Heritage Special Report

SR-01
September 20, 2004

Published by The Heritage Foundation

The Patriot Act Reader

Understanding the Law's Role in the Global War on Terrorism

Edited By:

Paul Rosenzweig
Alane Kochems
James Jay Carafano

The Heritage Foundation

The Patriot Act Reader

Understanding the Law's Role in the Global War on Terrorism

Edited by
Paul Rosenzweig, Alane Kochems, and James Jay Carafano, Ph.D.

Paul Rosenzweig is Senior Legal Research Fellow in the Center for Legal and Judicial Studies at The Heritage Foundation and Adjunct Professor of Law at George Mason University.

Alane Kochems is a research assistant for homeland security in the Kathryn and Shelby Cullom Davis Institute for International Studies at The Heritage Foundation.

James Jay Carafano, Ph.D., is Senior Research Fellow for National Security and Homeland Security in the Kathryn and Shelby Cullom Davis Institute for International Studies at The Heritage Foundation.

214 Massachusetts Avenue, NE
Washington, D.C. 20002–4999
(202) 546-4400 • heritage.org

Table of Contents

Foreword

Although a great deal of the debate over new law enforcement and intelligence systems and legislation focuses on perceived intrusions on civil liberties, Americans should keep in mind that the Constitution weighs heavily on both sides of the debate over national security and civil liberties. The President and Congress must respect and defend the individual civil liberties guaranteed in the Constitution when they act, but there is also no doubt that they cannot fail to act when the country faces a serious threat from a foreign enemy.

The Patriot Act is one response to how the United States is waging war against global terrorism while still remaining true to the country's founding ethics of freedom, equality, privacy, and human dignity. The Patriot Act accomplishes three critical goals. First, it gives investigators familiar tools to use against a new threat. Second, it breaks down a wall that has prevented information-sharing between agencies. Third, it updates U.S. laws to respond to the current Internet environment.

Notwithstanding its laudable objectives, much misinformation about the Act abounds and there are numerous scare stories about the potential for abuses in using the Act. However, Americans have strengthened substantially their ability to examine, oversee, and correct abuses of executive power. The public is in a stronger position today than it ever has been before to ensure that civil liberties are not infringed. And the power of oversight gives Americans freedom—freedom to grant the government powers, like those found in the Patriot Act, when the need arises, secure in the knowledge that they can restrain the exercise of those powers appropriately. In short, one lesson from history is that Americans should not be utterly unwilling to adjust their response to liberty and security in today's crisis of terrorism—for they have the capacity to manage that adjustment, and readjust it as necessary.

Edwin Meese III
Ronald Reagan Distinguished Fellow in Public Policy
The Heritage Foundation

I. Introduction

The Patriot Act[1] is a controversial law, some provisions of which will soon require reauthorization. In the post–9/11 world, it is important to understand just what the legislation permits and what it does not. While Congress and the President have constitutional obligations to protect Americans against attacks by foreign actors, that does not mean that the use of such power is always wise or necessary. The Patriot Act has come to symbolize an overstepping of the executive branch's power. Unfortunately, that image is based largely on misinformation.

Although the Patriot Act is very detailed and sometimes difficult to assess, when one takes the time to examine it, one finds that the legislation provides law enforcement the same tools to investigate terrorists as it has used to prosecute drug dealers and mobsters. Furthermore, there are numerous safeguards built into the legislation to prevent abuse of civil liberties. The Patriot Act is an ordinary and necessary piece of legislation.

The Patriot Act accomplishes three critical goals. First, it gives investigators familiar tools to use against a new threat. Second, it breaks down a wall that has prevented information-sharing between agencies. Third, it updates U.S. laws to respond to the current Internet environment. The Patriot Act is one response allowing the United States to wage war against an enemy that attacked the country in disguise, while remaining true to the country's founding ethics of freedom, equality, privacy, and human dignity.

The Patriot Act has, in conjunction with other legislation, strengthened civil liberties. It does so through such things as the expansion of judicial authorization, privacy officers to protect against invasions of privacy, mandatory reports to Congress, and Inspector General oversight. For instance, the Act has one of the most extensive reporting systems of any piece of enacted legislation. The Patriot Act is both common-sense and long overdue. It needs to be reauthorized so that the United States can continue fighting its war on terrorism both at home and abroad.

When assessing civil liberty questions, it is important not to lose sight of the underlying purpose of government: personal and national security. The balance between civil liberties and security is not a zero-sum game. Thus, it is vital to realize that there are significant factors weighing on both the civil liberty and national security sides of the scale. That is why, for example, the courts have recognized that in the national security context, the requirements of the Fourth Amendment apply somewhat differently than they do in the context of domestic law enforcement.

Suppressing terrorism will not be achieved by military means alone. Effective law enforcement and intelligence-gathering activities are key to avoiding new terrorist attacks. The traditional law enforcement model is highly protective of civil liberty in preference to physical security. However, September 11th changed this traditional calculus—our failure to prevent terrorism can be catastrophic. And so, our goal should be to minimize infringements on civil liberty while maximizing our preventative abilities.

The 9/11 Commission has emphasized the importance of the Patriot Act and considers it to be an essential weapon in the global war on terrorism. Prior to September 11, there was a wall of legal and regulatory policies that prevented effective sharing of information between the intelligence and law enforcement communities. The Patriot Act has worked to lower this wall between government agencies. The Patriot Act adopts as a general principle the rule that any information lawfully gathered during a foreign or domestic counterintelligence investigation or during a domestic law enforcement investigation should be able to be shared with other federal agencies. The artificial limitations that have been imposed on such information sharing are a relic of a bygone era and, in light of the changed nature of the terrorist threat, are of substantially diminished value today.

Based upon our limited experience thus far, it seems that the advantages gained are substantially greater than the potential dangers posed by changes in the investigative authority granted the executive branch—but Congress

1. The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. 107-56, 115 Stat. 272 (Oct. 26, 2001).

will make that assessment on a full record when it reconsiders these portions of the Patriot Act next year. In doing so, it would be wise to remember the past—and the problems that it identified as requiring change when it initially adopted the Patriot Act.

The government cannot decide policy based upon an over-wrought sense of fear. Most of the provisions of the Patriot Act have been previously used to combat organized crime, and there is no evidence of any real abuse. The key is empowering government to do the right things while exercising oversight to prevent the abuse of authority. So long as people keep a vigilant eye on police authority, so long as the federal courts remain open, and so long as the debate about governmental conduct is a vibrant part of the American dialogue, the risk of excessive encroachment on fundamental liberties can be avoided.

A final note: Most of this reader has appeared elsewhere. Please see the bibliography for specific sources.

Paul Rosenzweig
Alane Kochems
James Jay Carafano, Ph.D.

II. Protecting Civil Liberties and Fighting Terrorism: The USA Patriot Act

The following is an edited transcript of a Heritage Foundation event entitled "Protecting Civil Liberties and Fighting Terrorism: The USA Patriot Act," which was held May 4, 2004.

Introductory Remarks by Edwin Meese III
Ronald Reagan Distinguished Fellow in Public Policy
The Heritage Foundation

- The Patriot Act allows the investigative and surveillance techniques that have been applicable to other types of criminal activity, such as drug trafficking and organized crime, to be applied to terrorism.
- Despite the numerous safeguards built into the legislation, there is a great deal of misinformation being spread throughout the country, which has caused people to think falsely that civil liberties are threatened.

EDWIN MEESE III: After the events of the 11th of September 2001, a number of things happened. Military action was commenced against the terrorists. The Department of Homeland Security was established and legislation was passed to provide investigators and intelligence agents with the legislative authority and instruments to carry on the global war against terrorism, and particularly to defend homeland security.

For the most part, various investigative and surveillance techniques that have been applicable to other types of criminal activity, such as drug trafficking, organized crime, and the like have been applied to terrorism. But despite the fact that a great many safeguards were built into the legislation which has become known as the USA Patriot Act, a great deal of misinformation has been spread throughout the country causing some people to fear that civil liberties are in danger.

Today we have a panel of experts to talk about the Patriot Act, civil liberties, and homeland security and to set the record straight on this particular subject.

Our first speaker is James J. Comey, the Deputy Attorney General of the United States. He has a distinguished record as a prosecutor. He was the United States Attorney for the Southern District of New York. He has been in private practice, he has been an Assistant U.S. Attorney, and has now taken one of the leadership positions in the Department of Justice.

Remarks by James J. Comey
Deputy Attorney General of the United States

- The Patriot Act is very detailed and difficult to understand. However, once one examines the Act's details, one sees that it is an ordinary, yet necessary, piece of legislation.
- The Patriot Act takes tools currently available to other criminal investigators like roving wiretaps and sneak-and-peek warrants, and extends them to counterterrorism investigation, while establishing safeguards for the tools' use.

JAMES J. COMEY: Thank you Mr. Meese. I want to thank you and thank the Heritage Foundation for offering this opportunity to talk about the Patriot Act. It is an incredibly important piece of legislation and one I believe we cannot talk about enough. One of the challenges we in government face is urging our fellow citizens to find the space in their busy lives to understand the Patriot Act. We have had a couple of years with a lot of confusion, a lot of misunderstanding and, frankly, some outright misrepresentation about the Patriot Act, and that poses a great challenge for those of us in government. It is difficult sometimes to shout details into the wind of bumper stickers that we face on the Patriot Act. But the "angel" in the Patriot Act is in the details and so I'm very grateful to you and particularly grateful to the President of the United States for taking time to foster this debate and to educate the American public about the Patriot Act.

I've spoken an awful lot about the Patriot Act, as have the other folks on this panel. Recently, I spoke to a group on the Upper West Side of Manhattan. The next time you're at a cocktail party, I said to them, and you're standing around with a glass of a lovely chardonnay and someone says, "Isn't the Patriot Act evil?" before you nod reflexively, do me a favor: Ask that person, "What do you mean, specifically? What parts of it bug you? What parts of it do you think are evil?" And the response you're going to get is "Hum-i-na, hum-i-na, hum-i-na." This is because the details are challenging, the details are time-consuming, the details are often burdensome for people to master. But if they understand them and master them, the "hum-i-na, hum-i-na" will become an appreciation for how much of the Patriot Act is simply taking the tools that we've used for decades to lock up drug thugs and mobsters and for the first time allowing counterterrorism investigators to use them to lock up, to follow, to monitor al-Qaeda and other people who would do us grave harm.

What I want to do is give you a couple of examples about the way in which I've used the tools of the Patriot Act and the ways in which they are so ordinary and so smart that we have to have this debate now, even though these important tools sunset in 2005. We cannot, like some kid putting off a term paper until the night before it's due, and then cramming, cram on the Patriot Act because we cannot take the risk that we'll lose some of these tools.

First example: roving wiretaps. In the 1980s drug dealers, like most good folks, started using cell phones. Toward the mid-1980s they started to realize that we in government could track their drug-related conversations by getting wiretaps on those cell phones. So they started dumping their cell phones, swapping them with others, trading them out, getting new ones to stay ahead of law enforcement. Then, in the late 1980s, Congress gave drug investigators a tool. They allowed us to go to a federal judge, make the same showing that we need to obtain a wiretap—that is, probable cause to believe that a crime is being committed on this telephone—and with the making of an additional showing—that is, that the drug dealer is swapping phones to avoid surveillance—obtain an order that allows the government not just to intercept the conversations on a particular instrument but to intercept the conversations of that drug dealer no matter what phone he's on.

Why does that matter? If you know he's committing crimes on the phone, you could just go get another new order for the new phone. That's absolutely right, but that causes a period of darkness, in which the drug dealer gets rid of a phone, we then figure out he's on a new phone, write up a new order, and find a new federal judge. That can be done sometimes in six or seven hours—but in that period of time we've lost six or seven hours of important drug-related phone calls.

Why do I tell you that? What the Patriot Act did was take that tool and allow it to be used by foreign intelligence and foreign counterterrorism investigators. They can go to a federal judge on the Foreign Intelligence Sur-

veillance Act (FISA) Court. (People often forget that there are federal judges all over this program.) They can file a sworn affidavit that lays out probable cause to believe that a person is an agent of a foreign power or foreign terrorist organization and that that person is changing telephone instruments in an effort to avoid surveillance, and get an order that allows that foreign counterterrorism investigator to intercept the conversations of that individual no matter what phone he's using. That's a tool we've used to lock up drug dealers since 1986. Since the fall of 2001, it's a tool we can use to track al-Qaeda—and anybody who thinks that al-Qaeda is less clever than drug dealers is kidding themselves.

Could we do without this tool? Theoretically, we could, and we did without it before the fall of 2001. But that means a period of darkness—six hours, seven hours, eight hours, sometimes 24 hours—before we're able to get back up on the new phone. All of us learned, to the extent that we didn't know before, that those hours of darkness can be a time of great peril for America. We simply cannot afford to run that risk. We cannot afford to allow that tool to sunset.

Now, it just took me just three or four minutes to explain roving wiretaps. Finding the time for people to understand more than the bumper sticker about roving wiretaps can be difficult.

Second example: so-called sneak and peek search warrants. Again, that bumper sticker sounds bad. "Sneak and peek" sounds like we're going through your sock drawer late at night while you're sleeping. Let me explain what that is. Delayed notification search warrants are what we in law enforcement call that tool. We've been using it since before I was born to protect people and to protect evidence in our most sensitive investigations. Let me give you a personal example.

When I was in Richmond, Virginia, a violent gang of crack dealers from New York was looking to muscle in on the Richmond drug market. The Drug Enforcement Administration didn't quite have a handle on them, but they had one informant who told them that the gang had an apartment in the west end of Richmond where they had just delivered 5 kilos of cocaine.

We then had a choice to make. Do we go and seize those 5 kilos, risk the informant's life, and blow the investigation so that we can never identify the leaders, or do we let 5 kilos of cocaine walk onto the streets of Richmond so that we can preserve our investigation? We didn't have to make that choice. A judicially created mechanism called a delayed notification search warrant gave us the ability to conduct a search and delay telling the bad guys about it.

We went to a federal judge in Richmond and laid out in a sworn affidavit just what I've told you. Upon that showing of probable cause and that disclosure would risk lives and endanger evidence in a very important investigation, the federal judge gave the DEA permission to conduct the search and to make it look like a burglary.

So the DEA agents broke into the apartment. They took the TV, the stereo, and 5 kilos of cocaine, and in a little rhetorical flourish they poured some beer down the sink and left the beer cans around. They also broke a window from the outside in. Two leaders of this drug gang came to the apartment not long after the agents left and they called the cops.

A uniformed officer was sent (who had been briefed on what was happening) and he asked seemingly routine questions: "Who are you?" "Your date of birth, sir, and this is your apartment?" "Can I see your driver's license?" "And your buddy, here, is this his apartment too? And his name is?" He identified the leaders and tied them to the apartment. He asked them what had been taken, and they said, the TV, the stereo and they drank our beer. "Anything else taken?" "Nothing else taken." No mention of the drugs, which won't surprise you. And so law enforcement took the drugs off the street, and was able to follow up on the information that the officer collected and identify all the rest of the members of this drug gang. Two months later, after they were locked up, disclosure was made that the search had been conducted. The DEA offered, to anyone who would claim them, to return the TV and the stereo, and they paid the landlord for the fixing of the window.

When people take the time to listen to that example, their opinion changes dramatically. No one wants law enforcement to have to choose between endangering lives and letting kilos of cocaine walk onto the streets of a city in America. That's why judges created that the delayed notification search warrant. That's why judges on the Supreme Court concluded in 1979 that it was reasonable under the Fourth Amendment to use this tool. All the

Patriot Act did was put it in black letter law of a statute so there would be a uniform standard across this country. It's now available for counterterrorism investigations and the standard is set out for any federal prosecutor or federal agent that wants to use it in a drug or organized crime investigation. It is a tool that is much too important to the security of the United States—and frankly to the security of people who are plagued by drug gangs and by Mafia bosses—to be allowed to sunset.

So, if you take one thing away from my two quick points, it is that the angel is indeed in the details in the Patriot Act. It's smart, it's ordinary, it's essential. We need the help of all people who care about security to go to those cocktail parties and to stand there and to say, "What are the details about the Patriot Act, why does it matter?"

It is good to question government power. Our country was founded by people who had a big distrust of government power by certain parties. And I believe it's incumbent upon government to explain how we're using our power and a great thing to engage in that discussion. But if people understand how we're using these tools and why they matter so much, they will not want them to go away. Thank you for helping us find that space.

EDWIN MEESE III: Thank you very much Jim. We turn now to an old friend with whom I had the privilege of working in the Justice Department. Asa Hutchinson is the Undersecretary for Border and Transportation Security in the Department of Homeland Security. He has the major task of bringing together the various agencies that came to that department and that are responsible for borders, transportation, and enforcement of immigration laws. He has the bulk of the people in the department. Some 110,000 people are working for him on the monumental task of bringing into one force the people who have the responsibility for inspections on the border. He has been a member of Congress, he was the United States Attorney in Arkansas, and he has a distinguished record of public service. Please welcome Asa Hutchinson.

Remarks by Asa Hutchinson
Undersecretary for Border and Transportation Security

The Patriot Act accomplishes three critical goals.

- First, it gives investigators familiar tools to use against a new threat.
- Second, it breaks down a wall that has prevented information sharing between agencies.
- Third, it updates U.S. laws to respond to the current Internet environment.

ASA HUTCHINSON: I'm glad to be here today to talk about the Patriot Act. My friend Jim Comey was talking about drinking chardonnay in New York City and people raising questions about the Patriot Act. I was down in Georgia yesterday on family business, not drinking chardonnay but sweet tea. Someone came up to me and said, "Let me talk to you about the Patriot Act—and you think the government ought to be able to detain American citizens and not let them call their wife and keep them incommunicado?"

I've studied the Patriot Act. I know the Patriot Act, but I had no clue where this was coming from. People out there have misinformation about the Act and have a way of tagging things that they are concerned about to the Patriot Act. Of course it has nothing to do with the Patriot Act, and I gave her that assurance.

Jim correctly articulated that the tools that are given to fighting terrorism have been commonly used by us in fighting drugs and other organized crime elements for the past 20 to 35 years. I was just going to outline some important messages in the Patriot Act.

First, it gives old tools to use against a new threat, and that is critical for us. When I was the United States Attorney we used the delayed notification procedures for search warrants. It was absolutely essential, not just to go into the storage unit and find the drugs but also to delay notifying the owner of that storage unit so that you can know when they come to get into that locker that would have the cocaine there in that storage facility. So, we're updating that, giving that capability to law enforcement and in our national security efforts.

The second thing that it does is break down the wall dividing information. To me, it's the most essential thing that the Patriot Act does. It says that if you're collecting intelligence for national security purposes you can also, if there's a violation of law, share that information; if you're collecting it for law enforcement purposes and find out information that they ought to know in the counterterrorism arena, you can share that information. Previously, there were cultural walls and legal impediments. Those were broken down in the Patriot Act. It is absolutely essential for the information to flow to the people who need it every day in a very quick fashion.

The third thing that it does is update our laws to the age of the Internet. When I was in Congress, we held hearings in the Crime Subcommittee in 1998 or 1999 about how our electronic surveillance statutes really did not fit the Internet age. The Patriot Act updates our laws to include more sophisticated means of communications in a lot of different ways that are important for us in fighting crime.

Still, there are objections to the Patriot Act. Jim addressed one, about the delayed notice provision we've had for 35 years. Another objection that is raised is the Patriot Act allows the feds to go after your library records. I think of it in the drug context. Suppose an individual was arrested with a lot of chemicals and laboratory equipment. We think he had the intent to manufacture methamphetamine. He insists that he was doing chemical experiments. How do you show the intent? We found out that he had been regularly visiting a particular library. We would get a grand jury subpoena to see if he was actually reading books on making methamphetamine or logging on the Internet to get those recipes. That would help to establish his intent to utilize those recipes.

If you are investigating a Mohammed Atta, and you're trying to show that he had the intent to commit a terrorist act, it might be that you can show the intent for making explosive devices in the same way.

The important thing is that a court order must be gotten before any of this can be undertaken. It has been pointed out in numerous instances the Justice Department has not used this tool. I think you can understand why it is very important to have.

Although not not necessarily part of the debate, there are many new requirements in the Patriot Act. Congress used the Patriot Act to expedite the SEVIS rules used to monitor international students so that we know when they enter and leave the country. It required background checks on the 3.5 million drivers that are licensed to drive hazardous materials, which could be very dangerous in the hands of terrorists.

Finally I would mention that the Patriot Act gives us new abilities in the financial arena. Immigration and Custom Enforcement has been a part of the Department of Homeland Security since January of 2003. Using the tools given to them under the Patriot Act, customs investigators have made 13,000 arrests, gotten 720 indictments and 560 convictions, and seized approximately $150 million through financial investigations of illegal activity. The new financial investigation tools have been very important to breaking the cycle of terrorist funding.

So, the Patriot Act does a lot of things, but it has the important protections that are critical in our regard for civil liberties. From a Homeland Security perspective that is very important. We are mandated not just to protect the borders and transportation systems of the United States but also to protect our freedoms and civil liberties. It's something that we take very seriously. The Patriot Act is an important tool in that effort.

EDWIN MEESE III: William J. Fox is the Director of the Financial Crimes Enforcement Network (FINCEN), which deals with problems such as money laundering and in this context, particularly, the financing of terrorism.

One of the most important aspects of terrorist organizations is the support mechanism, and particularly the funding to allow them to operate. So one of the important counterterrorism tools is the ability to investigate the financings of these organizations.

Bill Fox has a long history of excellent work in the Treasury Department. He was Associate Deputy General Counsel at the Bureau of Alcohol, Tobacco, and Firearms as well as Acting Deputy General Counsel of the Treasury Department. He has worked a great deal on some of the key legislation that deals with financial crime.

Remarks by William J. Fox, Director of the Financial Crimes Enforcement Network (FINCEN)

- Title III addresses two issues. First, it enhances the government's ability to share information with regard to financial transactions. Second, it expands the regulatory scheme that is in place to deter, detect, and stop illicit funding, especially funding for terrorism.
- The enhanced regulatory scheme is a risk-based system. The government is setting the parameters and then asking the industry to create customized anti-money laundering programs that make sense for the type of business they do and the customers they have.

WILLIAM J. FOX: Thank you very much. It's really an honor to be here at the Heritage Foundation.

We've heard an anecdote from New York and we've heard an anecdote from Georgia. Let me give you anecdote from Nebraska, where I'm from.

I was honored to become the FINCEN's fourth director in December 2003. I went home to my family over the Christmas holidays and began to explain the job that I'd just achieved. The first thing I got back was, "Oh! You're those guys that have bank account information on every single American citizen, aren't you?" And I said, "Absolutely not!" But part of the reason, I think, for that belief out there in America is some of the misinformation that has occurred in and around the USA Patriot Act.

I'm here to talk today about Title III of that Act, a section called the International Money Laundering Abatement and Anti-Terrorist Funding Act of 2001. Title III of the Act is dedicated to addressing the issues or gaps that we had in our system as it relates to finance or illicit finance, whether that involves significant money laundering or whether it involves the financing of terror.

Really, Title III addresses two issues. The first is an enhancement of our information sharing capability when it comes to finance. And the second is an enhancement of the regulatory system we have in place to try to deter, detect and stop illicit funding, particularly the funding of terror.

Let's talk about information sharing first. Title III of the Act authorizes the sharing of information that is reported under a statute that FINCEN administers called the Bank Secrecy Act. For certain purposes when it comes to terrorism, we can now share important and critical financial information—not only with law enforcement, which we've done for a long time, but also with our intelligence community. Money and finance is a key way to detect terrorism. Money doesn't lie. Money allows us to follow and identify networks, and it is hypercritical, in my view, to be able to share some of that information under the right circumstances and under the right controls with the folks we've charged with protecting us from another attack.

Title III also amended the Right to Financial Privacy Act to allow greater access by law enforcement to consumer financial information—again, under the right circumstances and with the right protections. The Fair Credit Reporting Act was amended similarly.

Finally, Section 314 of Title III mandates greater information sharing both vertically and horizontally, with the financial industry that we regulate. Section 314 has received some press attention, and I would like to set the record straight as to what we are doing under this provision and what it's really all about.

Section 314(a) is essentially a pointer system. It's a way to save gumshoe work in these critical investigations. We will take a request from law enforcement, perhaps the Bureau of Immigrations and Customs Enforcement or the FBI, and we will blast names under investigation in a secure way to financial institutions. They will search their records and come back to us with a simple "Yes" if they have information. If they say "No," they don't come back to us. We then feed that information back to law enforcement, and it's up to them to get subpoenas or whatever legal authorization that is required to actually obtain that financial information. So the protections are actually built in there. We do not have bank account information at FINCEN. We don't want bank account information at FINCEN. But this

pointer system allows law enforcement to identify where financial information may exist out there in a way that saves a great deal of time when time is very critical.

There are only two purposes for the use of this important tool; the first, of course, is terrorism and the second is significant money laundering. We vet those requests at FINCEN to ensure that they meet a standard for the use of this important tool. And frankly, we ensure that law enforcement has actually reached the point where they can't find any additional information. In other words, we're not using this as just a short-cut for law enforcement to find this information. This is really a tool of last resort and it has worked incredibly well.

Since February 1, 2003 til April 27, 2004, 260 such requests involving 17,000 subjects were made by 12 federal law enforcement agencies. The breakdown is that 164 of those requests were related to significant money laundering cases and 96 related to terrorism investigations.

These requests identified 11,058 accounts that law enforcement did not previously know about. Over 700 subpoenas and other processes were set in motion to obtain those documents and those actions have led already to arrests and indictments. So we're very pleased with what's happened. Law enforcement has told us that this is an incredibly important tool for our capabilities to address particularly terrorism when time is really of the essence.

We are also enhancing our regulatory scheme pursuant to Title III of the Act. We're requiring a broader range of financial industries to adopt and create anti–money-laundering programs. These are industries such as broker/dealers, futures commissions merchants, casinos, money services businesses or businesses that transmit money (which can be a particular threat in relation to terrorist financing), mutual funds, credit card system operators. We've got proposed rules out on certain aspects of the insurance industry and on dealers in precious metals, jewels and stones. The Act actually mandates us to look at things like real estate closings and vehicles sales, and we're studying those issues to see whether or not it makes sense to bring those folks into a compliance.

I think it's important to emphasize that the system that we're implementing here is a risk-based system. In other words, we're setting certain parameters and we're asking the industry to create custom-made anti–money-laundering programs within those parameters that make sense for the business that they do and for the customers that they have. The feedback so far on that has been terrific. We are already seeing better reporting under the Bank Secrecy Act and more rich reporting that is helping law enforcement and, in the case of terrorism, even the intelligence community.

I think one of the challenges at FINCEN and in the federal government is to find a way to better communicate with the industry on assessing the risk posed by terrorist financiers and money launderers. Think of a river or stream and the illicit finance is a break in a dike or a river bed. We are working with the financial industries to try to repair that break as it happens or even maybe strengthen the river bed before it happens. But this is a very challenging aspect because money launderers and illicit financiers or terrorist financiers are usually two or three steps ahead. So it's our goal to try to catch up and get there ahead of them.

I just want to finish up by emphasizing again, as Secretary Hutchinson did, that we at FINCEN take concerns about privacy very seriously. In fact, I would argue that under our reporting regime, under the Bank Secrecy Act it's actually critical, it's a keystone. Finance is a way to get at criminals and terrorists. And we think it's incredibly important that we keep this information the way it's supposed to be and collect only that information that is relevant to that sort of work .

EDWIN MEESE III: Bill Bennett has a distinguished record of public service as Secretary of Education and Chairman of National Endowment for the Humanities under Ronald Reagan and as Director of the Office of National Drug Control Policy under the first President Bush. I consider him one of the leading commentators on society and culture, and he has either authored or edited some 14 books. In addition, he serves as a co-chairman of Empower America. But as if that wasn't enough, Bill has recently taken on some new responsibilities. He's chairman of an organization called Americans for Victory Over Terrorism, which is a project of the Claremont Institute, and has recently begun a nationally syndicated radio show.

Remarks by William J. Bennett, Co-Director of Empower America

- A critical question, to which the Patriot Act is one response, is how does the United State wage war against an enemy that attacked America in disguise, while at the same time remaining true to the country's founding ethics such as freedom, equality, privacy, and human dignity?
- The Patriot Act is both common sense and long overdue.
- The Act needs to be reauthorized so that the United States can continue fighting its war on terrorism both at home and abroad.

WILLIAM J. BENNETT: It's a pleasure to be on this distinguished panel. I have learned a lot already.

In light of the news that has come from Abu Ghraib prison, some will no doubt say that a government that cannot be trusted with prisoners cannot be trusted with suspects. That's not true. That's not the government of the United States we are talking about.

John Stuart Mill, I think, is appropriate here. He says, "Any standard will work ill if we suppose universal idiocy or barbarism to be conjoined with it." And that's true. As Justice Holmes said once, "The main remedy for most of what ails us is to grow more civilized." And that, I think, is an appropriate word to use given the current circumstance, because it is a battle between civilization and barbarism. It makes not a little difference, not some difference, but as Aristotle would say, "All the difference" whether the barbarism is an exception to your standard (Abu Ghraib now), or if barbarism is your policy (Abu Ghraib before). What happened over there with some of our military police and others is condemned by a civilized society and will be remedied by a civilized society.

I think our first task in talking about civil liberties in the context of this war is to remember a few things that it seems some people have forgotten, and to put the whole debate in a general and historical context. Our enemy attacked us in disguise, not in uniform, not in marked war planes from an enemy country. Unlike Pearl Harbor, our enemies trained abroad, moved here, lived here under the guise of legality, and used civilian aircraft and civilian tactics and civilians to kill as many innocent people as possible. Also, unlike Pearl Harbor, their targets were not military, but civilian. And unlike Pearl Harbor, it appears that much of the money used to finance our enemies came from money raised in the United States and from money raised in countries that are purported allies of the United States.

So, how do we wage war against such an enemy while at the same time staying true to our own founding ethics—ethics such as freedom and equality and privacy and human dignity, ethics that seem to be one of the main reasons for our enemies' wrath? These are not new questions. In *Federalist* No. 3, John Jay writes: "Among the many objects to which wise and free people find it necessary to direct their attention that of providing for their safety seems to be the first." Being a country that values such things as freedom, we have, several times, faced the question of how to reconcile that freedom with the first object of government—security—especially in wartime. One hundred and forty years ago Lincoln asked: "Must a government of necessity be too strong for the liberties of its own people or too weak to maintain its own existence?" The answer to Lincoln's question is now, as it was then, a resounding "No!"

But now, let us look to what has happened since 9/11, keeping in mind all the distinctions between that attack and the previous attack on us in 1941.

We have not, as Franklin Delano Roosevelt and the great liberal Earl Warren did, established internment camps for over 100,000 U.S. citizens whose only crime was looking like people we were at war with in another country. Nonetheless, the rhetoric is in some instances more heated about our response to 9/11 than it ever was in the 1940s. So-called conservative libertarians and liberal libertarians from the American Conservative Union and Bob Barr to the ACLU and John Kerry have at times made it sound like we live under Mitchell Palmer's Red Scare tactics or J. Edgar Hoover or I guess, one might say, Franklin Delano Roosevelt and Earl Warren.

But we don't live like that and we don't profile like that. We have given trials to those who claim abuses of our post–9/11 system. We have even released prisoners from Guantanamo to our detriment, as we now learn that four of those that we released have re-joined al-Qaeda in Afghanistan.

But let's be specific to the Patriot Act, The Patriot Act may be great fund-raising fodder for the ACLU. I'm happy to note, however, that the public is not buying into this media and inside-the-Beltway generated crisis. For all the 2003 Democrat primary attacks on John Ashcroft and the Patriot Act, it is worth noting, as George Will recently did, how such attacks have subsided in the wake of the news that over 60 percent of the public supports the Patriot Act without even knowing what it's about. Not a surprising statistic, given that 99 Senators voted for it. Who listening to the Democratic primaries remembers that fact?

Perhaps nothing concentrated the mind on this so much as Bill Clinton's Attorney General, Janet Reno, telling the 9/11 Commission just a couple of weeks ago that "Everything that's been done in the Patriot Act has been helpful." And just last October, Senator Joseph Biden called the criticism of the Patriot Act "ill-informed and overblown." Senator Dianne Feinstein said, "I have never had a single abuse of the Patriot Act reported to me." And when she asked the ACLU for examples of violations of civil liberties under the Patriot Act, Senator Feinstein said, "They had none."

So let me part with some of my fellow conservatives who oppose this Act and stand with Democrats such as Joe Biden, Dianne Feinstein, Janet Reno, and most conservatives and re-endorse the Patriot Act. We are not like the Kingdom of Jordan that engages in torture as a matter of policy; we court-martial those who torture on our behalf and we revile the practice. In light of the reports coming out of Abu Ghraib we are rightfully ashamed and angered.

When Daniel Patrick Moynihan declared that he was not ashamed to speak on behalf of the United States, a less than perfect country, he said, "Find me a better one. Do I suppose there are societies which are free of sin? No, I don't. Do I think ours is, on balance, and comparably the most hopeful set of human relations the world has ever seen? Yes, I do. Have we done obscene things? Yes, we have. How did our people learn about them? They learned about them on television and in the newspapers."

We use the law, we use the courts, we use the press. They are all sources of protection, and so is the Patriot Act. The Patriot Act is not only common-sensical but long overdue given the warnings we had for years before 9/11. We need to reauthorize the Patriot Act next year so we can continue fighting our war on terrorism, both at home and abroad; so that we can disrupt terrorist cells both at home and at abroad; and so that we don't, in the words of another great Democrat, Justice Robert Jackson, let our Bill of Rights become a suicide pact.

Concluding Remarks by Edwin Meese III

- The Patriot Act, in conjunction with other legislation, strengthened the civil liberties Congress has provided. This includes the expansion of judicial authorization, privacy officers to protect against invasions of privacy, mandatory reports to Congress, and Inspector General oversight.
- The Patriot Act has one of the most extensive reporting systems of any piece of enacted legislation.

EDWIN MEESE III: One of the interesting things about this whole subject is that in the Homeland Security Act and the Patriot Act Congress provided a number of strengthened protections of civil liberties. For example, the requirement of judicial authorization has been expanded. To gain access to business records of various sorts, including library records, you don't just get a grand jury subpoena, which is relatively easy; it now requires a judge's order.

There are officials to guard civil liberties provided for in both the Justice Department and the Department of Homeland Security. There's a privacy officer in the Department of Homeland Security whose sole responsibility is to guard against invasions of privacy that are contrary to the spirit of this legislation. There is now a provision in

the Patriot Act for money damages against the government, rather than simply against an offending officer (who's usually judgment-proof). Thus, if information gained through these various investigative techniques is abused, the person who is harmed can now get into the deep pocket of the federal government to satisfy their money damages. The Department of Justice Inspector General is required to investigation any allegation of abuse in any part of a terrorism investigation.

And finally, the Attorney General and the Department of Homeland Security are charged with making numerous reports to Congress so that the relevant committees of Congress can provide oversight. At the time of the reauthorization, if there are things that need to be changed or updated or corrected, lawmakers can act based upon full information coming from these reports. This is the most extensive reporting system of any statute in the entire federal code.

III. The Patriot Act for Thoughtful Conservatives

A. Theory

i. Some General Principles

Just because the Congress and the President have a constitutional obligation to act forcefully to safeguard Americans against attacks by foreign powers does not mean that every means by which they might attempt to act is necessarily prudent or within their power. Core American principles would seem to require that any new counter-terrorism technology (deployed domestically) should be developed only within the following bounds:

- No fundamental liberty guaranteed by the Constitution can be breached or infringed upon.
- Any increased intrusion on American privacy interests must be justified through an understanding of the particular nature, significance, and severity of the threat being addressed by the program. The less significant the threat, the less justified the intrusion.
- Any new intrusion must be justified 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 "fit" between the technology and the threat (that is, for example, if it is accurate and useful in predicting or thwarting terror), 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 against terror, uniquely, is one with no immediately foreseeable end. Thus, excessive intrusions may not be justified 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.

From these general principles can be derived other, more concrete conclusions regarding the development and construction of any new technology:

- 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, depending upon its sphere of operation.
- Similarly, no new system should alter or contravene existing operational system limitations. Development of new technology is not a basis for authorizing new government powers or new government capabilities. Any such expansion should be independently justified.
- No new system that materially affects citizens' privacy should be developed without specific authorization by the American people's representatives in Congress and without provisions for their oversight of the operation of the system.
- 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.

- Similarly, any new system should, to the maximum extent practical, be developed in a manner that incorporates technological improvements in the protection of American civil liberties.
- Finally, no new system should be implemented without the full panoply of protections against its abuse. As James Madison told the Virginia ratifying convention: "There are more instances of the abridgment of the freedom of the people by gradual and silent encroachments of those in power than by violent and sudden usurpations."[1]

These theoretical considerations and operational guidelines, while useful in constructing an *ex ante* heuristic for assessing new programs and law, are only of real value in application to concrete problems and proposed solutions. It is not enough to condemn every governmental initiative. Nor is it correct to give the government a blank check for all actions designed to repel terror. Rather, each program and proposal must be carefully assessed on its own individual merits. Measured against these standards, the Patriot Act, and related governmental programs hold up fairly well—by and large they pose little practical threat to civil liberty and they hold the promise of significant benefit.

ii. The Lessons of History and Contemporary Oversight

• We must not be too harsh in our retrospective judgments since hindsight is always 20/20. Furthermore, as we face today's challenges, we must be a little generous in our self-review, since it will remain unknown for many years whether today's fears are well-founded.

• A better view of history shows that the balance between liberty and security is more like a pendulum that gets pushed off-center by significant events (like September 11th). Once Americans have recovered from the shock of the catastrophe and after the threat recedes, the pendulum returns to the center.

• Factors that constrain excesses include a more activist court; a more partisan Congress; the growth of investigative journalism; the rise of public interest groups; the increase in the public's ability to monitor government; and a more educated public with regard to civil liberties.

As we consider the American response to terrorism and the use of executive power, many caution against repeating past excesses. They see in history a series of lessons about over-reactions in the face of war. In this vision, prior threats have necessarily led to good-faith, but overly zealous responses. The tension between civil liberty and national security is but one example of how we return to the same fundamental issues over and over again. Consider the following history.[2]

In 1798, the Napoleonic wars raged in Europe. President John Adams, a Federalist, effectively brought the United States into a state of undeclared war with France, on the side of the British. Thomas Jefferson and the Democratic Republican party opposed these measures as likely to provoke an unnecessary war. The Federalists, in turn, accused the Jeffersonians of treason.

To exacerbate the situation, the Federalist Congress enacted the Alien and Sedition Acts of 1798. The Alien Act authorized the President to deport any non-citizen he judged dangerous to the peace and safety of the United States, without a hearing or the right to present evidence. The Sedition Act prohibited the publication of false,

1. Speech to the Virginia Ratifying Convention, June 16, 1788, reprinted in Matthew Spalding, ed., *The Founders' Almanac* 133 (The Heritage Foundation, 2002).
2. This summary of the history is substantially derived from a lecture Professor Geoffrey Stone of the University of Chicago recently gave to the Supreme Court Historical Society. See Geoffrey Stone, *Civil Liberties in Wartime*, 28 J.S. Ct. Hist. 215 (2003). This article provides a far more detailed summary and understanding of these historical events, and is the source of much of the historical information summarized below, though it reaches different conclusions regarding the lessons to be drawn from that history.

scandalous, and malicious writings against the government, the Congress, or the President with intent to bring them into contempt or disrepute. These were, in effect, aggressive efforts to suppress political criticism of Adams, his policies, and his administration. The Act expired by its terms, and after Jefferson replaced Adams as President, he pardoned all those who were convicted under the Act. Though never tested in the Supreme Court, these acts are widely regarded as having been unconstitutional and a stain on American liberty.

During the Civil War, President Abraham Lincoln suspended the writ of habeas corpus on eight occasions. The broadest such suspension declared that "all persons . . . guilty of any disloyal practice . . . shall be subject to court martial."[3] As many as 38,000 civilians were imprisoned by the military in reliance on this authority. In 1866, a year after the war ended, the Supreme Court ruled that the President was not constitutionally empowered to suspend the writ of habeas corpus, even in time of war, if the ordinary civil courts were functioning. Here, again, the suspension is remembered by some as an excessive response to a crisis and has come to be regarded as an unfortunate wartime error.

In 1917, the United States entered World War I. During the war, federal authorities acting under the aegis of the Espionage Act prosecuted more than 2,000 people for their opposition to the war. As a result, virtually all dissent with respect to the war was suppressed. Though the Supreme Court initially approved most federal actions in support of the war, over the next half-century, the Court overruled every one of its World War I decisions, effectively repudiating the excess of that wartime era.

Finally, and most notoriously, on February 19, 1942, President Franklin Roosevelt signed Executive Order 9066,[4] which authorized the Army to "designate military areas" from which "any persons may be excluded." Over the next eight months, more than 110,000 people of Japanese descent were forced to leave their homes in California, Washington, Oregon, and Arizona. Though the Supreme Court upheld the President's action, it has come to be recognized as a grave error. In 1988, President Ronald Reagan offered an official presidential apology and reparations to each of the Japanese-American internees.

Some see in this history a cautionary note. As Professor Geoffrey Stone has said: "In time of war—or, more precisely, in time of national crisis—we respond too harshly in our restriction of civil liberties, and then, later regret our behavior."[5] We should not disregard that caution.

But reading too much into this history is a mistake—potentially quite a grave one. First, and most obviously, it disregards the reality of necessity. As Justice Arthur Goldberg so famously said, "while the Constitution protects against invasions of individual rights, it is not a suicide pact."[6] And while some of these reactions were plainly overreactions (nobody argues today that the internment of the Japanese served a useful military purpose), others were not.

Many, for example, think that Lincoln's suspension of the writ of habeas corpus was essential to the prosecution of the war. Some argue that it was necessary to protect the troops, save Maryland for the Union, and secure the safety of Washington, D.C. Lincoln certainly felt the necessity. And later in the war, the anti-draft riots in New York (made cinematically famous just a short while ago in *Gangs of New York*) threatened to deprive the Union army of conscripts. Lincoln feared that would lead to a premature end to the war—leaving the United States divided and slavery ongoing. Using the authority granted him by Congress in the Habeas Corpus Act, Lincoln directed the draft boards to ignore writs of habeas corpus issued to them by state courts seeking release of the conscripts. It is not unreasonable to argue that, however *de jure* improper Lincoln's acts were, they were *de facto* a justified necessity that ought, in retrospect, to be praised.

The first lesson here is that we should not be too harsh in our retrospective judgments—hindsight is always 20/20. But as we live within the times and face the challenges of today, we must be at least a little generous in our self-review, for we will not know for many years whether or not our fears of today are well-founded.

---

3. Roy P. Balser et al. eds., The Collected Works of Abraham Lincoln 436-37 (Rutgers Univ. Press 1953-55).
4. 7 Fed. Reg. 1407 (1942).
5. Geoffrey Stone, *Civil Liberties in Wartime*, 28 J.S. Ct. Hist. 215 (2003).
6. *Kennedy v. Mendoza-Martinez*, 372 U.S. 144, 160 (1963). Justice Goldberg was quoting Justice Robert Jackson, who made the same observation in *Terminnelo v. Chicago*, 337 US. 1 (1949) (Jackson, J., dissenting). "The choice is not between order and liberty. It is between liberty with order and anarchy without either. There is danger that, if the court does not temper its doctrinaire logic with a little practical wisdom, it will convert the constitutional Bill of Rights into a suicide pact." *Id.* at 37 (Jackson, J., dissenting).

Indeed, by comparison with past excesses, this history should actually give us some comfort. Many who are concerned with current activities think that we are on a downward spiral toward diminished civil liberties. But a better view of this history shows that the balance between liberty and security is more like a pendulum that gets pushed off-center by significant events (such as those of September 11th) than a spiral. Over time, after Americans have recovered from the understandable human reaction to catastrophe and after the threat recedes, the pendulum returns to center.

We should acknowledge the historical reality that when the wartime crisis passes, the balance swings back in favor of freedom and liberty. And since World War II, our society has matured such that the scope of the swings in the pendulum are not nearly as great as they have been in the past. Whatever one may think of the recent detention of three Americans as enemy combatants, for example, there can be little disagreement that the detention of three Americans (whose detention is based upon some quantum of individualized suspicion), is sufficiently different in degree from the wholesale detention of over 100,000 Japanese-Americans (whose detention was ordered in the complete absence of any individualized suspicion) as to be different in kind. To quote Chief Justice William Rehnquist:

> [T]here is every reason to think that the historic trend against the least justified of the curtailments of civil liberty in wartime will continue in the future. It is neither desirable nor is it remotely likely that civil liberty will occupy as favored a position in wartime as it does in peacetime. But it is both desirable and likely that more careful attention will be paid by the courts to the basis for the government's claims of necessity as a basis for curtailing civil liberty.[7]

What accounts for this seeming change in contemporary context? Though little empirical evidence exists, a rough analysis can identify a number of factors, all of which contribute to greater oversight in the exercise of executive authority, constraining the greatest excesses. These factors would include:

- A more activist Supreme Court that is far more willing to overturn executive branch action, acting as a limit on excessive power. Earlier times of crisis all occurred before the "rights revolution" of the 1960s and the growth of judicial power. Indeed, the current Rehnquist Court has invalidated more acts of Congress than any previous Court, exhibiting a high degree of involvement in curtailing authority.
- A more partisan Congress. Though sometimes seen as a bad thing, the growth of partisanship has created at least one positive benefit: a growth in the "market" for oversight of the executive branch. Since the Watergate era, we have seen an increasing use of congressional investigative authority—sometimes for good, and sometimes for ill. But the prospect of aggressive congressional oversight acts as a check on executive power, as even the prospect of public censure has the *in terrorem* effect of preventing abuse.
- The growth of investigative journalism. Clearly, this is another change that has some potential adverse consequences. But few can deny that post-Watergate, the press has come to more aggressively serve an important public function, exposing activities that some might otherwise prefer to keep secret. None can imagine a return to the days when the press actively participated in concealing FDR's injuries or JFK's dalliances. And that means, equally, that the prospect of secret prosecutions and secret searches and seizures is minimal, at best.
- The rise of the public interest groups. In no other time did Americans organize themselves into public interest groups in the way they do now. No other era saw the existence, for example, of numerous public interest litigation groups like the American Civil Liberties Union. These organizations, through their public information and litigation activities, act as an important check on the exercise of executive authority. They are, in effect, the "canary in the mineshaft," serving as an early warning system of abuse.
- The increase in the public's ability to monitor government. Though technology assuredly offers greater opportunity for our government to monitor our activities, that same technology holds the promise of greater public accountability by enhancing the transparency of government functions.

---

7. William Rehnquist, *All the Laws but One: Civil Liberties in Wartime* 224-25 (1998). Or, as Jeffrey Rosen has written: "[N]one of the legal excesses that followed 9/11 could compare to those that followed World War I." Jeffrey Rosen, *The Naked Crowd* 131 (Random House 2004).

- And, finally, the public seems far more educated about civil liberties today than at any time in the past. With the rise of the Information Age and the Internet, we are far more able to individually gather information necessary to make decisions and to organize a response to government power if one is deemed necessary. From the Ozzie and Harriet quiet of suburbia in the 1950s, we have come to a point where many Americans are vitally concerned about freedom, liberty, and government action and exercise their franchise with those concerns in mind.

As noted, there is little more than anecdotal evidence to support this analysis; yet it has the appeal of both common sense and consistency with contemporary experience. It appears that we have strengthened substantially our ability to examine, oversee, and correct abuses of executive power. The public is in a stronger position today than it ever has been before. And that power of oversight gives us freedom to grant the government great powers when the need arises, secure in the knowledge that we can restrain their exercise appropriately. In short, one lesson from history is that we should not be utterly unwilling to adjust our response to issues of liberty and security in today's crisis of terrorism—for we have the capacity to manage that adjustment and readjust it as necessary.

iii. The Constitutional Structure

- The President and Congress must respect and defend the individual civil liberties guaranteed in the Constitution when they act, but there is also no doubt that they cannot fail to act when the nation faces a serious threat from a foreign enemy.
- As we assess questions of civil liberty, it is important that we do not lose sight of the underlying purpose of government — personal and national security. While that balance is not a zero-sum game, it is vital that we recognize the significant factors on both sides of the scale.
- The courts have recognized that in the national security context, the requirements of the Fourth Amendment apply somewhat differently than they do in the context of domestic law enforcement.

While a large fraction of the debate over new law enforcement and intelligence systems focuses on perceived intrusions on civil liberties, Americans should keep in mind that the Constitution weighs heavily on both sides of the debate over national security and civil liberties. The President and congressional policymakers must respect and defend the individual civil liberties guaranteed in the Constitution when they act, but there is also no doubt that they cannot fail to act when we face a serious threat from a foreign enemy.

The Preamble to the Constitution acknowledges that the United States government was established in part to provide for the common defense. The war powers were granted to Congress and the President with the solemn expectation that they would be used. Congress was also granted the power to "punish … Offenses against the Law of Nations," which include terrorism.[8] In addition, serving as chief executive and commander in chief, the President also has the duty to "take Care that the Laws be faithfully executed," including vigorously enforcing the national security and immigration laws.

Thus, as we assess questions of civil liberty it important that we not lose sight of the underlying end of government: personal and national security. That balance is not a zero-sum game by any means. But it is vital that we not disregard the significant factors weighing on *both* sides of the scales.

Contemporary constitutional limitations have little to add to this equation. Under settled modern Fourth Amendment jurisprudence, law enforcement may secure without a warrant (through a subpoena) an individual's bank records, telephone toll records, and credit card records, to name just three of many sources of data. Other information in government databases (e.g., arrest records, entries to and exits from the country, and driver's licenses) may be accessed directly without even the need for a subpoena.

8. U.S. Const. art. I, § 8.

In 1967, the Supreme Court said that the Fourth Amendment protects only those things in which someone has a "reasonable expectation of privacy" and, concurrently, that anything one exposes to the public (i.e., places in public view or gives to others outside of his own personal domain) is not something in which he has a "reasonable" expectation of privacy—that is, a legally enforceable right to prohibit others from accessing or using what one has exposed.[9] So, for example, federal agents need no warrant, no subpoena, and no court authorization to:

- have a cooperating witness tape a conversation with a third party (because the third party has exposed his words to the public);
- attach a beeper to someone's car to track it (because the car's movements are exposed to the public);
- fly a helicopter over a house to see what can be seen; or
- search someone's garbage.

Thus, an individual's banking activity, credit card purchases, flight itineraries, and charitable donations are information that the government may access because the individual has voluntarily provided it to a third party. According to the Supreme Court, no one has any constitutionally based enforceable expectation of privacy in them. The individual who is the original source of this information cannot complain when another entity gives it to the government. Nor does he have a constitutional right to notice of the inquiry. Some thoughtful scholars have criticized this line of cases, but it has been fairly well settled for decades.

Congress, of course, may augment the protections that the Constitution provides, and it has with respect to certain information. There are privacy laws restricting the dissemination of data held by banks, credit companies, and the like. But in almost all of these laws (the Census being a notable exception), the privacy protections are good only as against other private parties; they yield to criminal, national security, and foreign intelligence investigations.

One important caveat should be made here. In the foregoing discussion we have identified principally the restrictions that apply to domestic law enforcement officials. Important additional restrictions continue to exist on the authority of foreign intelligence agencies to conduct surveillance or examine the conduct of American citizens. Conversely, however, the courts have recognized that in the national security context, the requirements of the Fourth Amendment apply somewhat differently than they do in the context of domestic law enforcement.

iv. Type I and Type II Errors—The Reality of Terrorism

• The suppression of terrorism will not be accomplished solely by military means. Rather, effective law enforcement and/or intelligence gathering activity are the key to avoiding new terrorist acts.

• The traditional law enforcement model is highly protective of civil liberty in preference to physical security thus tolerating more Type II errors (false negatives) than it does Type I errors (false positives). However, September 11th changed this traditional calculus by making Type II errors far more costly and by altering the way Type I errors are considered.

• While our goal should be to minimize both Type I and Type II errors, the growth in danger from Type II errors necessitates lowering our tolerance for Type I errors.

The full extent of the terrorist threat to America cannot be fully known. Consider, as an example, one domestic aspect of that threat—an effort to determine precisely how many al-Qaeda operatives are in the United States at this time and to identify those who may enter in the future.

Terrorism remains a potent threat to international security. The U.S. State Department has a list of over 100,000 names worldwide of suspected terrorists or people with contact to terrorists. Before their camps in

9. *Katz v. U.S.*, 389 U.S. 347 (1967).

Afghanistan were shut down, al-Qaeda trained at least 70,000 people and possibly tens of thousands more. Al-Qaeda–linked Jemaah Islamiyah in Indonesia is estimated to have 3,000 members across Southeast Asia and is still growing larger. Although the estimates of the number of al-Qaeda terrorists in the United States have varied since the initial attack on September 11, 2001, the figure provided by the government in recent, supposedly confidential, briefings to policymakers is 5,000. This 5,000-person estimate may include many who are engaged in fundraising for terrorist organizations and others who were trained in some fashion to engage in jihad, whether or not they are actively engaged in a terrorist cell at this time. But these and other publicly available statistics support two conclusions: (1) no one can say with much certainty how many terrorists are living in the United States; and (2) many who want to enter in the foreseeable future will be able to do so.

Understanding the scope of the problem demonstrates the difficulty of assessing the true extent of the risk to the United States. Consider this revealing statistic from 2002: "[M]ore than 500 million people [are] admitted into the United States [annually], of which 330 million are non-citizens."[10] Of these:

- Tens of millions arrive by plane and pass through immigration control stations, often with little or no examination.
- 11.2 million trucks enter the United States each year. Many more cars do so as well. More than 8.5 million cars cross the Buffalo–Niagara bridges each year alone, and only about 1 percent of them are inspected.
- According to the Department of Commerce, approximately 51 million foreigners vacationed in the United States last year, and this figure is expected to increase to 61 million in three years.
- There are currently approximately 11 million illegal aliens living in the United States. Roughly 5 million entered legally and simply overstayed their lawful visit.
- Over half a million foreign students are enrolled in American colleges, representing roughly 3.9 percent of total enrollment, including:
    1. 8,644 students from Pakistan.
    2. A total of 38,545 students from the Middle East, including 2,216 from Iran, 5,579 from Saudi Arabia, and 2,435 from Lebanon, where Hezbollah and other terrorist organizations train.
    3. About 40,000 additional students from North African, Central and Southeast Asian nations where al-Qaeda and other radical Islamic organizations have a strong presence.

To be sure, not all of these visitors pose a risk, but their sheer volume demonstrates the scope of the potential risk that some within this group do pose.

And, of course, the threat is not exclusively internal. The newest terrorist target may be global shipping. The world is particularly vulnerable to maritime terrorism and maritime piracy is growing increasingly rampant. Lloyd's List has reported that terrorists might be training maritime pilots in the Malacca Straits in order to capture a ship, pilot it into a port or chokepoint, and detonate it.

This illustrates the other part of the story. The danger to America posed by terrorists arises from the new and unique nature of potential acts of war. Virtually every terrorism expert in and out of government believes there is a significant risk of another attack. Unlike during the Cold War, the threat of such an attack is asymmetric. In the Cold War era, U.S. analysts assessed Soviet capabilities, thinking that their limitations bounded the nature of the threat the Soviets posed. Because of the terrorists' skillful use of low-tech capabilities (e.g., box cutters), their capacity for harm is essentially limitless. The United States therefore faces the far more difficult task of discerning their intentions. Where the Soviets created "things" that could be observed, the terrorists create only transactions that can be sifted from the noise of everyday activity only with great difficulty. It is a problem of unprecedented scope, and one whose solution is imperative if American lives are to be saved.

As should be clear from the outline of the scope of the problem, the suppression of terrorism will not be accomplished by military means alone. Rather, effective law enforcement and/or intelligence gathering activity are

10. White House, *Securing America's Borders Fact Sheet, available at* www.whitehouse.gov (last accessed Jan. 14, 2003).

the key to avoiding new terrorist acts. Recent history supports this conclusion. In fact, police have arrested more terrorists than military operations have captured or killed. Police in more than 100 countries have arrested more than 3,000 al-Qaeda–linked suspects, while the military captured some 650 enemy combatants. Equally important, it is policing of a different form—preventative rather than reactive, since there is less value in punishing terrorists after the fact when, in some instances, they are willing to perish in the attack.

The foregoing understanding of the nature of the threat from terrorism helps to explain why the traditional law enforcement paradigm needs to be modified (or, in some instances, discarded) in the context of terrorism investigations. The traditional law enforcement model is highly protective of civil liberty in preference to physical security. All lawyers have heard one or another form of the maxim that "it is better that 10 guilty go free than that one innocent be mistakenly punished."[11] This embodies a fundamentally moral judgment that when it comes to enforcing criminal law, American society, in effect, prefers to have many more Type II errors (false negatives) than it does Type I errors (false positives). That preference arises from two interrelated grounds. One is the historical distrust of government that, as already noted, animates many critics of the Patriot Act. But the other is, at least implicitly, a comparative valuation of the social costs attending the two types of error. We value liberty sufficiently highly that we see a great cost in any Type I error. And though we realize that Type II errors free the guilty to return to the general population, thereby imposing additional social costs on society, we have a common-sense understanding that those costs, while significant, are not so substantial that they threaten large numbers of citizens or core structural aspects of the American polity.

The post–September 11th world changes this calculus in two ways. First, and most obviously, it changes the cost of the Type II errors. Whatever the cost of freeing mob boss John Gotti or sniper John Muhammad might be, they are substantially less than the potentially horrific costs of failing to stop the next al-Qaeda assault. Thus, the theoretical rights-protective construct under which our law enforcement system operates must, of necessity, be modified to meet the new reality. We simply cannot afford a rule that "better 10 terrorists go free than that one innocent be mistakenly punished."

Second, and less obviously, it changes the nature of the Type I errors that must be considered. In the traditional law enforcement paradigm, the liberty interest at stake is personal liberty—that is, freedom from the unjustified application of governmental force. We have as a model the concept of an arrest, the seizure of physical evidence, or the search of a tangible place. As we move into the Information Age, and deploy new technology to assist in tracking terrorists, that model is no longer wholly valid.

Rather, we now add a related, but distinct conception of liberty to the equation—the liberty that comes from anonymity. Anonymity is a different, and possibly weaker, form of liberty. The American understanding of liberty interests necessarily acknowledges that the personal data of those who have not committed any criminal offense can be collected for legitimate governmental purposes. Outside the criminal context, such collection is typically done in the aggregate and under a general promise that uniquely identifying individual information will not be disclosed. Think, for example, of the Census data collected in the aggregate, or of the IRS tax data collected on an individual basis, reported publicly in the aggregate, and only disclosed outside of the IRS with the approval of a federal judge based upon a showing of need.

What these examples demonstrate is not so much that our conception of liberty is based upon absolute privacy expectations, but rather that government impingement on our liberty will occur only with good cause. In the context of a criminal or terrorism investigation, we expect that the spotlight of scrutiny will not turn upon us individually without some very good reason.

This conception of the liberty interest at stake (the interest that will be lost when Type I errors occur) also emphasizes one other point about privacy: In many ways the implementation of new laws and systems to combat terrorism are not an unalloyed diminution of privacy. Rather, the laws and practices can substitute one privacy intrusion (for example, a search of electronic data about an individual) for another privacy intrusion (the physical intrusiveness of body searches at airports). But this means that legal analysts cannot make broad value judgments.

11. E.g., *Furman v. Georgia*, 408 U.S. 238, 367 n.158 (1972) (Marshall, J., concurring). The aphorism has its source in 4 Blackstone, Commentaries, ch. 27, at 358 (Wait & Co. 1907).

Each person weighs the utility of his own privacy by a different metric. For many Americans, the price of a little less electronic privacy might not be too great if it resulted in a little more physical privacy; for others, the opposite result might hold. This suggests little in resolving the tension, save that it cautions against allowing the tension to be resolved by unrepresentative institutions, like the courts, and in favor of allowing more representative institutions, like the legislature, to do their best at evaluating the multi-variable privacy preferences of the population.

Finally, it bears noting that not all solutions necessarily trade off Type I and Type II errors, and certainly not in equal measure. Some novel approaches to combating terrorism might, through technology, actually reduce the incidence of both types of error. More commonly, we will alter both values but the comparative changes will be the important factor. Where many critics of the Patriot Act and other governmental initiatives go wrong is in their absolutism: They refuse to admit of the possibility that we might need to accept an increase in the number of Type I errors. But that simply cannot be right. Liberty is not an absolute value; it depends on security (both personal and national) for its exercise. As Thomas Powers of the University of Minnesota has written: "In a liberal republic, liberty presupposes security; the point of security is liberty."[12] The growth in danger from Type II errors necessitates altering our tolerance for Type I errors. More fundamentally, our goal should be to minimize both sorts of errors.

B. Why We Need the Patriot Act

i. Conclusions of the 9/11 Commission

- Witnesses before the 9/11 Commission have emphasized the importance of the USA Patriot Act and consider it to be an essential weapon in the global war on terrorism.
- Prior to September 11 a wall of legal and regulatory policies prevented effective sharing of information between the intelligence and law enforcement communities.
- The Patriot Act has worked to lower this wall between government agencies and should be reauthorized.

Nothing is more important than preventing another catastrophic terrorist attack on Americans. Nothing. That is why the work of the National Commission on Terrorist Attacks Upon the United States (9/11 Commission)—a comprehensive, objective review of how our law enforcement and intelligence operations can be improved to prevent a recurrence—is so vital. Whenever a team loses the game, it always reviews the videotape to see how it can improve.

During a recent public hearing of the 9/11 Commission, present and former government officials and even the Commissioners themselves emphasized the importance of one new tool adopted after September 11: the USA Patriot Act. They all agreed that the Patriot Act is an essential weapon in the nation's global war on terrorism. Congress should take note and, as President Bush urged in the State of the Union Address, act now to reauthorize provisions in the law due to expire next year.

Generally conducted in a nonpartisan manner—despite controversial testimony by former National Security Council staffer Richard Clarke that triggered a rancorous series of hearings—recent sessions provided an important and appropriate discussion of the underlying challenges of structure and strategy that limited both the Clinton and Bush administrations in effectively going after Osama bin Laden's murderous al-Qaeda network.

One key discussion point, in particular, should not be lost. Officials from *both* administrations acknowledged that before September 11 a "wall" of legal and regulatory policies prevented effective sharing of information between the intelligence and law enforcement communities. For example, as Attorney General John Ashcroft testified before the Commission in 1995, the Justice Department embraced legal reasoning that "effectively excluded"

12. Thomas Powers, *Can We Be Secure and Free?*, The Pub. Int. (Spring 2003).

prosecutors from intelligence investigations. At times, for prudential reasons, Justice Department officials even raised the "wall" *higher* than was required by law, to avoid any appearance of "impermissibly" mixing law enforcement and intelligence activities.

We now know that the erection of this "wall" had tragic costs. The "wall" played a large role in our inability to "connect the dots" of intelligence and law enforcement information before the September 11 attacks. As one frustrated FBI investigator wrote at the time, "Whatever has happened to this—someday someone will die—and wall or not—the public will not understand why we were not more effective and throwing every resource we had at certain 'problems.'"[13]

Largely in response to these problems, Congress passed the USA Patriot Act in the wake of the September 11 attacks. Though often derided by its detractors as a knee-jerk reaction to the September 11 tragedy, the law represented reforms that, as witnesses before the Commission correctly noted, had long been needed to improve U.S. counterterrorism efforts.

The supporters from both sides of the aisle who passed the Act should be gratified that representatives from the Clinton and Bush administrations, including former FBI Director Louis Freeh and Attorney General Janet Reno, reaffirmed the importance of the Patriot Act in improving the government's ability to share information and pursue terrorists.

The legislation has proved its worth in practice. It has facilitated dozens of reported terrorist investigations by removing both real and imagined barriers that kept the people trying to protect us from working together. And to date, as the Department of Justice Inspector General has reported, there has not been a single instance of abuse of the powers granted in the Act.

Safeguarding the civil liberties of American citizens is vitally important, as important during war as during periods of peace. But so too is preserving our security. The Patriot Act preserves both. Hysterical criticisms that the Act was unnecessary and is a threat to a healthy civil society have proved unfounded, and calls for repeal or significant revision are just wrongheaded.

Instead of second-guessing the Patriot Act, Congress should focus on passing legislation to reauthorize the powers granted in the law that are due to sunset in 2005; among these are the very provisions that brought down the "wall" in the first place. As the most recent 9/11 hearings have made clear, transnational terrorist threats will be with us for years to come. In 2006, we will still need the powers of the Patriot Act to protect Americans.

13. John Ashcroft, testimony before the National Commission on Terrorist Attacks Upon the United States, April 13, 2004, transcript at *www.9-11commission.gov/archive/hearing10/9-11Commission_Hearing_2004-04-13.htm* (July 12, 2004); see also James Jay Carafano, Ph.D. and Paul Rosenzweig, "A Patriotic Day: 9/11 Commission Recognizes Importance of the Patriot Act," Heritage Foundation *WebMemo* No. 480, April 15, 2004, at *http://www.heritage.org/Research/HomelandDefense/wm480.cfm*.

ii. Information Sharing

- The Patriot Act adopts as a general principle the rule that any information lawfully gathered during a foreign or domestic counter-intelligence investigation or during a domestic law enforcement investigation should be able to be shared with other federal agencies.
- While there have admittedly been excesses in the past, the right answer is oversight and control, not complete rejection of enhanced government capacity to combat terror.
- Based upon our limited experience thus far, it seems that the advantages gained are substantially greater than the potential dangers posed by changes in the investigative authority granted the executive branch—but Congress will make assessment on a full record when it reconsiders these portions of the Patriot Act next year. In doing so, it would be wise to remember the past, and the problems that it identified as requiring change when it initially adopted the Patriot Act.

The broadest criticism of the Patriot Act is that it was unnecessary—that it has added nothing to the efforts to avoid additional terrorist activities and that it is little more than a compilation of a "wish list" of law enforcement powers. This view, however, lacks persuasive force.

In particular, one aspect of the Patriot Act, embodied in Sections 203 and 218, was absolutely vital. Section 203 permits law enforcement information gathered under the aegis of a grand jury investigation to be shared with intelligence agencies. Section 218 allows the use of intelligence information gathering mechanisms whenever the gathering of intelligence information is a "significant" purpose of the investigation and allows the information gathered to be shared with law enforcement. Taken together, these two sections, in effect, tear down an artificial "wall" that existed between law enforcement and intelligence agencies and permit their cooperation.

Prior to the Patriot Act, a very real wall existed. It was derived from an earlier standard, requiring the use of intelligence gathering mechanisms only when foreign intelligence was the "primary purpose" of the activity. This old "primary purpose" standard derived from a number of court decisions. That standard was formally established in written Department of Justice guidelines in July 1995. While information could be "thrown over the wall" from intelligence officials to prosecutors, the decision to do so always rested with national security personnel—even though law enforcement agents are in a better position to determine what evidence is pertinent to their case. The old legal rules discouraged coordination, and created what the Foreign Intelligence Surveillance Court of Review calls "perverse organizational incentives." [14] The wall had some very negative real-world consequences. Former Department of Justice official Victoria Toensing tells of one: In the 1980s, terrorists hijacked an airplane, TWA Flight 847, which eventually landed in Lebanon. At the time that negotiations were ongoing, the FBI had the capacity (pursuant to a FISA warrant) to intercept the communications between the hijackers on the plane and certain individuals in America. Negotiations did not advance quickly enough, however, and the terrorists killed an American, Robert Stethem, and dumped his body onto the airport tarmac on live TV. The Department of Justice, as a result, announced its intention to capture and prosecute those responsible. This meant that the FBI's ongoing intercepts were no longer for the "primary" purpose of foreign intelligence gathering—the "primary" purpose was now clearly prosecution. And as a result, in the middle of a terrorist crisis, the FBI turned *off* its listening devices for fear of violating the prohibition against using intelligence gathering techniques in a situation where intelligence gathering was not the primary purpose. It is difficult to conceive of a more wrong-headed course of conduct, yet the FBI, rightly, felt that it was legally obliged to act as it did.

Nor is this the only instance in which the artificial "wall" has deterred vital information sharing between law enforcement and intelligence communities. Who can forget the testimony of FBI agent Coleen Rowley, who

14. *Sealed Case*, 310 F.3d at 743.

pointed to these very limitations as part of the reason the FBI was not able to "connect the dots" before September 11th. Instead, the culture against information sharing was so deeply ingrained that during the criminal prosecutions for the 1993 World Trade Center bombing, the Department of Justice actually raised the height of the artificial wall. Imposing requirements that went "beyond what is legally required," the Department instructed its FBI agents to "clearly separate" ongoing counterintelligence investigations from the criminal prosecution.[15] There is even some possibility that this wall may have been the contributing factor to our failure to prevent the attacks of September 11th.

Sections 203, and 218 tear down this wall, and empower federal agencies to share information on terrorist activity. This is an important, significant, positive development. One of the principal criticisms made in virtually every review of our pre-September 11th actions is that we failed to "connect the dots." Indeed, as the congressional review panel noted: "Within the Intelligence Community, agencies did not share relevant counter-terrorism information, prior to September 11th. This breakdown in communications was the result of a number of factors, including differences in agencies' missions, legal authorities and cultures."[16]

In short, the Patriot Act changes adopt as a general principle the rule that *any information lawfully gathered during a foreign or domestic counterintelligence investigation or lawfully gathered during a domestic law enforcement investigation should be capable of being shared with other federal agencies*. The artificial limitations on such information sharing are a relic of a bygone era and, in light of the changed nature of the terrorist threat, are of substantially diminished value today.

We have already had at least one test case demonstrating the potential utility of enhanced information sharing between intelligence and law enforcement organizations: the indictment of Sami Al-Arian for providing material support to several Palestinian terrorist organizations. The case, of course, has yet to be tried and Mr. Al-Arian is by law innocent until proven guilty. Thus, the truth of the government's assertions about him remain unproven and have yet to be tested.

But let us consider a hypothetical case and indulge in the assumption that the allegations are true. Let us imagine that, six months from now, the trial is over. If the allegations made in the indictment are substantiated, what will we have learned? Most pressingly, we will have learned that the charges against Mr. Al-Arian were delayed for at least five years by self-imposed legal obstacles barring the sharing of information between foreign counterintelligence and domestic law enforcement organizations.

The government's case against Mr. Al-Arian is apparently based upon foreign counterintelligence wiretap intercepts that date back as far as 1993. According to the information in those wiretaps, Mr. Al-Arian is charged with having knowingly provided financing to a terrorist organization with the awareness that the funds he provided would be used to commit terrorist acts. And that information has been in the possession of U.S. intelligence organizations for at least the past seven years.

It was not until the passage of the Patriot Act, and the ruling of the Foreign Intelligence Surveillance Court of Review in November 2002, that the intelligence community felt it was lawfully in a position to provide that information to law enforcement officials at the Department of Justice and the FBI. Only those changes enabled the government to bring the charges pending against Mr. Al-Arian.

If this is true, then we have made a wise change in policy. No one—not even Mr. Al-Arian—has publicly argued that the original foreign intelligence scrutiny of Mr. Al-Arian was unlawful or unwarranted. If it really is the case that one branch of our government lawfully had in its possession information about the criminal activity of a foreign national on American soil and that that branch was (or believed it was) obliged by law not to disclose that information to other branches of the government, then that fact alone will make some of the changes wrought by

15. *See* Memorandum from Jamie S. Gorelick, Deputy Attorney General, *Instructions on Separation of Certain Foreign Counterintelligence and Criminal Investigations* (1995).

16. *Report of the Joint Inquiry Into the Terrorist Attacks of September 11, 2001*, House Permanent Select Committee on Intelligence and Senate Select Committee on Intelligence, 107th Cong., 2nd Sess., S. Rep. No. 107–351 and H. Rep. No. 107–792, Dec. 2002, Finding 9, at xvii, *available at* http://www.fas.org/irp/congress/2002_rpt/911rept.pdf; *see also id.* at Finding 1, at xv (concluding that both Intelligence Community and FBI were not well organized to address domestic terrorism threat).

the Patriot Act worthwhile. To the extent that the law removed long-standing statutory barriers to bringing information gathered in national security investigations into federal criminal courts, it is to be welcomed.

Nor can it be convincingly argued that such changes violate the Constitution. To the contrary, as the Court of Review recently made clear, the perverse wall between intelligence and law enforcement was not constitutionally required; removing it, therefore, was constitutionally permissible. As the court said, the change wrought by the Patriot Act "is a reasonable response based on a balance of the legitimate need of the government for foreign intelligence information to protect against national security threats with the protected rights of citizens."[17] This is so because, as the court recognized (and as this paper argues), "ordinary" criminal prosecution is by nature different from that directed at foreign intelligence or terrorism crimes: "The main purpose of ordinary criminal law is twofold: to punish the wrongdoer and to deter other persons in society from embarking on the same course. The government's concern with respect to foreign intelligence crimes, on the other hand, is overwhelmingly to stop or frustrate the immediate criminal activity."[18]

This is not to say that we disregard the past. We cannot and should not ignore unfortunate examples of government excess: for example, the abuses of the FBI's COINTELPRO (counterintelligence program) in the 1960s and 1970s, when investigative authority was used to conduct surveillance of anti-war activists and civil rights groups. Similarly, as the Church Committee investigation disclosed, U.S. intelligence agencies have in several instances acted beyond the bounds of the law. The limitations on activity prior to September 11th grew out of those revelations and were an appropriate, understandable reaction to excess.

But we can no longer afford to hamstring our counterterrorism efforts in that way. The right answer is oversight and control, not complete rejection of enhanced government capacity to combat terrorists. Sections 203 and 218 provide that oversight: No FISA (Foreign Intelligence Surveillance Act) warrant issues without the approval of a neutral federal judge who reviews each application. Though the forum has changed, and the subject matter of the investigation has been expanded, those changes appear sensible in light of the need to maintain the confidentiality of national security information used in securing the requisite authority. It is therefore no surprise that, as adumbrated above, the courts have already made clear "that FISA as amended is constitutional because the surveillances it authorizes are reasonable."

Nor are the courts the only oversight mechanism in place. Portions of Section 203 and all of Section 218 are temporary. The increased information sharing authority granted to the government will "sunset" in December 2005. Thus, the oversight function of Congress is doubly important. It acts as a direct restraint on executive abuse through review. It will also be used to assess the utility of the changes that have occurred. Based upon our limited experience thus far, it seems that the advantages gained are substantially greater than the potential dangers posed by changes in the investigative authority granted the executive branch—but Congress will make assessment on a full record when it reconsiders these portions of the Patriot Act next year. In doing so, it would be wise to remember the past, and the problems that it identified as requiring change when it initially adopted the Patriot Act.

17. Sealed Case, 310 F.3d at 742.
18. *Id.* at 744.

C. Exploding Myths: The Patriot Act Is No Danger

• We cannot decide policy based upon an over-wrought sense of fear. Most of the steps proposed to combat terrorism were previously used to combat organized crime, and there is no evidence of any real abuse. No First Amendment liberties have been curtailed, no dissent or criticism suppressed.

• In reviewing our policies and planning for the future, we must be guided by the realization that this is not a zero-sum game. We can achieve both goals—liberty and security—to an appreciable degree.

• The key is empowering government to do the right things while exercising oversight to prevent the abuse of authority. So long as we keep a vigilant eye on police authority, so long as the federal courts remain open, and so long as the debate about governmental conduct is a vibrant part of the American dialogue, the risk of excessive encroachment on our fundamental liberties can be avoided.

i. Section 206: Roving Wiretaps

Section 206 of the Patriot Act authorized the use of "roving wiretaps"—that is, wiretaps that follow an individual and are not tied to a specific telephone or location—in terrorism investigations. America's original electronic surveillance laws (the Foreign Intelligence Surveillance Act [FISA] of 1978 and Title III of the Omnibus Crime Control Act of 1968) stem from a time when phones were the only means of electronic communications and all phones were connected by hard wires to a single network.

Roving wiretaps have arisen over the past 20 years for use in the investigation of ordinary crimes (e.g., drug transactions or organized crime activities) because modern technologies (cell phones, BlackBerries, and Internet telephony) allow those seeking to evade detection the ability to change communications devices and locations at will.

To begin with, one must understand the general structure of laws governing when law enforcement or intelligence agents may secure authorization to conduct electronic surveillance relating to suspected foreign intelligence or terrorism activity. Title III of the Omnibus Crime Control Act (the statute governing electronic surveillance for domestic crime) allows a court to enter an order authorizing electronic surveillance if "there is probable cause for belief that an individual is committing, has committed or is about to commit" one of a list of several specified crimes.

FISA (the statute governing intelligence and terrorism surveillance) has a parallel requirement: A warrant may issue if there is probable cause to believe that the target of the surveillance is a foreign power or the agent of a foreign power. FISA also requires that the government establish probable cause to believe that "each of the facilities or places at which the surveillance is directed is being used, or is about to be used" by the foreign power or the agent of the foreign power who is the target of surveillance. FISA court warrants thus are issued by federal judges, upon a showing of probable cause, and describe the things to be seized with particularity—the traditional three-prong test for compliance with the warrant clause requirements of the Fourth Amendment.

Thus, no one can argue that these FISA warrants violate the Constitution. To the contrary, as the Foreign Intelligence Surveillance Court of Review recently made clear, the FISA warrant structure is "a reasonable response based on a balance of the legitimate need of the government for foreign intelligence information to protect against national security threats with the protected rights of citizens." This is so because, as the court recognized, there is a difference in the nature of "ordinary" criminal prosecution and that directed at foreign intelligence or terrorism crimes: "The main purpose of ordinary criminal law is twofold: to punish the wrongdoer and to deter other persons in society from embarking on the same course. The government's concern with respect to foreign intelligence crimes, on the other hand, is overwhelmingly to stop or frustrate the immediate criminal activity."

Roving wiretaps (whether used in foreign intelligence or domestic criminal investigations) are, as noted, a response to changing technologies. Phones are no longer fixed in one place and can move across state borders at

the speed of flight. Sophisticated terrorists and criminals can change phones and communications devices constantly in an attempt to thwart interception.

In response to these changes in technology, in 1986 Congress authorized a relaxation of the particularity requirement for the investigation of drug offenses. Under the modified law, the authority to intercept an individual's electronic communication was tied only to the individual who was the suspect of criminal activity (and who was attempting to "thwart" surveillance) rather than to a particular communications device.

Section 206 authorized the same techniques for foreign intelligence investigations. As the Department of Justice has noted: "This provision has enhanced the government's ability to monitor sophisticated international terrorists and intelligence officers, who are trained to thwart surveillance by rapidly changing hotels, cell phones, and internet accounts, just before important meetings or communications."

One important safeguard is that the FISA court may authorize such roving wiretaps only if it makes a finding as to the terrorist's actions—that " the actions of the target of the application may have the effect of thwarting the identification" of a terrorism suspect.

ii. Section 213: Delayed Notification—"Sneak and Peak Warrants"

One section of the Patriot Act that has engendered great criticism is Section 213, which authorizes the issuance of delayed notification search warrants—which critics call "sneak and peek" warrants.

Traditionally, when the courts have issued search warrants authorizing the government's forcible entry into a citizen's home or office, they have required that the searching officers provide contemporaneous notification of the search to the individual whose home or office has been entered. Prior to September 11, some courts permitted limited delays in notification to the owner when immediate notification would hinder the ongoing investigation. Section 213 codifies that common law tradition and extends it to terrorism investigations. Critics see this extension as an unwarranted expansion of authority—but here, too, the fears of abuse seem to outstrip reality.

Delayed notification warrants are a long-existing crime-fighting tool upheld by courts nationwide for decades in organized crime, drug cases, and child pornography. For example, Mafia Don Nicky Scarfo maintained the records of his various criminal activities on a personal computer, protected by a highly sophisticated encryption technology. Law enforcement knew where the information was—and thus had ample probable cause to seize the computer. But the seizure would have been useless without a way of breaking the encryption. So, on a delayed notification warrant, the FBI surreptitiously placed a keystroke logger on Scarfo's computer. The logger recorded Scarfo's password, which the FBI then used to examine all of Scarfo's records of his various drug deals and murders. It would, of course, have been fruitless for the FBI to have secured a warrant to enter Scarfo's home and place a logger on his computer if, at the same time, it had been obliged to notify Scarfo that it had done so.

The courts have approved this common law use of delayed notification. Over 20 years ago, the Supreme Court held that the Fourth Amendment does not require law enforcement to give immediate notice of the execution of a search warrant. The Court emphasized "that covert entries are constitutional in some circumstances, at least if they are made pursuant to a warrant." In fact, the Court stated that an argument to the contrary was "frivolous." In an earlier case—the seminal case defining the scope of privacy in contemporary America—the Court said that "officers need not announce their purpose before conducting an otherwise [duly] authorized search if such an announcement would provoke the escape of the suspect or the destruction of critical evidence."

Section 213 of the Patriot Act thus attempts to codify the common law authority given to law enforcement for decades. As summarized by the Department of Justice: "Because of differences between jurisdictions, the law was a mix of inconsistent standards that varied across the country. This lack of uniformity hindered complex terrorism cases. Section 213 resolved the problem by establishing a uniform statutory standard."

Now, under Section 213, courts can delay notice if there is "reasonable cause" to believe that immediate notification may have a specified adverse result. The "reasonable cause" standard is consistent with pre-Patriot Act case law for delayed notice of warrants. And the law goes further, defining "reasonable cause" for the issuance of a court order narrowly. Courts are, under Section 213, authorized to delay notice only when immediate notification may

result in death or physical harm to an individual, flight from prosecution, evidence tampering, witness intimidation, or other serious jeopardy to an investigation.

In short, Section 213 is really no change at all; it merely clarifies that a single uniform standard applies and that terrorist offenses are included. Nor does Section 213 promise great abuse. Here, as in the past under common law, the officer seeking authority for delayed entry must get authorization for that action from a federal judge or magistrate—under the exact same standards and procedures that apply in getting a warrant to enter a building in the first place. And the law makes clear that in all cases law enforcement must ultimately give notice that property has been searched or seized. The only difference from a traditional search warrant is the temporary delay in providing notification. Here, the presence of oversight rules seems strong—certainly strong enough to prevent the abuse that some critics fear.

Nor can it be doubted that the delayed notification standards have performed a useful function and are a critical aspect of the strategy of prevention—detecting and incapacitating terrorists before they are able to strike.

One example of the use of delayed notification involves the indictment of Dr. Rafil Dhafir. A delayed notification warrant allowed the surreptitious search of an airmail envelope containing records of overseas bank accounts used to ship over $4 million to Iraq. Because Dhafir did not know of the search, he was unable to flee and he did not move the funds before they were seized. In another instance, the Justice Department described a hypothetical situation (based upon an actual case) in which the FBI secured access to the hard drive of terrorists who had sent their computer for repair. In still another, they were able to plant a surveillance device in a building used by terrorists as a safe house.

iii. Section 215: Libraries

Perhaps no provision of the Patriot Act has excited greater controversy than has Section 215, the so-called angry librarians provision. The section allows the Foreign Intelligence Surveillance Court in a foreign intelligence investigation to issue an order directing the recipient to produce tangible things.

The revised statutory authority in Section 215 is not wholly new. FISA has had authority for securing some forms of business records since its inception. The new statute modifies FISA's original business-records authority in a two important respects:

First, it "expands the types of entities that can be compelled to disclose information. Under the old provision, the FISA court could order the production of records only from 'a common carrier, public accommodation facility, physical storage facility or vehicle rental facility.' The new provision contains no such restrictions."

Second, the new law "expanded the types of items that can be requested. Under the old authority, the FBI could only seek 'records.' Now, the FBI can seek 'any tangible things (including books, records, papers, documents, and other items).'"[19]

Thus, the modifications made by Section 215 do not explicitly authorize the production of library records; but by its terms, it authorizes orders to require the production of virtually any business record. That might include library records, though it would include as well airline manifests, international banking transaction records, and purchase records of all sorts.

Section 215 mirrors, in the intelligence-gathering context, the scope of authority that already exists in traditional law enforcement investigations. Obtaining business records is a long-standing law enforcement tactic. Ordinary grand juries for years have issued subpoenas to all manner of businesses, including libraries and bookstores, for records relevant to criminal inquiries.

For example, in the 1997 Gianni Versace murder case, a Florida grand jury subpoenaed records from public libraries in Miami Beach. Likewise, in the 1990 Zodiac gunman investigation, a New York grand jury subpoenaed records from a public library in Manhattan. Investigators believed that the gunman was inspired by a Scottish occult poet, and wanted to learn who had checked out books by that poet. In the Unabomber investigation, law

19. Department of Justice, *The USA Patriot Act: Myth vs. Reality* 16 (2003).

enforcement officials sought the records of various libraries, hoping to identify the Unabomber as a former student with particular reading interests.

Section 215 merely authorizes the FISA court to issue similar orders in national security investigations. It contains a number of safeguards that protect civil liberties.

- First, Section 215 requires FBI agents to get a court order. Agents cannot compel any entity to turn over its records unless judicial authority has been obtained. FISA orders are unlike grand jury subpoenas, which are requested without court supervision and are subject to challenge only after they have been issued.
- Second, Section 215 has a narrow scope. It can be used only (1) "to obtain foreign intelligence information not concerning a United States person" or (2) "to protect against international terrorism or clandestine intelligence activities." It cannot be used to investigate ordinary crimes, or even domestic terrorism. Nor can it be used in any investigation premised solely on "activities protected by the first amendment to the Constitution."

This is narrower than the scope of traditional law enforcement investigations. Under general criminal law, the grand jury may seek the production of any relevant business records. The only limitation is that the subpoena may be quashed if the subpoena recipient can demonstrate that "there is no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury's investigation." There is no necessity of showing a connection to foreign intelligence activity nor any limitation against investigation of United States persons. Thus, unlike under Section 215, the grand jury may inquire into potential violations of any federal crime with effectively limitless authority.

Opponents make two particular criticisms of this provision: that the judicial review it provides for is a chimera, and that the provision of Section 215 imposing secrecy on the recipients of subpoenas issued pursuant to the section imposes a "gag rule" that prevents oversight of the use of the section's authority. Neither criticism, however, withstands close scrutiny.

Section 215 provides for judicial review of the application for a subpoena for business records. The language provides, however, that upon application, the court "shall" issue the requested subpoena. From the use of the word "shall," critics infer that the obligation to issue the requested subpoena is mandatory and, thus, that the issuing court has no discretion to reject an application. Of course, if this were true (which, as discussed below, it is not), then the absence of any judicial ability to reject an application would reduce the extent of judicial oversight.

But critics who make this argument (even if it were the case) miss the second-order effects of judicial review. It imposes obligations of veracity on those seeking the subpoenas, and to premise an objection on the lack of judicial review is to presuppose the mendacity of the subpoena affiants. It is also to presuppose the absence of any internal, administrative mechanisms in order to check potential misuse of the subpoena authority. And, most notably, it presupposes that the obligation to swear an oath of truthfulness, with attendant perjury penalties for falsity, has no deterrent effect on the misuse of authorities granted.

But even more significantly, this criticism misreads the statute, which, while saying that the subpoena "shall" issue, also says that it shall issue as sought or "as modified." The reviewing judge thus explicitly has authority to alter the scope and nature of the documents being sought—a power that cannot be exercised in the absence of substantive review of the subpoena request. Thus, the suggestion that the provisions of Section 215 preclude judicial review is simply mistaken. To the contrary, Section 215 authorizes judicial review and modification of the subpoena request which occurs before the subpoena is issued. This is a substantial improvement over the situation in traditional grand jury investigations where the subpoena is issued without judicial intervention and the review comes, at the end, only if the subpoena is challenged.

Nor is judicial oversight the only mechanism by which the use of Section 215 authority is monitored. The section expressly commands that the Attorney General "fully inform" Congress of how the section is being implemented. On October 17, 2002, the House Judiciary Committee, after reviewing the Attorney General's first report, indicated that it was satisfied with the Justice Department's use of Section 215: "The Committee's review of classified

information related to FISA orders for tangible records, such as library records, has not given rise to any concern that the authority is being misused or abused." If it were—if, for example, the Department were conducting investigations based upon the reading habits of suspects, in violation of the First Amendment—we can be sure that Congress would have said so. That it has not demonstrates that, once again, critics' fears far outpace reality.

The second criticism—that Section 215 imposes an unwarranted gag rule—is equally unpersuasive. Section 215 does prohibit recipients of subpoenas from disclosing that fact—a precaution that is necessary to avoid prematurely disclosing to the subjects of a terrorism investigation that they are subject to government scrutiny. That prohibition might be independently justified, given the grave nature of the potential threats being averted.

But it need not be—for, again, the secrecy provisions of Section 215 merely extend existing rules in traditional law enforcement grand juries to the more sensitive intelligence arena. In the grand jury context, it is common for custodians of third-party records to be prohibited from disclosing the existence of the document request. Banks, for example, may be obliged to conceal requests made to them. And it is clear, beyond peradventure, that these grand jury secrecy obligations are constitutional. For example, when the nanny of JonBenet Ramsey was called to testify before a state grand jury, state law prohibited her from disclosing the substance of her testimony. When she challenged that law (on the ground that it infringed her freedom of speech), her challenge was rejected by the courts.

iv. Section 803: Material Support

The "material support" provisions of the Patriot Act are of mixed use. A beginning premise is that, in this context (unlike most other aspects of the Patriot Act) the executive response to terror has directly raised the specter of a potential threat to core First Amendment advocacy—opposition, for example, to the Administration's policy regarding Iraq, or globalization of the economy. Unlike other aspects of the Patriot Act (for example, the much-derided but absolutely necessary delayed notification provisions of Section 213) where the costs of Type II errors are high and the relative costs of Type I errors minimal, in the context of investigating organizations that are both potential terrorist groups and potential political organizations the possible costs of a Type I error are higher. The fundamental right to openly criticize the government is a broad public right, held by all in common. As such, we should be especially careful before allowing new policies to trench upon that right.

The Patriot Act might be seen to impinge on First Amendment freedoms in its prohibition against providing material support to terrorist organizations. Some organizations have humanitarian aspects to their work and say that their humanitarian efforts are distinct from the allegedly terrorist acts of related organizations. They thus argue that it impinges on First Amendment freedoms of speech and association for supporters to be criminally prosecuted when all they are doing is providing material support to the humanitarian aspects of the organization. The executive responds, not unreasonably, that money is fungible and that contributions to the humanitarian aspects of the organization are readily "passed through" to the terrorist arms of related organizations. We thus face the difficult conundrum of distinguishing between conduct aimed to support legitimate political and humanitarian groups and conduct that is a mere subterfuge for supporting terrorist organizations.

It must first be acknowledged that much of the ambiguity in the statute pre-dates the Patriot Act itself. It was an earlier statute, the Anti-Terrorism and Effective Death Penalty Act of 1996 (AEDPA), that gave the Secretary of the Treasury the authority to designate terrorist organizations, and made it a crime to provide material support to organizations so designated. The Patriot Act, in Section 810 enhanced the criminal penalties and also, in Section 805, expanded the scope of the statute—making clear that it applied to those who provided expert assistance to terrorist organizations and applied to acts outside the United States. Section 805 also expanded the list of terrorism crimes for which it is illegal to provide material support and clarified that material support includes all types of monetary instruments. But the core concept—that providing support to terrorist organizations is wrong—predates September 11.

It must also be understood that Congress was cognizant of the First Amendment concerns of trenching on protected political advocacy when it enacted AEDPA, yet chose to act anyway—largely because of the felt necessity: "Several terrorist groups have established footholds within ethnic or resident alien communities in the United States," and "[m]any of these organizations operate under the cloak of a humanitarian or charitable exercise . . . and thus operate largely without fear of recrimination." Thus, Congress determined that the prohibition on material

support was the only option available: "There is no other mechanism, other than an outright prohibition on contributions, to effectively prevent such organizations from using funds raised in the United States to further their terrorist activities abroad." As a consequence, Congress saw a prohibition on material support for terrorist organizations as "absolutely necessary to achieve the government's compelling interest in protecting the nation's safety from the very real and growing terrorist threat."[20]

Lest it be accused of excess, before passing AEDPA Congress also examined various constitutional issues raised by a ban on material support. The House of Representatives report acknowledged that "[t]he First Amendment protects one's right to associate with groups that are involved in both legal and illegal activities." That report emphasized that the contemplated ban on material support "does not attempt to restrict a person's right to join an organization. Rather, the restriction only affects one's contribution of financial or material resources to a foreign organization that has been designated as a threat to the national security of the United States." [21] In short, even before September 11, Congress attempted to carefully construct a balanced and nuanced approach that both recognized the liberty interests at stake *and* understood the necessity of enhanced investigative authority.

Vagueness. Some, nonetheless, challenge the application of these provisions; they think Congress got the balance wrong. Their principal avenue of challenge is to say that these provisions are vague—a contention with which this paper disagrees. Nonetheless, at least one appellate court has held that the terms "personnel" and "training" as used in the material support provisions of AEDPA are impermissibly vague. A district court likewise has held that the phrase "expert advice"—added to the law by the Patriot Act—is impermissibly vague.

Unlike the conclusions regarding the intent of the Patriot Act (which will be addressed below), these decisions (which purport to find vagueness in words of common usage) are highly suspect. More significantly, because the construction given to the *scienter* requirement sufficiently limits potential abuse, the vagueness challenges to Section 2339 of AEDPA are unnecessary.

Fair Notice and Language. As a basic principle of due process, criminal prohibitions must give a person of ordinary intelligence "fair warning" of criminality. The law does not need to define an offense with mathematical certainty, but must provide "relatively clear guidelines as to prohibited conduct."[22] This doctrine recognizes that some exercise of prosecutorial discretion in choosing cases is inevitable. All that the Constitution requires is that Congress, through the text of the statutes, "establish minimal guidelines to govern law enforcement."[23] To prove that a statute is unconstitutionally vague on its face, a defendant must "at least demonstrate[] implication of 'a substantial amount of constitutionally protected conduct.'"[24] Most important, if a class of offenses can be made constitutionally definite by a reasonable construction of the statute, the courts are under a "duty to give the statute that construction."[25] The Ninth Circuit panel seems to have failed to exercise that "duty,"—one that could readily have been accomplished by consulting dictionary definitions of the words chosen by Congress.

The terms chosen by Congress—"personnel," "training," and "expert advice"—are sufficiently clear in their meaning to provide fair warning to a person of reasonable intelligence as to the potential that his or her conduct falls within the statutory prohibition. The term "personnel," for example, generally describes employees or others working affiliated with a particular organization and working under that organization's direction or control. The Oxford English Dictionary defines it as: "The body of persons engaged in any service or employment, esp. in a public institution, as an army, navy, hospital, etc.; the human as distinct from the *material* or material equipment (*of* an institution, undertaking, etc.)"[26] Thus, "personnel" has a discernible and specific meaning, familiar to members of the working world who act in organizations.

---

20. *See* H.R. Rep. No. 104-383, at 43-45 (1995).
21. *See id.* at 45 ("The ban does not restrict an organization's or an individual's ability to freely express a particular ideology or political philosophy. Those inside the United States will continue to be free to advocate, think, and profess the attitudes and philosophies of the foreign organizations. They are simply not allowed to send material support or resources to those groups, or their subsidiary groups, overseas.").
22. *Posters N' Things, Ltd. v. United States*, 511 U.S. 513, 525 (1994).
23. *Kolender v. Lawson*, 461 U.S. 352, 358 (1983).
24. *Schwartzmiller v. Gardner*, 752 F.2d 1341, 1348 (9th Cir. 1984).
25. *United States v. Harriss*, 347 U.S. 612, 618 (1954).

The word "personnel" is also used in numerous other places in the criminal code. For example, the code refers to: "United States personnel" assigned to a foreign mission or entities (18 U.S.C. 7(9)(B)); "ground personnel" preparing an aircraft for flight (18 U.S.C. 31(5)(A)); "senior personnel" of executive branch and independent agencies (18 U.S.C. 207(c)); civilian law enforcement "personnel," and "personnel" of the Department of Defense (18 U.S.C. 831(d) & (e)(2)(B)(ii)); and "personnel" of the Armed Forces (18 U.S.C. 2277(b)). If the term "personnel" is vague in as employed in AEDPA, then it is equally vague in these other contexts—yet no one would seriously offer that argument.

Similarly, the ban against providing "training" to designated foreign terrorist organizations is not unconstitutionally vague. The verb "train" is commonly understood to mean: "To subject to discipline and instruction for the purpose of forming the character and developing the powers of, or of making proficient in some occupation." More particularly, to train is "[t]o instruct and discipline in or for some particular art, profession, occupation or practice; to make proficient by such instruction and practice."[27] It boggles the mind to suggest that Congress cannot proscribe teaching foreign terrorists how to become better terrorists; yet if the logic of the vagueness argument is followed, that would be the result. The statutory ban rightly can be read to preclude the training of foreign terrorists on how to use weapons, build bombs, evade surveillance, or launder funds—and that's a good thing.

And, finally, "expert assistance" is not in any way vague. It is a common concept in the law. For example, Rule 702 of the Federal Rules of Evidence defines "expert" testimony to be based on "scientific, technical, or other specialized knowledge." The Oxford English Dictionary offers a similar definition: "One whose special knowledge or skill causes him to be regarded as an authority; a specialist."[28] In turn, "advice" is an equally familiar term, meaning: "Opinion given or offered as to action; counsel." [29]

Indeed, with respect to all of these terms, one might reasonably ask opponents of the provision what language they would suggest to clarify the alleged vagueness. They can offer none, because, at bottom, their argument is the solipsistic one of Sartre.

Standing and Overbreadth. Nevertheless, the Ninth Circuit held that two of these phrases—"training" and "personnel"—were vague, and a district court has determined that "expert assistance" is vague as well. Looking closely at the reasoning of these two courts demonstrates how badly astray they have gone in their analysis.

The Ninth Circuit offered two examples of training that might raise First Amendment concerns: instructing a designated terrorist organization on how to petition the United Nations, and teaching conflict resolution to such an organization. In some instances, the district court was concerned that similar actions could be construed as the provision of "expert assistance." But the possibility of such applications does not mean the statutes are vague and does not justify invalidating the provisions in their entirety on a facial challenge.

Indeed, settled law is to the contrary. An individual who asserts that a statute is vague must establish its vagueness as to his own conduct. The hypothetical "expert political advocate" who might be caught in the alleged vagueness of the words "training" and "expert assistance" is not a ground for facially invalidating the statute. Rather, the proper course is an applied challenge to the law on vagueness grounds as cases and circumstances warrant. For this reason, as the Supreme Court has said, where an individual had fair notice from the language of the statute that his own conduct is prohibited, he has no standing to assert that the statute was vague, as it might hypothetically be applied to others.

What is really at issue here is not vagueness. The real question is one of alleged overbreadth. In other words, the language of the statute is clear. But it is also clear that an ill-minded government could seek to apply these clear words to protected First Amendment conduct. Thus, the concern is a potentially overbroad application of the law—beyond the core areas of concern that everyone concedes are constitutionally proscribable to areas of expres-

---

26. See *Oxford English Dictionary* (1999 ed.) (CD-ROM Ver. 2.0) (emphasis in original) [hereinafter OED (1999 ed.)]; see also *Webster's Third New International Dictionary* (defining "personnel" as "a body of persons employed in some active service (as the army or navy, a factory, office, airplane)").
27. See *OED* (1999 ed.).
28. See *OED* (1999 ed.).
29. See *OED* (1999 ed.); see also Random House Dictionary 29 (2d ed. 1987) (" an opinion or recommendation offered as a guide to action, conduct, etc.").

sive conduct where the government should not tread. The Ninth Circuit, by ignoring the correct issue, missed the right analysis.

But even if it had asked the right question, the result—voiding the statute—would (as the district court recognized) be wrong. As the Supreme Court said just this past year, "there comes a point at which the chilling effect of an overbroad law, significant though it may be, cannot justify prohibiting all enforcement of that law—particularly a law that reflects 'legitimate state interests in maintaining comprehensive controls over harmful, constitutionally unprotected conduct.'"[30] The Court went on to explain:

> [T]here are substantial social costs *created* by the overbreadth doctrine when it blocks application of a law to constitutionally unprotected speech, or especially to constitutionally unprotected conduct. To ensure that these costs do not swallow the social benefits of declaring a law "overbroad," we have insisted that a law's application to protected speech be "substantial," not only in an absolute sense, but also relative to the scope of the law's plainly legitimate applications, . . . before applying the "strong medicine" of overbreadth invalidation.[31]

Thus, "[t]he overbreadth claimant bears the burden of demonstrating, 'from the text of [the law] and from actual fact,' that substantial overbreadth exists."[32]

And this, at the core, demonstrates why the overbreadth challenge should fail. As already discussed, the text of the law does not suffer from unreasonable scope. And, as noted at the outset, there are no "actual facts" of abuse that have been reported—no public advocates criminalized for their political speech. And the social costs of declaring these laws overbroad is potentially catastrophic. The United States has a "legitimate state interest" in controlling the "constitutionally unprotected conduct" of providing material support for terrorism (teaching a terrorist how to build a bomb is not protected free speech). Courts that rule otherwise fail to recognize that the paradigm of pure law enforcement can no longer be applied. The cost of the Type II errors is simply too great. And thus, as the Supreme Court said in a far more benign context in *Hicks*, the social costs of striking the entire law as overly broad counsel strongly against that result.

Nor is this view mere speculation. Already, these laws (AEDPA, as codified in 18 U.S.C. § 2339, and Section 805 of the Patriot Act) have been used in a number of cases to prosecute potential terrorist activities. For example, John Walker Lindh was charged with providing "personnel" to al-Qaeda based on acts of attending its terrorist training camp, swearing allegiance in *jihad*, and volunteering for military service in its forces. These charges were then upheld against vagueness and overbreadth attacks. A half-dozen other cases can also be identified. To accept the reasoning of the courts on vagueness or overbreadth grounds is to despair of any real ability to address this conduct—and that is, regretfully, a result we simply cannot afford.

It is also a result that is unnecessary. Rather than distorting the doctrines of vagueness and overbreadth to protect hypothetical innocent First Amendment actors, a far more direct and appropriate method (already adopted by the Ninth Circuit) exists to limit the potential for abuse: construing the *scienter* requirements in a manner that protects innocent actors.

Material Support and Scienter. The Ninth Circuit has interpreted the intent requirements of Section 2339B. Here, the Ninth Circuit got it more or less right.

What must the government prove the supporter knew in order to show the supporter in violation of the criminal prohibition? The statute says that "Whoever . . . knowingly provides material support to a foreign terrorist organization" is guilty of a crime.[33] Does it suffice to show that the supporter purposefully did the act which constitutes the offense—i.e., that he provided material support by donating money to the organization—or must government also show that the supporter knew of the organization's designation as a terrorist organization or of the unlawful activities that caused it to be so designated.

---

30. *Virginia v. Hicks*, 123 S. Ct. 2191, 2197 (2003).
31. *Id.* (citations omitted; emphasis in original).
32. *Id.* at 2198.
33. 18 U.S.C. § 2339B.

Here, the government's position—that it need not prove knowledge of the designation—goes too far and risks trenching on First Amendment freedoms of speech and association. The requirement that a crime involve culpable purposeful intent has a solid historical grounding. As Justice Robert Jackson wrote:

> The contention that an injury can amount to a crime only when inflicted by intention is no provincial or transient notion. It is as universal and persistent in mature systems of law as belief in freedom of the human will and a consequent ability and duty of the normal individual to choose between good and evil. A relation between some mental element and punishment for a harmful act is almost as instinctive as the child's familiar exculpatory "But I didn't mean to," and has afforded the rational basis for a tardy and unfinished substitution of deterrence and reformation in place of retaliation and vengeance as the motivation for public prosecution. Unqualified acceptance of this doctrine by English common law was indicated by Blackstone's sweeping statement that to constitute any crime there must first be a "vicious will."[34]

Though the text of Section 2339B requires that the supporters have acted "knowingly"—a seeming protection from the imposition of unwarranted liability—if interpreted as the government suggests, that requirement would be but a parchment barrier to what is, in effect, the imposition of absolute liability. The government's interpretation would presume that all supporters are charged with knowing all of the intricate regulatory arcana that govern the designation by the Treasury Secretary of terrorist organizations—a presumption that generally applies (and perhaps misapplies) in the context of a closely regulated industry. As a consequence, under the government's interpretation, the only requirement imposed by requiring proof that one has acted "knowingly" is that the government must demonstrate that the defendant has purposefully done the act constituting the offense—and in the context of a charitable donation that showing is trivial. Nobody donates money (or provides advice) by mistake or accident. As Justice Potter Stewart noted: "As a practical matter, therefore, they [would be] under a species of absolute liability for violation of the regulations despite the 'knowingly' requirement."[35]

What is particularly disturbing about the government's argument is that it works in tandem with the statutory amendment authorizing significantly harsher penalties. Historically, when the courts first considered laws containing reduced intent requirements, the laws almost uniformly provided for very light penalties such as a fine or a short jail term, not imprisonment in a penitentiary. As commentators noted, modest penalties are a logical complement to crimes that do not require specific intent. Indeed, some courts questioned whether any imprisonment at all could be imposed in the absence of intent and culpability. This historical view has, of course, been lost: Laws with reduced *mens rea* requirements are often now felonies. And even misdemeanor offenses can, through the stacking of sentences, result in substantial terms of incarceration.

But this should not be the uniform case—especially where, as here, much innocent conduct, otherwise protected by the First Amendment, would be swept up in the broader definition. We should not lose sight of a fundamental truth: "If we use prison to achieve social goals regardless of the moral innocence of those we incarcerate, then imprisonment loses its moral opprobrium and our criminal law becomes morally arbitrary."[36] Or as the drafters of the Model Penal Code said:

> It has been argued, and the argument undoubtedly will be repeated, that strict liability is necessary for enforcement in a number of the areas where it obtains. But if practical enforcement precludes litigation of the culpability of alleged deviation from legal requirements, the enforcers cannot rightly demand the use of penal sanctions for the purpose. Crime does and should mean condemnation, and no court should have to pass that judgment unless it can declare that the defendant's act was culpable. This is too fundamental to be compromised.[37]

The broad statutory language, which does not make clear what intent must be proven has, fortunately, begun to be interpreted by the courts in a restrictive manner. That welcome development demonstrates that we can grant

34. *Morisette*, 342 U.S. at 250-51.
35. *International Minerals & Chemical Corp.*, 402 U.S. at 569 (Stewart, J., dissenting).
36. *United States v. Weitzenhoff,* 35 F.3d 1275, 1293 (9th Cir. 1993) (Kleinfeld, J., dissenting from denial of rehearing *en banc*).
37. American Law Institute, Model Penal Code § 2.05 and Comments at 282–83 (1985).

the government additional powers to combat terrorism while reasonably anticipating that the checking mechanisms in place will restrain to excessive a use of those powers.

And, lest one think that from this discussion that the authors have fallen into the trap of exalting liberty over security, two important points should be added:

First, we should have every confidence that by and large executive branch authorities are already screening cases for these very criteria. There is little (indeed no) reason to suspect that officials are using Section 805 as a means of condemning wholly innocent behavior. Thus, the imposition of a *scienter* requirement, while perhaps allowing some guilty to escape at the margins, will have little effect in the run-of-the-mine cases. In short, it substantially lowers the risks of Type II errors while not appreciably enhancing the probability of Type I errors.

Second, and equally important, the addition of a *scienter* requirement will not eliminate the ability of the government to rely on other standard doctrines of criminal law, such as willful blindness, with which faux claims of innocence may be rebutted. Defendants will not be able to avoid penalties by maintaining a willful blindness to the true nature of the organization. Our collective American experience is that juries are quite good at sorting the sham claims of innocence from the legitimate ones.

Lessons Learned. Finally, stepping back for a moment, what we can learn from the foregoing analysis and our experience with the court's construction of Section 2339B. Frankly, there is cause for optimism.

Some portions of the Ninth Circuit's opinion can be disagreed with profoundly, while other portions are commendable. But what is most commendable of all is that the judicial review function is working. And review—both by the Courts, and by this Congress—is essential, for oversight in its varying forms enables us to limit the executive exercise of authority. Paradoxically, however, it also allows us to empower the executive; if we enhance transparency appropriately, we can also comfortably expand governmental authority, confident that our review of the use of that authority can prevent abuse. While accommodating the necessity of granting greater authority to the executive branch, we must also demand that the executive accept greater review of its activities.

It was more than 10 years into the Cold War before the legal and structural systems that would sustain us through the 50-year struggle were put in place. We cannot, and should not, expect that at the start of this long struggle we will get it right the first time.

As Michael Chertoff the former Assistant Attorney General for the Criminal Division has written:

> The balance [between liberty and the response to terror] was struck in the first flush of emergency. If history shows anything, however, it shows that we must be prepared to review and if necessary recalibrate that balance. We should get about doing so, in light of the experience of our forbearers and the experience of our own time.[38]

Others have echoed that call.

Right now, the judicial debate will continue. If the views of the Ninth Circuit prevail, then Congress will be well positioned to fix the problem with additional language. If they do not prevail, then the courts and Congress will nonetheless remain ready to police the boundaries of executive authority and ensure against abuse.

And that is exactly as it should be. John Locke, the seventeenth-century philosopher who greatly influenced the Founding Fathers, was equally right when he wrote: "In all states of created beings, capable of laws, where there is no law there is no freedom. For liberty is to be free from the restraint and violence from others; which cannot be where there is no law; and is not, as we are told, a liberty for every man to do what he lists."[39] Thus, the obligation of the government is a dual one: to protect civil safety and security against violence *and* to preserve civil liberty.

38. Michael Chertoff, "Law, Loyalty, and Terror," *The Weekly Standard* 15, 17 (Dec. 1, 2003).
39. John Locke, *Two Treatises of Government*, ed. Peter Laslett (Cambridge: Cambridge University Press, 1988), 305.

IV. Civil Rights Violations: Fiction and Reality

- Criticism of the Patriot Act misapprehends important distinctions: Criticism often blurs potential and actuality.
- Much of the belief in the potential for abuse stems from a misunderstanding of the true nature of the new powers that government has deployed to combat terrorist threats.

The key is empowering government to do the right things while exercising oversight to prevent the abuse of authority. So long as we keep a vigilant eye on police authority, so long as the federal courts remain open, and so long as the debate about governmental conduct is a vibrant part of the American dialogue, the risk of excessive encroachment on our fundamental liberties can be avoided.

A governing rule for assessing our response to terror can be readily summarized from the writings of Chief Justice Rehnquist. 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."[1]

Everyone does not share Chief Justice Rehnquist's vision of the balance between liberty and order. Recent months have seen the growth of a new movement—call it the "anti-anti-terrorism" movement, if you will. The thesis of the movement, which has some of the appearances of a political campaign, is that steps being taken domestically to combat the potential for terrorist attacks are too intrusive and a threat to cherished civil liberties.

The principal focus of the campaign is the USA Patriot Act. Taking many forms, the campaign argues that provisions of the Patriot Act, and related laws and practices, have greatly infringed upon American liberties while failing to deal effectively with the threat of terrorism. Criticism of the anti-terrorist campaign is not, however, limited to the Patriot Act—many other aspects of the Bush Administration's domestic response to terrorism have come under fire. To some degree, the Patriot Act as conceived by the public is broader than its actual provisions. Its very name has come to serve as a symbol for all of the domestic anti-terrorist law enforcement actions. It has become, if you will, a convenient shorthand formulation for all questions about the alteration in the balance between civil liberty and national security that have occurred since September 11.

There are two overarching themes that animate criticism of the Patriot Act (using the phrase now in the broad, symbolic sense already noted): First, critics of the Patriot Act frequently decry the expansion of executive authority in its own right. They equate the potential for abuse of executive branch authority with the existence of actual abuse. They argue, either implicitly or explicitly, that the growth in executive power is a threat, whether or not the power has, in fact, been misused in the days since the anti-terrorism campaign began. In essence, these critics come from a long tradition of limited government that fears any expansion of executive authority, notwithstanding the potential for benign and beneficial results, because they judge the potential for the abuse of power to outweigh the benefits gained.

The second theme of many criticisms of the Patriot Act and other government responses is one we might call a fear of technology. In service of our efforts to combat terrorism the government has begun to explore ways of taking advantage of America's superior capacity to manage data through new information technologies. The Transportation Security Administration's proposal for a new computer-assisted passenger-screening program (CAPPS II—now known as Secure Flight) is one such program.

These new technologies offer two advantages over current investigative practices: They have the potential to both expand the ambit of the information available to federal law enforcement and intelligence agencies and enhance

1. *See* note 7, *supra*.

the efficiency with which those agencies are able to examine and correlate information already in their possession. And both possibilities raise corresponding fears among critics of the programs. Expanded access to information increases executive power. And with greater efficiency comes more effective use of power. Thus, the hesitancy to use new technology, though sometimes born of technological apprehension, also resonates with the principal theme of critics: a reluctance to expand the capacity of the government to examine the lives of individuals.

Criticism of the Patriot Act, however, sometimes misapprehends important distinctions: Much of the belief in the potential for abuse stems from a misunderstanding to the true nature of the new powers that government has deployed to combat those threats. To a surprising degree, opposition to the executive response to terror is premised on a mistaken, and sometimes overly apocalyptic, depiction of the powers that have accrued to the government.

More fundamentally, those who fear the expansion of executive power in the war on terrorism offer a mistaken solution: prohibition. While we could afford that solution in the face of traditional criminal conduct, we cannot afford that answer in combating the threat of terror. In the context of current circumstances, vigilance and oversight, enforced through legal, organizational and technical means, are the answer to potential abuse—not prohibition. We must keep a watchful eye to control for the risk of excessive encroachment; and if we do so, the likelihood of erosion of civil liberties can be substantially reduced.

Thus far, we have succeeded in meeting that goal. With respect to the Patriot Act (now using those words in the narrower and technical sense of a particular law), the record is, in fact, one of success. The Inspector General for the Department of Justice has reported that there have been no instances in which the Patriot Act has been invoked to infringe on civil rights or civil liberties. This is consistent with the conclusions of others. For example, at a Senate Judiciary Committee Hearing on the Patriot Act Senator Joseph Biden (D-DE) said, "some measure of the criticism [of the Patriot Act] is both misinformed and overblown." His colleague, Senator Dianne Feinstein (D-CA) said: "I have never had a single abuse of the Patriot Act reported to me. My staff . . . asked [the ACLU] for instances of actual abuses. They . . . said they had none." Even the lone Senator to vote against the Patriot Act, Russ Feingold (D-WI), said that he "supported 90 percent of the Patriot Act" and that there is "too much confusion and misinformation" about the Act. These views—from Senators outside the Administration and an internal watchdog—are at odds with the fears often expressed by the public.

The Report of the Inspector General is particularly instructive in this regard. According to the IG, the Patriot Act identifies certain specific groups that would be vulnerable to potential abuse from backlash due to the terrorist attacks of September 11. These include Muslims, Arabs, Sikhs, and South Asians. Between June 2003 and December 2003 (the most recent reporting period), the IG received 1,266 complaints suggesting potential civil rights or civil liberties violations (including many that were not within the IG's or DOJ's jurisdiction). Of these 720 were deemed "unrelated"—that is, they either cited no improper act by any DOJ employee/contractor or identified no discernible nexus between the alleged conduct and any civil rights/civil liberty violations. Many of these complaints appear to have been frivolous (e.g., allegations that the government was broadcasting harmful electronic signals at an individual).

Another 384 were complaints outside of the IG's jurisdiction because, for example, they alleged acts by local law enforcement or private businesses. Some of these were significant allegations (e.g. of excessive use of force by local police) and others were less serious (e.g., that INS or TSA inspectors were rude). In any event, all of these allegations, whether true or not, relate to traditional law enforcement issues and are unrelated in any way to the Patriot Act.

Thus, at bottom only 162 complaints were within the scope of the Department's activity. But these 162 were examined simply because they made a *prima facie* claim of a violations. Examples included alleged excessive force used by Bureau of Prisons officers and alleged fabrication of evidence by FBI agents. In then end only 17 of these investigations were deemed to warrant the opening of an investigation and substantial review.

It is important to emphasize that figure. Since September 11, DOJ agents in myriad capacities have encountered common citizens in literally hundreds of thousands of different situations, perhaps millions: from simple interviews to full-scale searches and everything in between. From those many, many interactions, only 17 warranted close review. That is a remarkably low rate of error—even assuming that all 17 investigations in fact identified actual violations (an issue as to which the IG's report is silent).

Finally, even more remarkable is the conclusion of the IG with regard to the Patriot Act itself: "*None of the 162 matters [within the IG's jurisdiction] involved complaints alleging misconduct by DOJ employees related to their use of a substantive provision of the Patriot Act.*" Far from there being any actual violations, there were not even any colorable allegations of a violation of civil rights or civil liberties under the Act. And, notably, this conclusion is from an IG who has not been reticent to criticize the Department where appropriate.

Racial or National Origin Profiling. Racial profiling poses a deeply difficult and intractable problem. As a society, we reject general reliance on immutable characteristics such as race or gender. On the other hand, the problems of terrorism pose new and greater dangers. The proper way to define the "reasonableness" of law enforcement activity is to assess three separate values: the degree of intrusion occasioned by the activity, the harm being averted, and the "closeness of the fit" between the scope of activity in question and the harm being averted.

Looked at through this prism of analysis, it is easy to see why most racial profiling is wisely rejected. Typically, the harm being averted is a general common law crime and the "fit" is poor at best ,and often non-existent. Profiling African-Americans for driving on certain roadways fits in this category. If it exists, it is unjustifiable and unconstitutional.

But this also suggests that, in *very limited* circumstances, the balance might change when the object is to prevent terrorism, and the use of national origin data and characteristics is much more narrowly applied.

The new Department of Justice policy strikes the right balance. It recognizes that for "traditional law enforcement activities" involving routine law enforcement actions such as traffic stops, federal law enforcement officers should never rely on race or ethnicity, except to the understandable extent that they have a suspect description that includes such information. The policy also makes clear that in connection with a specific investigation, law enforcement may only consider race or ethnicity if there is a "close fit" to an identified criminal incident either because of geography or a temporal connection. These are good rules. They make clear that, in general, race and ethnicity are not relevant to investigations for common law crimes.

The Department's policy also makes clear, however, that in the case of terrorism—that is, in cases where national security or some other catastrophic threat is involved—the general constitutional framework applies. Thus, in very rare circumstances where substantial predication exists, the Department contemplates a regime permitting investigation that includes a component of ethnicity or national origin. This, too, recognizes the fundamental importance of national security, while honoring the rule of law. We have a right to expect that such instances will be rare—but we must also recognize that on a few occasions they may be necessary.

Finally, we should turn our attention to the inevitable problems that will arise because of a potential invidious use of racial or ethnic classification for reasons that are only masquerading as legitimate. One thinks, immediately, of the security officer who targets for additional screening and inspection men of a particular ethnicity (a case, by the way, that the DOJ guidelines expressly declare improper and prohibit). How can we fight that all too real prospect?

One answer may lie in technology. Not all solutions necessarily trade off Type I and Type II errors, and certainly not in equal measure. Some novel approaches to combating terrorism might, through technology, actually reduce the incidence of both types of error. Consider, for example, various proposals for enhanced electronic data screening procedures, such as the Secure Flight (formerly CAPPS II) proposal now being developed by the Transportation Security Administration. Systems like this (and other similar proposals) do not result in a one-way diminution of privacy. Rather, they require trade-offs in different types of privacy: substituting one privacy intrusion (into electronic data) for another privacy intrusion (the physical intrusiveness of body searches at airports).

Rules-driven risk assessment systems such as Secure Flight/CAPPS II substitute hard data and *a priori rules* for instinct and racial stereotypes. Thus, they will undoubtedly have the salutary effect of reducing the need for random searches and eliminate the temptation for screeners to use objectionable characteristics of race, religion, or national origin as a proxy for threat indicators. For many Americans, the price of a little less electronic privacy might not be too great if it resulted in a little more physical privacy, fewer random searches, and a reduction in invidious racial profiling.

Glossary

Delayed notification warrant: Also known as a sneak-and-peek warrant. A written order by a judge which authorizes a law enforcement officer to search a specific place and to seize evidence without first notifying the owner of the intention.

International Money Laundering Abatement and Anti-Terrorist Funding Act of 2001: The Act is in Title III of the Patriot Act and is dedicated to addressing gaps in the intelligence and law enforcement systems as they relate to finance, such as significant money laundering or financing terrorist activities.

FINCEN: Financial Crimes Enforcement Network. A body that deals with problems such as money laundering and financing of terrorism.

FISA: Foreign Intelligence and Surveillance Act (enacted in 1978).

Pen register: A mechanical device that logs telephone numbers dialed without listening to the conversation.

Probable cause: Required under the Fourth Amendment for the issuance of certain warrants. Needs reasonable grounds to believe that the person has committed or is committing a crime or that a place is connected to a crime.

Roving wiretap: Electronic or mechanical eavesdropping on a person regardless of the device being used by target.

Search warrant: A written order by a judge which authorizes a law enforcement officer to search a specific place and to seize evidence.

SEVIS: Student and Exchange Visitor Information System. A system for tracking foreign students in the United States.

Sneak-and-peek warrant: See delayed notification warrant.

Subpoena: A written order commanding a person to appear or to bring materials before a court or tribunal.

Trap and trace: Technology which records phone numbers and traces the phone call to a location.

Type I error: Also known as a false positive. The error occurs when someone or something is deemed to match an entry in a database but in actuality does not.

Type II error: Also known as a false negative. The error occurs when someone or something is considered not to match an entry in a database but in reality it does.

Wiretapping: Electronic or mechanical eavesdropping done usually be law enforcement with a court order.

Sources

James Jay Carafano and Paul Rosenzweig, " A Patriotic Day: 9/11 Commission Recognizes Importance of the Patriot Act," Heritage Foundation *WebMemo* No. 480, April 15, 2004.

Edwin Meese III and Paul Rosenzweig, "The SAFE Act Will Not Make Us Safer," Heritage Foundation *Legal Memorandum* No. 10, April 30, 2004.

Paul Rosenzweig, "Civil Liberty and the Response to Terrorism" 42 *Duquesne Law Review* 663 (2004)

———, Testimony before the Committee on the Judiciary, U.S. Senate, in Hearing, "Aiding Terrorists—An Examination of the Material Support Statute," May 5, 2004.

———, Testimony before the United States Commission on Civil Rights in Hearing, "Anti-Terrorism Efforts, Civil Liberty, and Civil Rights," March 19, 2004.

———, Testimony before the Committee on Transportation and Infrastructure, Subcommittee on Aviation, U.S. House of Representatives, in Hearing, "The Transportation Security Administration's Computer-Assisted Passenger Prescreening System (CAPPS II)," March 17, 2004.

———, Testimony before the Technology and Privacy Advisory Committee, U.S. Department of Defense, regarding "Legal Principles and the Terrorism Information Awareness System," June 19, 2003.

———, Testimony before the Committee on the Judiciary, Subcommittee on the Constitution, U.S. House of Representatives, in Hearing "Anti-Terrorism Investigations and the Fourth Amendment After September 11: Where and When Can the Government Go to Prevent Terrorist Attacks?" May 20, 2003.

———, Testimony before the Committee on Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, U.S. House of Representatives, in Hearing, "Can the Use of Factual Data Analysis Strengthen National Security?" May 20, 2003.

———, Testimony before the Permanent Select Committee on Intelligence, U.S. House of Representatives, in Hearing, "Securing Freedom and the Nation: Collecting Intelligence Under the Law," April 9, 2003.

———, "Principles for Safeguarding Civil Liberties in an Age of Terrorism," Heritage Foundation *Executive Memorandum* No. 854, January 31, 2003.