestic preparedness for incidents involving weapons of mass destruction;

2. Assess the progress of Federal training programs for local emergency responses to incidents involving weapons of mass destruction;

3. Assess deficiencies in programs for response to incidents involving weapons of mass destruction, including a review of unfunded communications, equipment, and planning requirements, and the needs of maritime regions;

4. Recommend strategies for ensuring effective coordination with respect to Federal agency weapons of mass destruction response efforts, and for ensuring fully effective local response capabilities for weapons of mass destruction incidents; and

5. Assess the appropriate roles of State and local government in funding effective local response capabilities.

That Act required the Advisory Panel to report its findings, conclusions, and recommendations for improving Federal, State, and local domestic emergency preparedness to respond to incidents involving weapons of mass destruction to the President and the Congress three times during the course of the Advisory Panel's deliberations—on December 15 in 1999, 2000, and 2001. The Advisory Panel's tenure was extended for two years in accordance with Section 1514 of the National Defense Authorization Act for Fiscal Year 2002

(S. 1358, Public Law 107-107, 107th Congress, First Session), which was signed into law by the President on December 28, 2001. By virtue of that legislation, the panel was required to submit two additional reports—one on December 15 of 2002, and one on December 15, 2003.

Advisory Panel Composition (A Unique Membership Focused on First Responders)

Mister Chairman, please allow me to pay special tribute to the men and women who serve on our panel. This Advisory Panel is unique in one very important way. It is not the typical national "blue ribbon" panel, which in most cases historically have been composed almost exclusively of what I will refer to as "Washington Insiders"—people who have spent most of their professional careers inside the Beltway. This panel has a sprinkling of that kind of experience—a former Member of Congress and Secretary of the Army, a former State Department Ambassador-at-Large for Counterterrorism, a former senior executive from the CIA and the FBI, a former senior member of the Intelligence Community, the former head of a national academy on public health, two retired flag-rank military officers, a former senior executive in a non-governmental charitable organization, and the head of a national law enforcement foundation. But what truly makes this panel special and, therefore, causes its pronouncement to carry significantly more weight, is the contribution from the members of the panel from the rest of the country:

- Three directors of state emergency management agencies, from California, Iowa, and Indiana, two of whom now also serve their Governor's as Homeland Security Advisors

- The deputy director of a state homeland security agency

- A state epidemiologist and director of a state public health agency

- A former city manager of a mid-size city

- The chief of police of a suburban city in a major metropolitan area

- Senior professional and volunteer fire fighters

- A senior emergency medical services officer of a major metropolitan area

- And, of course—in the person of your witness—a former State governor

These are representatives of the true "first responders"—those heroic men

and women who put their lives on the line every day for the public health and safety of all Americans. Moreover, so many of these panel members are also national leaders in their professions: our EMS member is a past president of the national association of emergency medical technicians; one of our emergency managers is the past president of her national association; our law officer now is president of the international association of chiefs of police; our epidemiologist is past president of her professional organization; one of our local firefighters is chair of the terrorism committee of the international association of fire chiefs; the other is chair of the prestigious national

Interagency Board for Equipment Standardization and InterOperability.

Those attacks continue to carry much poignancy for us, because of the direct loss to the panel. Ray Downey, Department Deputy Chief and chief-incharge of Special Operations Command, Fire Department of the City of New York, perished in the collapse of the second tower in the September 11 attack on the New York World Trade Center.

Panel Reports

In the history of the Panel, we produced five advisory reports to the Congress and to the President of the United State. The first report in 1999 assessed threat. The second report in 2000 developed the fundamentals of a national strategy for combating terrorism.

The third report, dedicated to Ray Downey who lost his life in the World Trade Center, filled out a national strategy in five key subject areas: state and local response capabilities, health and medical capabilities, immigration and border control, cybersecurity, and use of the military. Our fourth report in 2002, issued in the year following the 9-11 attacks, further made recommendations on how to marshal the national effort towards a national strategy. It paid special attention to the needs of intelligence sharing and the proper structure for counterterrorism activities inside the United States. Our last report was issued on December 15, 2003. That finalreport sought to express some end-vision and direction for the United Statesas it develops its national strategy and makes the country safer.

Fifth Report (2003) – Forging America's New Normalcy: Securing our Homeland, Preserving Our Liberty

Mister Chairman, the Advisory Panel released its fifth and final report on December 15, 2003. In that report, the strategic vision, themes, and recommendations were motivated by the unanimous view of the panel that its final report should attempt to define a future state of security against terrorism—one that the panel has chosen to call "America's New Normalcy."

That strategic vision offered by the panel reflects the guiding principles that the panel has consistently enumerated throughout its reports:

- It must be truly national in scope, not just Federal.

- It should build on the existing emergency response system within an all-hazards framework.

- It should be fully resourced with priorities based on risk.

- It should be based on measurable performance.

- It should be truly comprehensive, encompassing the full spectrum of awareness, prevention, preparedness, response, and recovery against domestic and international threats against our physical, economic and societal well-being.

- It should include psychological preparedness.

- It should be institutionalized and sustained.

- It should be responsive to requirements from and fully coordinated

with State and local officials and the private sector as partners throughout the development, implementation, and sustainment process.

- It should include a clear process for strategic communications and community involvement.

- It must preserve civil liberties.

In developing the report, panel members all agreed at the outset that it could not postulate, as part of its vision, a return to a pre-September 11 "normal." The threats from terrorism are now recognized to be a condition must face far into the future. It was the panel's firm intention to articulate a vision of the future that subjects terrorism to a logical place in the array of threats from other sources that the American people face every day—from natural diseases and other illnesses to crime and traffic and other accidents, to mention a few. The panel firmly believes that terrorism must be put in the context of the other risks we face, and that resources should be prioritized and allocated to that variety of risks in logical fashion.

In 2004 our panel proffered a view of the future—five years hence—that it believes offers a reasonable, measurable, and attainable benchmark. It believes that, in the current absence of longer-term measurable goals, this benchmark can provide government at all levels, the private sector, and our citizens a set of objectives for readiness and preparedness. The panel did not claim that the objectives presented in this future view are all encompassing. Neither do they necessarily reflect the full continuum of advances that America may accomplish or the successes that its enemies may realize in the next five years. The view is a snapshot in time for the

purpose of guiding the actions of today and a roadmap for the future.

The panel said that America's new normalcy by January of 2009 should reflect:

- Both the sustainment and further empowerment of individual freedoms in the context of measurable advances that secure the homeland.

- Consistent commitment of resources that improve the ability of all levels of government, the private sector, and our citizens to prevent terrorist attacks and, if warranted, to respond and recover effectively to the full range of threats faced by the nation.

- A standardized and effective process for sharing information and intelligence among all stakeholders—one built on moving actionable information to the broadest possible audience rapidly, and allowing for heightened security with minimal undesirable economic and societal consequences.

- Strong preparedness and readiness across State and local government and the private sector with corresponding processes that provide an enterprise-wide national capacity to plan, equip, train, and exercise against measurable standards.

- Clear definition about the roles, responsibilities, and acceptable uses of the military domestically—that strengthens the role of the National Guard and Federal Reserve Components for any domestic mission and ensures that America's leaders will never be confronted with competing choices of using the military to respond to a domestic emergency versus the need to project our strength globally to defeat those who would seek to do us harm.

- Clear processes for engaging academia, business, all levels of government, and others in rapidly developing and implementing research, development, and standards across technology, public policy, and other areas needed to secure the homeland—a process that focuses efforts on real versus perceived needs.
Well-understood and shared process, plans, and incentives for protecting the nation's critical infrastructures of government and in the private sector—a unified approach to managing our risks.

The panel's Future Vision back in 2009 included specifics details involving:

- State, Local, and Private Sector Empowerment

- Intelligence

• Information Sharing

• Training, Exercising, Equipping, and Related Standards

• Enhanced Critical Infrastructure Protection

• Research and Development, and Related Standards

• Role of the Military

The GAO and DHS have prepared lengthy reports to enhance homeland security of our nation and the Congress is doing its due diligence. Hearings like we are having today move forward the idea of making progress happen, but we must always consider the role of the military as we decide on our future homeland policy.

In Conclusion

Civil Liberties are the foundation of the Gilmore Commission. The panel addressed the on-going debate in the United States about the tradeoffs between security and civil liberties. It concluded that history teaches, however, that the debate about finding the right "balance" between security and civil liberties is misleading, that the traditional debate implies that security and liberty are competing values and are mutually exclusive. It assumes that our liberties make us vulnerable and if we will give up some of these liberties, at least temporarily, we will be more secure.

It concluded that civil liberties and security are mutually reinforcing. The panel said that we must, therefore, evaluate each initiative along with the combined effect of all initiatives to combat terrorism in terms of how well they preserve all of the "unalienable rights" that the founders believed were essential to the strength and security of our nation—rights that have become so imbedded in our society and ingrained in our psyche that we must take special precautions, take extra steps, to ensure that we do not cross the line.

To be included for the record:
APPENDIX E—CIVIL LIBERTIES IN A POST-9/11 WORLD*

The attacks of September 11, 2001, led to new laws, policies, and practices designed to enhance the nation's security against the terrorist threat. These security measures have prompted a debate about their impact on civil liberties. For its final report, the Advisory Panel seeks to contribute to the development of a long-term, sustainable approach to security that protects not just lives but also our way of life.

The panel could advance this objective by reframing the terms of the civil liberties debate and emphasizing the importance of understanding the implications of the fundamentally altered environment in which individual counterterrorism initiatives need to be evaluated. Rather than the traditional portrayal of security and civil liberties as competing values that must be weighed on opposite ends of a balance, these values should be recognized as mutually reinforcing. Under this framework, counterterrorism initiatives would be evaluated in terms of how well they preserve all of the unalienable rights that the founders believed

were essential to the strength and security of our nation: life, liberty, and the pursuit of happiness.

Moreover, an effective evaluation should focus not just on individual initiatives but on the way these initiatives fit into a fundamentally changed approach to counterterrorism overall. For example, we have moved from a largely law enforcement approach in combating terrorism to a global war in which the continental United States is part of the battlefield. It is important to analyze the impact this may have on public reaction, judicial interpretation, and the applicable legal framework. Similarly, the FBI now has a broader mission that often eliminates the traditional requirement for a criminal predicate to justify intrusive investigative techniques. "Law enforcement" means something different than it did on September 10, 2001. These new paradigms must inform the evaluation of existing and proposed laws and policies.

Reframing the Debate

In times of crisis, when the pressure for dramatic change is most intense, it is helpful to return to the fundamental principles that have guided this nation since its inception. As Thomas Jefferson advised in his first Inaugural Address, "[The essential principles of our Government] form the bright constellation which has gone before us and guided our steps through an age of revolution and reformation. . . . [S]hould we wander from them in moments of error or of alarm, let us hasten to retrace our steps and to regain the road which alone leads to peace, liberty and safety."

The Declaration of Independence rests on the premise that there are certain "unalienable rights," including "Life, Liberty and the Pursuit of Happiness." Terrorists seek to destroy all three. A successful strategy to defeat the terrorists' objective, then, should seek to preserve not just life, but also liberty and our way of life.

Moreover, history teaches that the debate about finding the right "balance" between security and civil liberties is misleading. This traditional debate implies that security and liberty are competing values and are mutually exclusive. It assumes that our liberties make us vulnerable and if we will give up some of these liberties, at least temporarily, we will be more secure. Yet, consider the context in which civil liberties were first firmly established. The framers of the Constitution had just survived a true threat to their existence and were acutely aware of the fragility of their nascent nation. In this uncertain and insecure environment, the framers chose not to consolidate power and restrict freedoms but to devolve

---

* Suzanne Spaulding, J.D.

power to the people and protect civil liberties from encroachment. They recognized that civil liberties and security are mutually reinforcing. Security clearly ensures the freedom to exercise our liberties, but it is also true that the exercise of civil liberties and our way of life contributes to our strength and security.

For example, no one individual or handful of people possesses the knowledge, wisdom, and skills to defeat the threat of terrorism. The solutions can only be derived through collective wisdom and innovation emerging from the marketplace of ideas that flourishes in a free society. The frequent admonition to “think outside the box” reflects the recognition that iconoclastic, nonconformist input maximizes the prospects for finding solutions. To meet today’s threats, we need technological breakthroughs, such as the development of sensors to detect deadly chemicals or biological agents, and new ideas, such as ways of educating and assisting citizens to effectively protect themselves in the event of a terror attack. These developments are far less likely to emerge where "group think" dominates.

Yet many of the security measures added or expanded after September 11 involve efforts to detect terrorists by looking for “outliers.” Government officials at all levels, as well as the American public, have been instructed to watch for activity that is different or outside the norm. Combine this with the prospect of increased government surveillance over an ever-widening range of activities and individuals, and the pressure to conform grows.

Protection of civil liberties and our way of life also promotes the kind of relationship between the government and the governed that keeps the nation strong and secure. The framers understood that the strongest nation would be one in which the people viewed their government as “us” and not “them.” The brave men and women who struggled on September 11 to keep their plane from being used to decapitate the government confirmed that the most effective antidote to threats inside our borders is an informed citizenry committed to preserving a nation in which they have a very real stake. Yet security restrictions can begin to drive a wedge between government and the people. Before the attacks of September 11, between 10,000 and 20,000 visitors roamed the halls of the U.S. Capitol on busy days. Now, visitors are only allowed if they are on a tour, and the number is down to about 1,000. Similar limitations on access characterize Federal offices all across the country. A government that shuts off the halls of power inside jersey barriers and cloisters its public servants behind armed guards runs the risk of detaching itself from the governed.

Local police have learned how essential it is to become a more integral part of their communities.[1] Moreover, citizen support is strengthened by a sense that the system is just and fair. If that conviction begins to erode, so might vital citizen support. Thus, some police departments have expressed concern about some of the activities that Federal officials have asked them to undertake in their local communities, particularly with regard to enforcement of immigration laws. The concern is greatest with respect to the Arab-American community, where support for government efforts could yield significant benefits but relations are often severely strained by policies perceived to be discriminatory.

Similarly, one of the greatest risks of the current plans for responding to bioterrorism, which are based primarily on compulsory measures, such as quarantine or mandatory vaccinations, is that they may create an adversarial relationship between the government and the public. One of the most compelling advantages of adding the option of a measure such as “Shielding,” or “stay at home,” is that it undermines the terrorist objective by building on the strengths of democracy. Our system of government reflects the framers’ faith in the wisdom of an informed citizenry to make decisions about what is best for themselves, their families, their communities, and their nation. Shielding reflects that same

belief and takes advantage

of the strengths of a democracy, empowering ordinary citizens through education and community-based decisionmaking.

The rights described in the Declaration of Independence and enshrined in the Constitution were not viewed as a luxury of peace and stability but as the best hope for a people embarking on the dangerous and daring endeavor of creating a new nation. They are no less essential to the nation's security today. Thus, proposed security measures should be evaluated on how well they frustrate the terrorists' targeting not just of life, but also liberty and the pursuit of happiness. The impact on these latter rights may be clear and direct, such as denial of due process, or subtler, such as chilling First Amendment activity, creating pressure to conform, or otherwise deterring lawful activity. These more subtle effects are largely a result of the sense that government is casting a broad net that is more likely to "catch" nonterrorists—i.e., us.

Many of the security initiatives implemented since September 11 have been challenged as possible violations of the Fourth Amendment prohibition against unreasonable search or seizure. Some of these challenges are currently pending in Federal courts. However, this paper focuses on the more subtle and potentially profound impact on the exercise of First Amendment rights and, more broadly, on the ability to pursue our way of life.

Evaluating an initiative's impact on "the Pursuit of Happiness" can also yield a more accurate assessment of its cost. Overly burdensome financial reporting requirements, for example, may not infringe on core civil liberties, but they do raise transactional costs and will inhibit beneficial activity along with criminal activity. Similarly, the opportunity to fly may be viewed as a privilege rather than a right, but overly stringent and apparently arbitrary security hurdles can not only have an economic impact but also increase public skepticism about security measures generally.

A clearer assessment of the full costs of security measures should provide insights into more effective ways of achieving the desired impact on terrorist activity while minimizing the impact on our way of life. Narrowing the scope of new legal authorities, providing procedural or technological safeguards against abuse, or simply doing a better job of educating the public on implementation might significantly reduce the potential harm from new measures without significantly reducing their effectiveness against terrorism.

Possible Recommendation:

Efforts to combat terrorism should be evaluated in terms of how well they frustrate the terrorists' objective of destroying life, liberty, and the pursuit of happiness.

Understanding the Broader Context

The civil liberties debate often focuses on specific laws, policies, or practices. However, as this analysis attempts to illustrate, these initiatives are implemented in the context of fundamental changes in our counterterrorism approach, which can have a significant

consequences for their overall effectiveness and erode the protection of life, liberty, and the pursuit of happiness. This presents a significant challenge for evaluating civil liberties in the post-9/11 world.

The War on Terrorism

One of the most immediate and dramatic changes brought about on the morning of September 11, 2001, was the shift from viewing terrorist attacks as first and foremost a crime to viewing them as belligerent operations in an ongoing war. Americans are only now beginning to sort through the full implications of this shift. It was fairly straightforward as manifest in the combat operations in Afghanistan. However, the end of that conflict did not signal the end of the global war on terrorism. Thus, all actions taken to protect Americans from terrorist attack occur in the context of this war—a war in which the enemy cannot be distinguished by uniforms, nationality, or location, with no defined battlefield, and with no discernable end point. This war has an impact on how courts and the Congress view the actions of the Executive Branch, on which laws apply, and on how those laws are applied.

As Supreme Court Chief Justice William Rehnquist noted in his book on civil liberties in wartime, *All the Laws but One*, it is often said that law is silent during war (*Inter arma silent leges*). In part, this is because, as a matter of law, the government's authority to restrict civil liberty is greater during war than in peacetime. But Rehnquist also observes that "[q]uite apart from the added authority that the law itself may give the President in time of war, presidents may act in ways that push their legal authority to its outer limits, if not beyond." In addition, courts are reluctant to decide a case against the government on an issue of national security during a war. Rehnquist ultimately rejects the traditional maxim, concluding that the laws will not be entirely silent in time of war, but he does conclude that "they will speak with a somewhat different voice."

It becomes important, then, to understand the impact that this "somewhat different voice" may have on the legal framework for counterterrorism

Homeland Defense—Distinguishing Between Law Enforcement and Military Operations

The attacks of September 11 brought home the reality that the continental United States is part of the battlefield in this unconventional war. As those who live along the Potomac River just outside the nation's capital can attest, the U.S. military patrols this battlefield regularly in an effort to detect and deter enemy combatants. As further testament to the importance of the domestic mission of the military, the Department of Defense established a new command, the Northern Command, whose responsibilities include homeland defense and support to civil authorities. Yet, these new domestic missions for the military have received relatively little public discussion and debate.

One consequence of the homeland defense mission is its potential impact on the application of Posse Comitatus. Questions have been raised as to whether the Posse Comitatus Act[2] provided DoD with sufficient flexibility to perform its domestic missions. What has been missed in much of that discussion, however, is that Posse Comitatus only applies when soldiers are asked to perform law enforcement functions. It does not apply to military operations. In today's environment, activities or situations that look very much like

law enforcement may turn out to be military operations or activities.[3]

Thus, if terrorists were known to be hiding inside a warehouse and the military arrived on the scene, it might not be clear whether any action they took was part of a military operation against enemy combatants or a law enforcement activity against suspected criminals. The application of Posse Comitatus would be uncertain. Yet, some of the concerns that prompted the Posse Comitatus Act might also apply to the domestic use of the military in a combat operation.

Guidance on the use of force by the military is usually provided by "rules of engagement" (ROEs). Yet there are reportedly no clearly articulated rules of engagement or "use of force" rules to govern the military's actions inside the United States in such a situation as that described above. It is hard to imagine how troops could have been adequately trained to respond appropriately to such a contingency without the development of such guidelines.

Possible Recommendations:

The potential for serious infringement of liberties stemming from the domestic deployment of troops could be significantly reduced by the development of ROEs for the continental United States, rigorous training, and publicly articulated standards and procedures for determining when the military is conducting a military operation in its homeland defense role and when it is conducting law enforcement activities. These issues need to be fully discussed in the public arena so that the American people understand and are prepared for the military's intervention, should that become necessary.

DOD Intelligence Collection

Another consequence of the homeland defense mission is the enhanced collection of intelligence by the military inside the United States. Just as the military undertook intensive intelligence collection in Afghanistan prior to and during the war in order to support its combat operations, the military is collecting intelligence on the battlefield here in the United States. Thus, the Defense Advanced Research Projects Agency (DARPA) has funded research into advanced data mining technology that would gather information from U.S. companies, though not about U.S. persons. In addition, the *New York Times* reported that DoD, along with the CIA, was seeking authority similar to that currently exercised by the FBI to compel U.S. businesses to provide records on targeted individuals.[4] The National Imagery and Mapping Agency, which is responsible for analyzing images from satellites, has significantly increased its interest in targets inside the United States.

Yet, our system of laws and safeguards did not anticipate the homeland defense mission. For example, domestic intelligence collection by DoD has generally been viewed as a law enforcement activity governed by Posse Comitatus and related policies. However, as discussed above, today domestic intelligence collection is presumably being undertaken for military purposes, something the current legal framework did not contemplate.

It is not entirely clear how the courts will view intrusive intelligence collection, such as satellite imagery, undertaken inside the United States for military purposes during a time of war. As we have seen in the cases involving electronic surveillance, the courts have

allowed some distinction between purely domestic situations and those involving a foreign power or an agent of a foreign power. In that situation, however, Congress chose to step in and articulate clear procedures to govern electronic surveillance for intelligence purposes inside the United States, enacting the Foreign Intelligence Surveillance Act in 1978.[5] This new context may warrant similar clarification.

Even with respect to actions overseas, the global war on terrorism may render certain laws inapplicable. For example, the Congress and the Executive Branch developed an extensive system of safeguards with respect to covert actions. However, the relevant statute notes that the requirements to do not apply to "traditional military activities."[6] Thus, not only are actions that might look like law enforcement susceptible to being labeled military operations, activities that might otherwise be considered covert actions are also likely to be viewed as military operations if undertaken by DoD. To the extent that this complicates oversight by Congress and the Executive Branch, it may also frustrate efforts to fully understand the civil liberties implications of the war on terrorism.

Possible Recommendations:

Congress should consider working with the Administration to develop, in statute and/or Executive Order, new guidelines and procedures for domestic intelligence collection by the military. Definitions may need to be revisited or additional safeguards added in order to address the challenges of this unconventional war.

Enemy Combatants

The war on terrorism brings with it the legal framework of the law of armed conflict. Yet this body of law was developed to govern the actions of nation states. Attempts to apply it to nonstate actors in nontraditional global conflict present unique challenges. This is most clearly evidenced in the legal issues surrounding the detention of suspected terrorists as "enemy combatants."

The courts are currently considering *habeas corpus* cases involving the detention as enemy combatants of two American citizens, Yasser Esam Hamdi and Jose Padilla. Hamdi was taken into custody in Afghanistan during the armed conflict there, while Jose Padilla was initially taken into custody by law enforcement officers in O'Hare Airport and detained under the material witness statute. A few days before a hearing on the legality of his detention, Padilla was removed from the criminal justice system, designated as an enemy combatant, and transferred to military custody.

The U.S. Court of Appeals for the Fourth Circuit, in Richmond, Virginia, has held in the Hamdi case that the President has the authority to designate U.S. citizens as enemy combatants and detain them without access to a lawyer. However, the court has noted that Hamdi was apprehended in a "zone of active combat" and "during a military campaign on foreign soil." Thus, it is not clear that the court would reach the same conclusion in the case of someone captured inside the United States, such as Jose Padilla.

U.S. District Judge Michael B. Mukasey in New York is hearing Padilla's case. While he has agreed with the 4th Circuit that the President has the authority to detain a U.S. citizen

as an enemy combatant, he has ruled that Padilla "must have the opportunity to present evidence that undermines the reliability of the [government's] declaration." Unlike the 4th Circuit, Judge Mukasey ruled that "the only practical way" to give Padilla that opportunity was for Padilla to have access to his attorneys. The government argues that access to attorneys will defeat efforts to gather intelligence from these detainees that could prevent another terrorist attack. The government is appealing this decision and oral arguments were expected in the fall. To date, Padilla has been held in solitary confinement for more than a year with no access to his attorneys. Under international law, prisoners of war can be detained for the duration of the conflict. No one has yet speculated on when the war on terrorism might end.

These cases have raised concerns about the potentially indefinite detention of Americans with no formal charges and no right to challenge the basis for their designation as enemy combatants. When individuals are detained outside a zone of combat, the risk of error is significantly heightened. Moreover, some concern has arisen that the threat to remove a criminal defendant from the civilian court into the indefinite status of an enemy combatant may introduce a level of coercion into our criminal justice system that threatens its fairness.

The government is pursuing policies that seek to preserve maximum flexibility to meet the unique and potentially unforeseeable challenges inherent in this new approach to terrorism as an ongoing war. Thus, it is reluctant to articulate hard and fast rules or make categorical statements that might wind up limiting options in the future. Yet, in addition to the direct impact on those detained, this approach risks undermining public support over time by raising concerns of arbitrariness. Moreover, the uncertainty about the scope of this approach can have a chilling effect, just as with vague or overbroad criminal statutes.

Possible recommendations:

If the current enemy combatant policy is evaluated in terms of how well it protects life, liberty, and the pursuit of happiness, some changes might be recommended. Such recommendations might include establishing guidelines that define, at least in general terms, the circumstances under which an individual might be designated as an enemy combatant and the length of time an individual so designated could be held incommunicado for purposes of intelligence interrogation, as well as providing access to an attorney at the end of that period of time for those detainees taken into custody somewhere other than in a zone of active combat or foreign military campaign. Clearer guidance on the circumstances that might lead to eventual release or the filing of criminal charges against detainees would also reduce the sense that the designation is a legal "black hole."

Similar clarifications on the policies regarding non-U.S. citizens detained in Guantanamo Bay, Cuba, might also serve to sustain national and international support over the long haul.

More broadly, given the significant implications of the legal status that this war, unlike the war on drugs, appears to have, it may be appropriate for the Administration, Congress, and the courts to consider distinguishing between the war against al Qaeda and its affiliates and broader counterterrorism efforts aimed at the phenomenon of terrorism generally or at other terrorist groups or individuals. Legal justification for this distinction, and for drawing some lines around the scope of the "enemy" could be found in the Congressional authorization for

the use of force after September 11, which has been cited by the Executive Branch as part of the legal basis for such actions as the detention of enemy combatants.

The resolution authorized the President to "to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons." It is not clear that the "global war on terrorism" is limited to those covered by this authorization. While efforts to combat terrorism may well need to be broader than just those responsible for September 11 and their helpers, and include those who have never targeted the United States or Americans, it may be worth considering whether all of those efforts should have the legal status of a traditional war.

The Changing Role of Law Enforcement

Another significant change in the overall environment in which security initiatives should be evaluated is in the roles and mission of the FBI and local law enforcement. Where the Bureau's mission had been to investigate criminal activity with the objective of bringing a successful prosecution, the primary mission today is to prevent a terrorist attack. Criminal prosecution is simply one possible avenue for achieving this objective. Intelligence collection and disruption, neither of which requires any criminal predicate, are now equally important roles for FBI agents. The move away from the traditional requirement for a criminal predicate to justify law enforcement activity has potentially far reaching implications. Not only has this change prompted some concomitant changes laws and policies it also affects the application of laws already on the books. The full impact of these changes on the nation's ability to protect life, liberty, and our way of life may not be known for years.

A fundamental principle of our democracy is that law-abiding citizens should be able to go about their lives without fear of government detention or interference. Law enforcement authority was, by definition, to be used to enforce the laws. Interference by law enforcement was to be limited to those situations involving a violation of the law, usually criminal laws. Thus, we require crimes to be clearly defined so that people can know when they are violating the law. Law enforcement may mistakenly target an innocent person, but such mistakes should be rare and the system should operate to detect those mistakes as promptly as possible.

When law enforcement officials start looking for "suspicious" activity rather than criminal activity, this clarity is lost. People are left to speculate about whether their activity might be viewed as suspicious. While it may still be unlikely that a law-abiding citizen will be convicted of terrorism, they may well come under heightened scrutiny. This can have several consequences. The mere prospect that the government may be watching is sufficient to deter some people from engaging in otherwise lawful activity, including such protected activity as exercise of religion or free speech. Moreover, enhanced surveillance raises the prospect that the government will detect nonterrorism violations, such as failure to pay child support or problems with income taxes. Just as Al Capone was locked up for tax fraud, Attorney General John Ashcroft has said the government will go after suspected

terrorists for “spitting on the sidewalk.” Thus, violations that might not otherwise be detected or rise to a level warranting prosecution may result in liability because “suspicious” activity led to heightened scrutiny. While few would object to using whatever laws are applicable to lock up terrorists, this approach also places nonterrorists at greater risk of prosecution if they engage in behavior the government has labeled as “suspicious.” Aside from its chilling effect, this can eventually impugn the perceived credibility and fairness of the system, undermining vital citizen support.

Law-abiding individuals may also be at greater risk of other kinds of government interference, short of criminal prosecution because of the FBI’s increasing reliance on “disruption” techniques. The intelligence community has traditionally used disruption overseas when there is information indicating a possible attack but either inadequate information or insufficient capability to move directly against the terrorists. In those situation, intelligence officials, usually working with cooperative foreign governments, will generate activity designed primarily to intimidate the terrorists into delaying or canceling the attack. “Rounding up the usual suspects”—detaining members of the communities of which the terrorists are thought to be a part—is a classic form of disruption. Authorities may get lucky and actually take into custody someone who is necessary for the attack but, at a minimum, they put the terrorists on notice that the government knows something is up. The Attorney General and FBI Director have made it clear that disruption is now part of the strategy inside the United States, raising issues not present in the overseas context. To some extent, at least, the large-scale detentions and questioning of immigrants after September 11 was part of a disruption campaign. Other kinds of government disruption that fall short of criminal prosecution might include IRS audits, denying permission to board an airplane, or extensive questioning or searches each time you try to board a plane. These activities do not require any criminal predicate for justification and often are not governed by the safeguards the system usually imposes to prevent abuses of government authority. Typically, the targeted individuals have little recourse to challenge the basis for the government action, unlike the protections built into the criminal justice system.

Concern about being caught up in antiterrorism actions because you have engaged in “suspicious,” rather than criminal, activity is heightened by technology designed to enhance the government’s surveillance capability. Broad search capabilities designed to find terrorists based on a “profile” raise the greatest concern. These might include some proposals for data mining, as well as such physical surveillance technologies as facial recognition and gait analysis. Underlying this heightened concern is skepticism about the government’s ability to create a profile accurate enough to detect all terrorist activity and only terrorist activity. Instead, many fear that the profile will miss some terrorists and “catch” too many nonterrorists. Similar concerns underlie the controversy over technologies that would access databases of questionable accuracy in such programs as CAPPS II. These concerns might be alleviated, then, if the public were assured of the accuracy and effectiveness of the data and the profile and if the “cost” to nonterrorists of being mistakenly profiled were relatively low. A more accurate system for “profiling” terrorists, if one could be developed, might actually enhance civil liberties and reduce the fear of unwarranted government interference by reducing the likelihood that law-abiding individuals would be targeted.

Proposals for a national ID card also raise the prospect of heightened government

surveillance. The idea of a card that can be a more reliable form of identification through the use of biometrics, for example, would address a number of security concerns. However, in order for the biometrics to be an identifier, presumably the government must have some way of matching the data. For example, if the biometric identifier were fingerprints or DNA, the government would need to have everyone's fingerprints or DNA on file in order to match the card with the name. This is personal information the government currently does not have for most Americans. Moreover, as more and more businesses, employers, locations, and others begin to require these ID cards, they will form records of our every action. These records will be susceptible to government access.

Many of the challenges to various surveillance and search techniques are based on the Fourth Amendment prohibition of unreasonable searches and seizures. However, evaluations of these techniques should also include consideration of their potential chilling effect on protected activity. In counterterrorism efforts, particularly, Fourth Amendment and First Amendment rights are often closely connected. As Supreme Court Justice Lewis Powell noted in a decision on electronic surveillance, "[n]ational security cases…often reflect a convergence of First and Fourth Amendment values not present in cases of 'ordinary' crime. Thought the investigative duty of the executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech."[7] This is particularly pronounced in investigations targeting politically or religiously motivated terrorism.

Possible Recommendations:

Efforts to detect possible terrorists living in our midst could more effectively preserve life, liberty, and the ability to pursue happiness if safeguards could be developed to maximize the fairness and effectiveness of the methods utilized.

For example, concerns about government surveillance and use of profiling might be alleviated by the development of technologies and methodologies to maximize the effectiveness of terrorist "profiles" and strengthen the accuracy of data. Privacy concerns could be eased by ensuring that data remains "anonymous"—allowing computers to do "blind" matches so that no person has access to the names—until a court, magistrate, or other independent authority determines that the investigator has met an appropriate threshold for allowing names to be matched with data.

The costs of a "false positive" should also be reduced, perhaps by establishing mechanisms that would allow individuals to get off watch lists, developing more timely mechanisms for verifying information leading to a "hit," and placing limits on the type of action that can be taken on the basis of such a hit.
Accountability could be enhanced by using technology to build in rigorous audit controls to detect unauthorized activity, such as improper storage of information on protected activity, or inappropriate searches of databases or uses of surveillance technology.[8]

Law Enforcement and Intelligence

As FBI and local law enforcement focus on prevention, it becomes harder to distinguish

between law enforcement and intelligence. According to the revised Attorney General Guidelines issued in May 2002, law enforcement activity includes activities related to counterterrorism and foreign intelligence. (*AG Guidelines on General Crimes, Racketeering Enterprise, and Terrorism Enterprise Investigations*, Section VI(C).) FBI activity is defined as "law enforcement activity" even if it involves actions designed to collect intelligence rather than to investigate criminal activity.

Traditionally, as FBI Director Robert Mueller has told the Advisory Panel, criminal investigators brought a certain discipline to the collection and analysis of information because that information might eventually be evidence in a criminal prosecution. Law enforcement officers at the local, State, and Federal level knew that if information was not collected in a manner consistent with the Fourth Amendment, for example, it could not be used at trial. This served as a safeguard against the potential abuse of law enforcement powers. However, since prosecution is no longer the primary objective, this safeguard may no longer be effective. Indeed, it has been reported that many of those detained after September 11 were not read their *Miranda* rights or given access to counsel because the objective of the detention was to collect intelligence information rather than to use that information in a prosecution. Most were detained under the material witness statute and, while this is probably not unconstitutional,[9] it is a different way of doing business for the FBI and it may be appropriate for Congress to consider whether new safeguards are needed.

Other investigative techniques have also been broadened to apply even when there is no indication of criminal activity. For example, online searches for information about individuals or groups prior to September 11 could not be conducted in the absence of some showing of possible criminal activity. Law enforcement actions that touched on First Amendment activity, particularly the exercise of religion, were subject to particular scrutiny. Many agents in the field interpreted this policy as a virtual ban on such actions and important opportunities to detect terrorist recruitment efforts, for example, may have been lost.

The revised AG Guidelines authorize FBI agents to visit any place and attend any event that is open to the public and conduct online search activity or access online sites and forums, on the same terms and conditions as members of the public generally, for the purpose of detecting or preventing terrorist activities. Section 411 broadly defines "terrorist activities" and again makes it clear that criminal activity is not required.

The most significant concern with allowing the monitoring of such First Amendment activities as exercise of religion and freedom of speech is that it will have a chilling effect. This concern is exacerbated if those doing the monitoring are allowed to keep files on individuals they observe.

The AG guidelines attempt to address this concern by stating that:

The law enforcement activities authorized by this Part do not include maintaining files on individuals solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of any other rights secured by the Constitution or laws of the United States. Rather, all such law enforcement activities must have a valid law enforcement purpose as described in this part.

This apparent safeguard is not as strong as it might at first appear. First, files could be maintained if they were for another purpose *in addition to* monitoring constitutionally protected activity. Moreover, the activities permitted must have a valid law enforcement purpose but, as discussed above, that term is now very broadly defined.

Possible Recommendation:

The potential chilling effect of broadened surveillance authority could also be reduced if, in addition to barring the collection or storage of information *solely* for monitoring protected activity, a more rigorous standard was imposed for any targeting that involved protected activity. The key would be to ensure that the higher threshold was not interpreted in the field as effectively a prohibition against such collection or storage, as happened in the past.[10]

Changes in FISA

The blurred distinction between law enforcement and intelligence has been most clearly evidenced in the application of the Foreign Intelligence Surveillance Act (FISA). Pursuant to FISA, the FBI can apply for orders from the Foreign Intelligence Surveillance Court (FISC) authorizing electronic surveillance or physical searches where there is *probable cause* to believe that the target is a foreign power or an agent of a foreign power, as opposed to the traditional Title III wiretap authority used in criminal cases, which requires probable cause to believe the target is involved in criminal activity. Unlike surveillance or searches authorized under the criminal code, FISA activities can be undertaken without ever notifying the target.

The definition of a foreign power includes "a group engaged in international terrorism or in preparation therefore." "Agent of a foreign power" includes a non-U.S. person who is a member of an international terrorism group or any person, including a U.S. person, who knowingly engages in sabotage or international terrorism, or activities in preparation therefore, for or on behalf of a foreign power; or knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or knowingly aids and abets persons engaged in such activities.

Long interpreted by some elements of the intelligence community as applying only where the "primary purpose" of the surveillance was foreign intelligence rather than law enforcement, the statute was amended as part of the USA PATRIOT Act to allow its use when foreign intelligence was merely a "significant purpose." Subsequently, the Foreign Intelligence Court of Review concluded that there was never any constitutional requirement for distinguishing between a law enforcement and foreign intelligence purpose where the two overlap, as they do with regard to international terrorism. The court tore down the wall that had been erected over a period of 25 years between these two communities.

One immediate impact of this is to allow criminal investigators to receive information collected pursuant to FISA. However, it also allows those investigators to assist in identifying targets. For all practical purposes, FISA has now replaced the traditional

criminal wiretap authority for all international terrorism investigations. Again, one significant impact of this change is to effectively remove the requirement for a criminal predicate for electronic surveillance of international terrorism suspects.

In addition, the potential scope of the FISA authority may have been significantly expanded by other changes in the law. The statute prohibiting material support to terrorists, for example, was also broadened in the USA PATRIOT Act and is now being challenged in court as unconstitutionally vague and overbroad. If "material support" as broadly defined in that statute informs the FISA threshold that allows targeting of individuals who "knowingly aid and abet" individuals engaged in international terrorism, the scope of potential FISA targets has grown correspondingly. If constitutional challenges to the material support statute are upheld, they may call into question the legitimacy of the related FISA collection.

Possible Recommendation:

Congress should carefully monitor the application of FISA, as amended, particularly in light of the decision of the Foreign Intelligence Court of Review and changes in other laws, to ensure that the powers authorized still meet constitutional requirements and do not chill legitimate activity.

Section 215—Library Records

Another change to FISA contained in the USA PATRIOT Act that has been of particular concern to civil liberties advocates is the expanded authority to compel libraries, bookstores, schools, Internet service providers, retailers, and others to turn over information to the government. Section 215 of the PATRIOT Act amended FISA to give the FBI the authority to seek an order from a FISA judge or magistrate requiring anyone served with such an order to turn over "any tangible things (including books, records papers, documents, and other items)." Prior to this amendment, this authority was limited to business records held by common carriers, hotels, storage facilities, or car rental companies. The provision as amended is not limited to businesses or business records but would apparently apply to tangible things held by any individual or entity. Its potential application to libraries and bookstores is what has prompted the greatest concern.

The amendment makes several other changes to the provision. The original provision required that the information was being sought pursuant to an FBI investigation and that there were "specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power." Neither of these requirements was carried over to the amended version. Applications seeking information on non-U.S. persons need only be "to obtain foreign intelligence information."

However, if the information sought involves a U.S. person, the amended provision can only be used if its purpose is to protect against international terrorism or clandestine intelligence activities (espionage) and only if it is not conducted *solely* on the basis of activities protected by the First Amendment to the Constitution. Thus, a request to a library to turn over records indicating what books were checked out by a U.S. person presumably would be justified if it were *related* to an international terrorism investigation—generally a fairly relaxed standard. Moreover, as with the AG Guidelines on maintaining files, the bar on

inquiries based "solely" on protected activity—without a more definitive requirement for showing a connection to terrorism—provides limited protection.

The records covered by Section 215 could have been sought prior to the USA PATRIOT Act by getting a subpoena from a grand jury. However, convening a grand jury requires a criminal predicate. Moreover, grand jury subpoenas would not necessarily enjoy the same level of secrecy imposed by Section 215.

Possible Recommendations:

As suggested above, concerns about the application of Section 215 might be alleviated if a higher threshold were imposed to collect information directly related to First Amendment activity, in addition to barring collection based solely on protected activity. For example, we know that several of the
September 11 hijackers used library computers prior to the attacks. If investigators pick up Internet activity that they reasonably believe is related to terrorism and can identify that it came from a computer in a library during a certain time on a certain day, it makes sense to give them authority to find out who used the library's computers at that time. However, a significantly higher threshold, such as that required to monitor voice communications, should be required to give the government access to information on the content of that activity or what books someone checked out.

More fundamentally, having a separate domestic intelligence collection agency might allow the FBI to return to a context in which a criminal predicate is once again a prerequisite for law enforcement activity. It could also provide a clearer context in which to evaluate and address concerns that relate specifically to the collection of intelligence inside the Unites States, separate and apart from the issues related to what actions the government can take based on that information. Clarifying the distinction between intelligence collection authority and law enforcement power could also clarify oversight responsibility.

Treatment of Immigrants

Because the terrorists involved in the attacks of September 11, like many of those involved in the first bombing of the World Trade Center, were noncitizens, terrorism prevention efforts have had a particular focus on the immigrant community. It is important to improve the nation's ability to know who has entered or is attempting to enter this country. However, because enforcement of our immigration laws and policies has been so lax for so many years, an "enforcement deficit" invites potential discrimination or at least the perception of discriminatory treatment. Moreover, the complexity of immigration requirements and delays in processing paperwork means many people are unwittingly or unavoidably out of status at any given time.

For example, in an effort to get a better understanding of foreigners already present in the country, the government has initiated a registration program. The numbers are too great to register all foreigners at once. Since the hijackers came from the Middle East and that is the ideological home of al Qaeda, the decision was made to register visitors from those countries first. What has exacerbated concern over this disparate treatment is that a significant number of those showing up to register wound up being charged with immigration violations and, often, deported. As with the heightened scrutiny for suspicious

activity described above, the immigration violations were only detected because of the registration requirement. Thus, young Arab men were more likely to be caught and deported because of the decision to require them, as opposed to young men from other countries, to register.

The opportunity to visit this country is a privilege rather than a right. Moreover, the ability of a country to control who enters and lives in their country is a fundamental sovereign right. Thus, countries have wide latitude in setting immigration policies. Once an individual has entered the country, however, more rights begin to attach. The Supreme Court has said that virtually all of the constitutional protections apply to immigrants who have "substantial contacts" with this country.

Moreover, as noted at the outset of this analysis, because community relations can be an important element in preserving security, policies that pass constitutional muster may nevertheless diminish security if they undermine the sense that the system is fair and just. The objections of some in local law enforcement to suggestions that they should take a more active role in enforcing immigration laws, for example, reflect, in part, this concern about disrupting important community relations.

Possible Recommendations:

One possible way to evaluate the rights of immigrants is to distinguish between the fundamental rights accorded to all people—what the founders referred to as unalienable rights—and the whole panoply of specific rights granted by virtue of the social compact between a government and those it governs. In the enemy combatants' situation, for example, you might conclude that all detainees have basic rights against arbitrary detention or torture. Thus, the government must explain the basis for their detention. However, noncitizen/resident detainees may not have a right to challenge their detention in U.S. courts. That right could be viewed as deriving from the social compact and therefore only available to U.S. citizens or permanent residents. This is consistent with the way the Supreme Court has generally viewed these issues.

As noted, however, security may actually be enhanced by adopting policies sensitive not just to the legal rights of immigrants but also to the impact of those policies on the immigrants' way of life and thus on community relations. The "enforcement deficit" is difficult to address short of an overhaul of our immigration policies and enforcement resources. However, at a minimum, evaluations of the actions taken against immigrants as part of the effort to prevent another terrorist attack should include the security costs of infringing on immigrant liberties and way of life.

Conclusion

As Justice Louis Brandeis observed, "Those who won our independence believed that the final end of the state was to make men free to develop their faculties. . . . They valued liberty both as an end and as a means. They believed liberty to be the secret of happiness and courage to be the secret of liberty."

If this nation can maintain the courage to preserve liberty in the face of terror, it will succeed

in sustaining a long-term strategy that defeats the terrorists' objectives.

---

[1] See "Community Policing and Terrorism", Matthew C. Scheider and Robert Chapman, *Journal of Homeland Security*, April 2003, available at http://www.homelandsecurity.org/journal/Articles/displayarticle.asp?article=88, which emphasizes that "community policing philosophy is well positioned to play a central role in local law enforcement responses to terrorism" p. 2.
[2] 18 USC sec 1385.
[3] Jose Padilla, the terrorist suspect arrested in O'Hare Airport and subsequently designated an enemy combatant (*see "Enemy Combatants" section, below*), argued that his detention by the military violated the Posse Comitatus Act (PCA). The court found, however, that PCA did not apply: "Padilla is not being detained by the military in order to execute a civilian law or for violating a civilian law, notwithstanding that his alleged conduct may in fact violate one or more such laws. He is being detained in order to interrogate him about the unlawful organization with which he is said to be affiliated and with which the military is in active combat, and to prevent him from becoming reaffiliated with that organization. Therefore, his detention by the military does not violate the Posse Comitatus Act." Order of Judge Michael Mukasey, U.S. District Court, SDNY, December 4, 2002, at 47.

[4] *See* http://www.cbsnews.com/stories/2003/05/02/attack/main552014.shtml.
[5] 50 USC 1801 et seq.
[6] 50 USC 413b.
[7] United States v. United States District Court (Keith), 407 U.S. 297 (1972).
[8] These kinds of safeguards might also be applicable to privacy concerns regarding health records. Developing appropriate mechanisms for preventing the abuse of access to health information might ease concerns about sharing that information with law enforcement or others who may need it to prevent or mitigate a bioterrorism attack, for example.
[9] Courts have upheld the use of the material witness statute in this context and the Supreme Court has recently held—though in a fractured opinion that left some questions open—that coercive interrogation without criminal prosecution does not violate the Constitution, at least where the interrogation does not "shock the conscience." (*Chavez v. Martinez*, No. 01–1444, Decided May 27, 2003.)

[10] Again, parallels exist in the health arena, where misunderstandings about the application of HIPAA have unnecessarily restricted information sharing.