AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

IMPLEMENTATION OF THE USA PATRIOT ACT: EFFECT OF SECTIONS 203(B) AND (D) ON INFORMATION SHARING

HEARING

BEFORE THE

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

APRIL 19, 2005

Serial No. 109–15

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://www.house.gov/judiciary

U.S. GOVERNMENT PRINTING OFFICE

20–707 PDF WASHINGTON : 2005

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

F. JAMES SENSENBRENNER, JR., Wisconsin, *Chairman*

HENRY J. HYDE, Illinois
HOWARD COBLE, North Carolina
LAMAR SMITH, Texas
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
STEVE CHABOT, Ohio
DANIEL E. LUNGREN, California
WILLIAM L. JENKINS, Tennessee
CHRIS CANNON, Utah
SPENCER BACHUS, Alabama
BOB INGLIS, South Carolina
JOHN N. HOSTETTLER, Indiana
MARK GREEN, Wisconsin
RIC KELLER, Florida
DARRELL ISSA, California
JEFF FLAKE, Arizona
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TOM FEENEY, Florida
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas

JOHN CONYERS, JR., Michigan
HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
MARTIN T. MEEHAN, Massachusetts
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
ANTHONY D. WEINER, New York
ADAM B. SCHIFF, California
LINDA T. SÁNCHEZ, California
ADAM SMITH, Washington
CHRIS VAN HOLLEN, Maryland

PHILIP G. KIKO, *Chief of Staff-General Counsel*
PERRY H. APELBAUM, *Minority Chief Counsel*

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

HOWARD COBLE, North Carolina, *Chairman*

DANIEL E. LUNGREN, California
MARK GREEN, Wisconsin
TOM FEENEY, Florida
STEVE CHABOT, Ohio
RIC KELLER, Florida
JEFF FLAKE, Arizona
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
LOUIE GOHMERT, Texas

ROBERT C. SCOTT, Virginia
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
MARTIN T. MEEHAN, Massachusetts
WILLIAM D. DELAHUNT, Massachusetts
ANTHONY D. WEINER, New York

JAY APPERSON, *Chief Counsel*
ELIZABETH SOKUL, *Special Counsel on Intelligence and Homeland Security*
JASON CERVENAK, *Full Committee Counsel*
MICHAEL VOLKOV, *Deputy Chief Counsel*
BOBBY VASSAR, *Minority Counsel*

CONTENTS

APRIL 19, 2005

OPENING STATEMENT

Page

The Honorable Howard Coble, a Representative in Congress from the State of North Carolina, and Chairman, Subcommittee on Crime, Terrorism, and Homeland Security 1

The Honorable Robert C. Scott, a Representative in Congress from the State of Virginia, and Ranking Member, Subcommittee on Crime, Terrorism, and Homeland Security 2

WITNESSES

The Honorable Michael T. McCaul, a Representative in Congress from the State of Texas

Oral Testimony 4

Prepared Statement 6

Ms. Maureen Baginski, Executive Assistant Director, Office of Intelligence, Federal Bureau of Investigation

Oral Testimony 9

Prepared Statement 11

Mr. Barry Sabin, Chief, Counterterrorism Section for the Criminal Division, U.S. Department of Justice

Oral Testimony 15

Prepared Statement 18

Mr. Timothy H. Edgar, National Security Policy Counsel, American Civil Liberties Union

Oral Testimony 23

Prepared Statement 25

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Prepared Statement of the Honorable Robert C. Scott, a Representative in Congress from the State of Virginia, and Ranking Member, Subcommittee on Crime, Terrorism, and Homeland Security 57

Prepared Statement of the Honorable Maxine Waters, a Representative in Congress from the State of California 57

Prepared Statement of the Honorable Sheila Jackson Lee, a Representative in Congress from the State of Texas 59

Brief *Amicus Curiae* of the American Civil Liberties Union of Virginia, Inc. in Support of Motion for Return of Property and to Unseal the Search Warrant Affidavit 62

IMPLEMENTATION OF THE USA PATRIOT ACT: EFFECT OF SECTIONS 203(B) AND (D) ON INFORMATION SHARING

TUESDAY, APRIL 19, 2005

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON CRIME, TERRORISM,
AND HOMELAND SECURITY
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 3:03 p.m., in Room 2141, Rayburn House Office Building, the Honorable Howard Coble (Chair of the Subcommittee) presiding.

Mr. COBLE. Good afternoon, ladies and gentlemen. We will come to order. Today is the second hearing in a series of ten in which the Judiciary Committee will review the provisions of the USA PATRIOT Act set to expire on December 31 of this year.

Prior to the terrorist attacks of 9/11, the Federal Government understood that information sharing between Government agencies was essential for national security. Executive Order 12333, issued in 1981, explains timely and accurate information about the activities, capabilities, and plans and intentions of foreign powers, organizations, and persons and their agents, is essential to the national security of the United States.

All reasonable and lawful means must be used to ensure that the United States will receive the best intelligence available. Unfortunately, achieving information sharing has been difficult, due to court-created restrictions, statutory prohibitions, and a resulting atmosphere of apprehension within the agencies charged with protecting our national security.

The 9/11 attacks made clear to all of us that civil liberties are endangered if the Government does not have the capacity to protect its people. Many, including the 9/11 Commission, pointed to the lack of information sharing as affecting the Government's ability to stop the 9/11 attacks. It is the responsibility of the Congress, it seems to me, to ensure that information sharing is facilitated in order to protect our civil liberties.

The attacks of September 11, 2001, clarified the immediate need for agencies to cooperate and share intelligence and law enforcement information. The USA PATRIOT Act began that process to allow information to be more freely shared, but the Committee on the Judiciary did not stop there. It passed additional legislation to assure that this vital information was provided to appropriate officials to protect our national security.

The Committee passed the Homeland Security Information Sharing Act and the Federal-Local Information Sharing Partnership Act of 2001, to remove the barriers for state and local officials to share and receive law enforcement and intelligence information with Federal officials. These two bills were added to the Homeland Security Act, which became law in 2002.

With these improvements, Congress understood the need for extensive oversight, and the Judiciary Committee continues to meet this mandate. Congress, and this Committee in particular, recognize that the Government must have the ability to protect our Nation after 9/11 and, with this heavy responsibility, the Congress must continue to protect civil liberties.

As part of the USA PATRIOT Act, the Congress included a sunset provision on certain new authorities in the Act. Two of these provisions, section 203(b) and 203(d), improved information sharing, but are due to expire on December 31 of this year, unless the Congress reauthorizes them.

Today, we will hear testimony on the need for these sections and on the concerns relating to information sharing between the Intelligence Community and law enforcement.

And I think I would be remiss, ladies and gentlemen, if I did not mention the fact that today marks the tenth anniversary of the devastating and inexcusable terrorist attack that occurred in Oklahoma City; at that time, the most severe terrorist attack that this country had endured, only to be surpassed by the 9/11 attacks. So it is my hope that we don't have to acknowledge subsequent attacks. But that will be for another day, I presume.

I look forward to hearing the testimony from our distinguished panel and witnesses, and look forward as well to hearing from our distinguished gentleman from Virginia, the Ranking Member, Mr. Bobby Scott.

Mr. SCOTT. Thank you, Mr. Chairman. I am pleased to join you in convening the hearing on subsections 203(b) and (d) of the USA PATRIOT Act, and join you in acknowledging the tenth anniversary of the attack; which reminds us of the importance of the work that we're doing.

We sunsetted both of those subsections, 203(b) and (d), along with a number of other provisions that were—because we were exposing the public to extraordinary Federal Government police powers enabling them to pry into individuals' private activities and spread information collected all over town without direct court supervision and oversight.

Our Country's founders are leery—were leery of Government power, particularly in the area of criminal law, so checks and balances were made an integral part of the criminal justice system, to ensure that people would be secure against unwarranted Government intrusion into their private properties and affairs, and that Government could not easily prove crimes against accused persons or accomplish a similar result by use of Government powers to harass or smear a citizen.

Today, with the cost of legal representation and the contingent of media eager to exploit sensationalism, mere suspicion or investigation of a crime can result in as much problems that our founders sought to protect us against. We will hear examples of this kind

of extraordinary Government power from one of our speakers today.

Mr. Chairman, as a compromise on not getting the level of judicial supervision and oversight many of us felt were warranted in connection with the extension of these extraordinary powers, by unanimous vote of the full Committee we voted to sunset these provisions after 2 years. This would allow us to exercise congressional oversight of these extraordinary powers within a short period of time. However, against the might of the Administration and the Senate, we ended up with a 4-year sunset.

And while I expect we will hear testimony about how useful the provisions have been, we still may not know a lot of what's going on, or what percentage has been useful, or what has been made of it, or what is being done with the information collected, or how long it will be kept, whether it's used or unused.

I look forward to the testimony of our witnesses and the light they will shed on these issues, and thank you, Mr. Chairman.

Mr. COBLE. I thank the gentleman. Ladies and gentlemen, it's the practice of the Subcommittee to swear in all witnesses prior to appearing before it, so if you would please stand and raise your right hands.

[Witnesses sworn.]

Mr. COBLE. Let the record show that each of the witnesses answered in the affirmative. And you may be seated.

Our first witness today is our colleague, Mr. Michael T. McCaul, Congressman from the Tenth District of Texas. Prior to beginning his career in Congress, Mr. McCaul served as Chief of Counterterrorism and National Security for the U.S. Attorney's Office in the Western Judicial District of Texas. He received his bachelor's degree from Trinity University, and his law degree from Saint Mary's University School of Law, and is a graduate of the Senior Executive School of Government at Harvard University.

Our second witness is Maureen A. Baginski, Executive Assistant Director of the FBI Office of Intelligence. Prior to joining the FBI, Ms. Baginski led the National Security Agency's Signals Intelligence Directorate. Ms. Baginski holds a master of arts degree in Slavic languages, and a bachelor of arts degree in Russian and Spanish, from the State University of New York in Albany.

Our next witness is Mr. Barry M. Sabin. Mr. Sabin is the Chief of the Counterterrorism Section for the Criminal Division of the Justice Department. Prior to beginning this role, Mr. Sabin served in the United States Attorney's Office in Miami, Florida. And Mr. Sabin received his bachelor's and master's degrees from the University of Pennsylvania, and his law degree from the New York University School of law.

Our final witness today is Mr. Timothy H. Edgar, the National Security Policy Counsel for the American Civil Liberties Union. Mr. Edgar was a law clerk for Judge Sandra L. Lynch, of the United States Court of Appeals for the First Circuit. He is a graduate of Dartmouth College and the Harvard Law School.

I guess you survived those severe winters in New Hampshire; did you, Mr. Edgar?

Mr. EDGAR. Yes, I did, Mr. Chairman.

Mr. COBLE. Ladies and gentlemen, we're delighted to have each of you here. We impose the 5-minute rule here against you all, and against us. So when you see that amber light, that is your warning that the clock is ticking. And the red light, of course, indicates that the 5 minutes have elapsed. We advise you of that in advance, so you won't be surprised. So if you all could adhere to the 5-minute rule, we would be appreciative.

And I'm pleased to recognize our colleague from Texas, Mr. McCaul.

TESTIMONY OF THE HONONORABLE MICHAEL T. McCAUL, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. MCCAUL. Well, thank you, Mr. Chairman and Ranking Member Scott, for giving me the opportunity to appear before you today and share with you my experiences in this on this very important issue. This is really why I ran for Congress, to ensure that our laws give law enforcement the tools they need to protect our Nation. My experience in the Justice Department prior to running for Congress, I believe, is relevant, and hopefully will provide some insight to the Committee.

When we talk about information sharing, when we talk about sharing between the criminal division in the Justice Department and the Intelligence Community, and from intelligence to the criminal side, I'd be remiss if I didn't talk about the law.

I served as a career prosecutor in the public integrity section at main Justice when the so-called "wall" between the criminal division and the FBI's foreign counterintelligence section was in place. After 9/11, I served as Chief of Counterterrorism in the U.S. Attorney's Office in Texas. My jurisdiction included the President's ranch, the State capitol, and the Mexican border.

I practiced law under the PATRIOT Act—including the ones which brought down the wall and the information sharing provisions we're discussing today. Also, prior to that, I served as deputy attorney general under then attorney general and now United States Senator John Cornyn.

I'd like to take us back to 1995, and I know that you're familiar with this memo. But at that time, the United States Attorney General adopted policies and procedures for contacts between the FBI and the criminal division concerning foreign counterintelligence investigations. This policy essentially prohibited the criminal division from controlling or directing FCI investigations. Eventually, these procedures would be narrowly interpreted to act as a wall between the FBI intelligence officials from communicating with the criminal division.

As noted by the 9/11 Commission report, this wall may have created a climate that helped contribute to 9/11. Indeed, an FBI agent testified that efforts to conduct a criminal investigation of two of the hijackers were blocked due to concerns over the wall.

Frustrated, he wrote to FBI headquarters saying, "Some day, someone will die and, wall or not, the public will not understand why we were not more effective at throwing every resource we had at certain problems. Let's hope the National Security Law Unit will stand behind their decisions then, especially since the biggest

threat to us now, Osama bin Laden, is getting the most protection." Now, these words are prophetic today.

Another good illustration of the wall creating a dangerous confusion is the case of Wen Ho Lee and the Los Alamos investigation. The first time the Chief of Counter Espionage in the Justice Department even heard of Wen Ho Lee was when he read about him in the "New York Times."

And indeed, in my own experience, I was assigned to investigate allegations that China attempted to corrupt and influence our elections. With the cooperation of witnesses, we were able to uncover some evidence that the director of Chinese intelligence may have funneled money to influence the presidential election. The frustration, however, came from the lack of coordination and communication with the foreign counterintelligence side of the house, particularly when our criminal investigation moved into the intelligence arena.

Ultimately, these examples portray an inefficient system in which the left hand literally did not know what the right hand was doing.

Today, thanks to the PATRIOT Act, this wall has come down. The PATRIOT Act helps us connect the dots, by removing the legal barriers that prevented law enforcement and the Intelligence Community from sharing information and coordinating to protect national security.

My own experience in the Justice Department after the wall came down was profound and dramatically improved. As chief of counterterrorism, I spearheaded the efforts of the Joint Terrorism Task Force. No longer did the barriers of communication exist. Indeed, the FBI's foreign counterintelligence agents and the Intelligence Community were full partners at the table. And for the first time, FBI intelligence files were reviewed by criminal division prosecutors and agents.

In addition, criminal files and grand jury materials, previously non-disclosable under rule 6(e), were now available in intelligence and terrorist cases. Our greatest task was to identify and locate the terrorist cells, and one of the tools we used to achieve this goal was through the use of national security wiretaps, or FISAs.

In addition to FISAs, the PATRIOT Act, in my view, provides many other tools necessary for law enforcement in the war on terrorism. First, it updates the law to the modern technology age. Second, it promotes efficiency by providing for nation-wide search warrants in terrorism cases. And finally, the PATRIOT Act takes laws which we've long applied to drug dealers and organized crime, and applies them to terrorists.

While most of the matters I worked on since the PATRIOT Act in the U.S. Attorney's Office remain classified, one example I can talk about where the provisions in the PATRIOT Act were extremely helpful was in a case involving allegations of a terrorist attack on the Fourth of July, 2003.

Mr. COBLE. Your 5 minutes are up, Mr. McCaul, if you could wrap up.

Mr. MCCAUL. Mr. Chair, if I could just ask for an additional 2 minutes, as a Member?

Mr. COBLE. Very well.

Mr. MCCAUL. I appreciate it. In late June—because I believe this story is compelling. In late June, we received intelligence from overseas from a specific and credible source that a terrorist attack was going to occur on the Fourth of July in the State of Texas. At the same time, we also received e-mails from an Internet chat room from an individual named "Apostasy Hears Voices" who threatened to commit terrorist acts at numerous locations throughout the United States.

The voice stated, "I have planned a little event for the Fourth of July. Roasted Americans on Independence Day. It will be the second largest terrorist demonstration in U.S. history." He described himself as having the name "Ali Aussie," a student at the University of Texas who had been on a mission for 4 years on a student visa as a member of a cell.

He stated that each cell acts independently for the most part, so that if one cell gets caught, the other cells are not compromised; which is consistent with how Al Qaeda operates. He concluded with the following words, "I did enjoy watching Americans burn alive in the World Trade Center event, barbecued Americans."

You can imagine in our office getting this information in conjunction with a threat alert that came from overseas. The JTTF went quickly into action, sharing intelligence information and coordinating with multiple jurisdictions.

By utilizing the PATRIOT Act, I was able to save valuable time by obtaining a national search warrant for electronic evidence for terrorist-related activities. Given the urgency of the matter and potential loss of human life, time was critical and of the essence. These provisions allowed us to execute the search warrants on the Internet service provider to obtain the information in real time.

Once we received the information, an arrest warrant was executed on the 3rd of July, just one day before the alleged planned attack. The defendant was charged with violating Federal law by using the Internet to make threats and to kill or injure persons.

Fortunately, the threat turned out to be a hoax. But it had been a real threat, and we had to assume that it was. And had it been a real threat, we would have saved lives. And that, in my judgment, is what the PATRIOT Act is all about: protecting and saving lives.

And in closing, Mr. Chairman, I can envision no bigger national security mistake than to go back to the way things were. Thank you.

[The prepared statement of Mr. McCaul follows:]

PREPARED STATEMENT OF THE HONORABLE MICHAEL T. MCCAUL

I would like to thank Chairman Coble and Ranking Member Scott for allowing me to testify before this Subcommittee in support of the USA PATRIOT Act.

My experience in the Justice Department prior to running for Congress is, in my opinion, relevant to this discussion and I would like to offer any insight and perspectives that may be helpful to this Committee. I served as a career prosecutor in the Public Integrity Section at Main Justice when the so called "Wall" between the Criminal Division and the FBI's Foreign Counter Intelligence was in place. After 9/11, I served as the Chief of Counter-Terrorism and National Security for the U.S. Attorney's office in the Western District of Texas. My jurisdiction included the President's ranch, the State Capitol, and the Mexican border. In that capacity, I practiced law under the USA PATRIOT Act provisions, including the one which brought down the "Wall." I also served as Deputy Attorney General under then Attorney General and now United States Senator John Cornyn.

In 1995, the Attorney General adopted policies and procedures for Contacts between the FBI and the Criminal Division Concerning Foreign Counterintelligence investigations ("FCI"). This policy prohibited the Criminal Division from "directing or controlling" FCI investigations. Eventually these procedures would be narrowly interpreted to act as a "wall" to prevent FBI Intelligence officials from communicating with the Criminal Division.

As noted by the 9/11 Commission report, this wall may have created a climate that helped contribute to 9/11. An FBI agent testified that efforts to conduct a criminal investigation of two of the hijackers were blocked due to concerns over the "wall." Frustrated, he wrote to FBI headquarters, "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. Let's hope the National Security Law Unit will stand behind their decisions then, especially since the biggest threat to us now [Osama Bin Laden], is getting the most protection."

Another good illustration of the wall creating dangerous confusion is in the case of Wen Ho Lee and the Los Alamos investigation. The first time the Chief of the Counter-Espionage Section in the Justice Department heard about the Wen Ho Lee case was when he read about it in the New York Times.

Indeed, in my own experience, I was assigned to investigate allegations that China attempted to corrupt and influence our elections. With the cooperation of witnesses, we were able to uncover some evidence that the Director of Chinese Intelligence may have funneled money to influence the Presidential election. The frustration came from the lack of coordination and communication with the foreign counterintelligence side of the house particularly when our criminal investigation moved into the intelligence arena.

Ultimately, these examples portray an inefficient system in which the left hand did not know what the right hand was doing.

As stated by the FISA Court of Review, "Indeed effective counterintelligence, we have learned, requires the wholehearted cooperation of all the government's personnel who can be brought to the task—A standard which punishes such cooperation could well be thought dangerous to national security."

Today, thanks to the Patriot Act, that wall has come down. The PATRIOT Act helps us "connect the dots" by removing the legal barriers that prevented law enforcement and the intelligence community from sharing information and coordinating activities in the common effort to protect national security. It dismantled the walls of separation and enabled a culture of cooperation that is essential to our integrated antiterrorism campaign. The President and the Attorney General recognized that without the ability to share information, including intelligence, we risked the very survival of this nation.

As stated by Senator Leahy, "This bill breaks down traditional barriers between law enforcement and foreign intelligence. This is not done just to combat international terrorism, but for any criminal investigation that overlaps a broad definition of "foreign intelligence."

My experience in the Justice Department after the wall came down was profound and dramatically improved. As Chief of Counter-Terrorism I spearheaded the efforts of the Joint Terrorism Task Force. No longer did the barriers of communication exist. Indeed, the FBI's foreign counterintelligence agents and the intelligence community were full partners at the table. For the first time, FBI intelligence files were reviewed by Criminal Division prosecutors and agents. In addition, criminal files and grand jury materials, previously non-disclosable under Rule 6(e) were now available in intelligence cases. Our greatest task was to identify and locate the terrorist cells. One of the tools we used to achieve this goal was through the use of National Security Wiretaps or FISAs (Foreign Intelligence Surveillance Act).

Many of the crimes prosecuted in the Justice Department may not appear to be "terrorist" related. They include fraudulent documents, alien smuggling, money laundering, as well as weapons and drug violations. For instance, in the case of Ramzi Yousef, the perpetrator of the '93 World Trade Center Bombing; if we had pursued his immigration violation as aggressively as it would be today, perhaps the first Al Qaeda cell in the United States would have been disrupted.

In addition to FISAs, the Patriot Act provides many other tools for law enforcement in the war on terrorism. First, the PATRIOT Act updated the law to the technology. No longer will we have to fight a digital-age battle with antique weapons—legal authorities left over from the era of rotary telephones.

Next, it promotes efficiency by providing for nationwide search warrants in terrorism cases. Prosecutors and investigators save valuable time because they are able to petition the local federal judge who is most familiar with the case and who is overseeing the nationwide investigation.

While most of the matters I worked on since the PATRIOT Act remain classified, one example where these provisions in the PATRIOT Act were extremely helpful was in a case involving allegations of a terrorist attack on July 4th, 2003. In late June, we received intelligence from a specific and credible source that a terrorist attack was going to occur on the 4th of July in the State of Texas. At the same time, we also received E-mails from an internet chat room from an individual named "Apostasy Hears Voices" who threatened to commit terrorist act at numerous locations throughout the United States as a member of an unknown terrorist cell. Specifically, the individual threatened that on the 4th of July 2003, significant locations in Austin, Texas, Washington D.C., New York, Miami, Charlotte, San Francisco, Seattle, and Portland would be attacked by terrorists. The Voice stated, "Well I have planned a little event for July 4th . . . Roasted Americans on Independence Day. It will be the second largest terrorist demonstration in U.S. history." He described himself as having the name "Ali Aussie" a student a the University of Texas who has been on a "mission" for four years on a student visa as a member of a cell. He stated that "each cell acts independently for the most part so that if one cell gets caught, the other cells are not compromised which is consistent with how Al Qaeda operates. He concluded with the following words, "I did enjoy watching Americans burn alive in the WTC event, BBQ Americans."

The JTTF quickly went into action sharing intelligence, information and coordinating with multiple jurisdictions. By utilizing the Patriot Act provisions 18 U.S.C. 2702 s 219, 220, I was able to save valuable time by obtaining a national search warrant for electronic evidence for terrorist related activities.

Given the urgency of the matter and potential loss of human life, time was critical and of the essence. These provisions allowed us to execute search warrants on the internet service provider to obtain subscriber information in real time. Once we received the information, an arrest warrant was obtained and the defendant was arrested on July 3rd, one day before the alleged planned attack. The defendant was charged with violating 18 U.S.C. 844(e) by using the internet to makes threats to kill or injure persons by an explosive device. Fortunately, the threat turned out to be a hoax. But had it been a real threat, and we have to assume they all are, we would have saved lives. And that in my judgment is what the Patriot Act is all about—protecting and saving lives.

There has been much talk from critics of the PATRIOT Act regarding allowing many of the information sharing provisions in the law. Having served under its provisions before and after the bringing down of the "Wall" and the implementation of the PATRIOT Act, I can envision no bigger National security mistake than to go back to the way things were. Section 203(b) closed a dangerous gap between criminal investigations and counterterrorism. Each restriction on information sharing makes it more difficult for investigators to connect the dots to prevent terrorist attacks. If this section were to expire, US officials would be allowed to share certain foreign intelligence information with foreign intelligence services like MI–5 and the Massad but not with our own CIA.

This section has been used by the Department of Justice on a regular basis and has been instrumental to the increased coordination and information sharing between intelligence and law enforcement that has taken place over the last three and a half years. This provision has been used to help officials break up terror cells within the US, such as in Portland, Oregon and Lackawanna, NY.

The FBI has stated that thanks to 203(d), agents can involve other agencies in investigations, resulting in the type of teamwork that enables more effective and responsive investigations, improves use of resources, allows for follow up investigations by other agencies when the criminal subject leaves the US, and helps prevent the compromise of foreign intelligence investigations.

Finally, the PATRIOT Act takes laws which have long-applied to drug dealers and organized crime, and applies them to terrorists. For example, for years law enforcement has been able to use roving wiretaps, which follow all communications used by a suspect as opposed to just one telephone line. The PATRIOT Act simply authorizes the use of this technique in national-security intelligence investigations and amends the Foreign Intelligence Surveillance Act to conform to the parallel provision found in the Federal Wiretap Statute.

Contrary to critics' assertions, the Justice Department cannot do anything without court supervision. The USA PATRIOT Act does not abrogate the role played by the judiciary in the oversight of the activities of federal law enforcement. Federal agents still have to obtain judicial approval before they can search a residence. Federal agents still have to obtain judicial approval before they can install a wiretap.

I'd like to leave you with the following words:

The confrontation that we are calling for with the apostate regimes does not know Socratic debates Platonic ideals nor Aristotle diplomacy. But it does know the dia-

logue of bullets, the ideals of assassination, bombing, and destruction, and the diplomacy of the cannon and machine-gun. Islamic governments have never and will never be established through peaceful solutions and cooperative councils. They are established as they always have been through pen and gun—by word and bullet—and by tongue and teeth. This is the preface to the Al Qaeda Training Manual.

These words demonstrated the widely held belief that the question is not if the terrorists will strike us again, but rather when and where.

Thomas Jefferson once said that "the cost of freedom is eternal vigilance." Those words ring more true today than ever before.

We owe it to the citizens of this country to reauthorize the USA PATRIOT Act. For if we don't, and another terrorist attack occurs on our shores, we will all be held accountable.

Mr. COBLE. I thank the gentleman. Now that the door is ajar, I am going to be obliged to give you all 7 minutes, as well. If you can do it in five, we would be appreciative. And folks, I failed to tell you where that ominous red light appears. It's on the panels before you.

Ms. Baginski, good to have you with us.

TESTIMONY OF MAUREEN A. BAGINSKI, EXECUTIVE ASSISTANT DIRECTOR, OFFICE OF INTELLIGENCE, FEDERAL BUREAU OF INVESTIGATION

Ms. BAGINSKI. Thank you, Mr. Chairman. Thank you, Ranking Member Scott. It's very nice to be here. I really am happy to be here today, and I come as a lifelong member of the Intelligence Community. As you said, in my last position, 25 years with the National Security Agency, which is the Nation's foreign intelligence, signals intelligence collection and dissemination organization.

What is common between the job at NSA and the job at the FBI is that my job is to ensure that intelligence, which is just vital information about those that would do us harm, gets in the hands of those charged with defending our Nation from our adversaries.

In both of those jobs, we have a dual imperative. The first is to produce information to protect the Nation, and the second is to ensure that we are protecting the rights of U.S. citizens as we are doing it. As an intelligence professional and as a citizen, I believe that the USA PATRIOT Act has been an essential tool in allowing us to fulfill those dual imperatives.

We don't share information for the sake of sharing information. We actually do it to prevent harm to the Nation. It is the global nature of the threat that we face that demands the information sharing across geography, across organizations; because no one organization can actually do this job alone.

To defeat the adversaries we face today, we have to increasingly be more like a global network. And it is the PATRIOT Act that has allowed the law enforcement community to become a very vital node on that global information network.

Here is an example. PATRIOT Act section 203(b) authorizes us to share foreign intelligence information obtained under title III electronic surveillance with other officials, including intelligence, law enforcement officers. And if this provision were allowed to expire, we would have a greatly impaired global network, because in theory, the FBI agents would be able to share this information with foreign intelligence services, such as MI-5, but arguably would not be able to share that information with the CIA. The result would be inconsistent with the spirit of what we're trying to achieve, but

most clearly with the spirit of the recently passed intelligence reform bill.

There are two components to information sharing, and we have to talk about the two of these very distinctly, I think. The first is the actual acquisition or collection of the information, as I would describe it from my intelligence background, and the legal authorities and policies that govern that collection. And the second is how the information is then stored and shared, once it is collected.

All of us that are involved here at this table and outside of this room in the collection of information do so against a carefully set—a carefully established set of laws and policies. Intelligence agencies, criminal investigators, we are all governed by legal authorities and policies that derive from those.

For example, in my case, the FBI authority to collect intelligence information is very clearly laid out in law, and guided at each step by guidelines set by the Attorney General. And our collection authorities are also overseen and controlled by Federal courts.

Under the PATRIOT Act, a Federal judge must still approve search warrants and wiretaps for counterintelligence and counterterrorism investigations, and we must establish probable cause to obtain a FISA warrant. So that's on the collection end.

The information sharing component happens after the legal collection of the information. And section 203(b) and (d) have allowed us to share legally collected information from our intelligence and criminal investigations operations both inside the FBI and outside of the FBI; and as the Congressman described, the wall having come down.

But I want to give you a very concrete example that I work with every day that this has enabled. And probably, the best example of this can be seen in the National Counterterrorism Center, formerly the TTIC.

In the National Counterterrorism Center 15 different agencies come together, bringing their legally collected, but independently collected, information to carry out three very important functions for the Nation. The first is the production of all-source terrorism analysis. The second is updating the database that other Federal entities use to prevent—this is known as our watch list—to prevent known or suspected terrorists from entering U.S. borders. And of course, the third is to have the intelligence they need to exercise their counterterrorism plans and perform independent alternative analysis.

Now, in this center legally collected information comes together in the same room. FBI people are there. And the way that the FBI people, the FBI analysts, share their information with representatives from other agencies is by relying on the provisions of 203(d). They would be able to have their information, but without those provisions it would be less clear to them how they could share information from criminal investigations that bear on terrorism-related things absent 203(d).

It's a very important thing, and a very worthwhile thing to go see legal collection come together with these very important analytic functions that are often referred to as "connecting the dots." But in their sum, they prevent harm to the Nation.

And just to wrap up, experience has taught us—and I think this is very important to understand in the nature of today's threat—there is no neat dividing line that distinguish criminal, terrorism, and foreign intelligence activity or information. Criminal, terrorist, and foreign intelligence organizations and activities are often interrelated and interdependent.

If you look at alien smugglers, drug traffickers, they have something in common. They control the means of conveyance; they control borders; they control things. They will smuggle anything. They will smuggle people; they will smuggle drugs; they will smuggle terrorists. And in the worst case, they will smuggle nuclear weapons. Intelligence is critical across all of these programs precisely to get to that point of connecting these things.

So in summary, we have found the information sharing provisions of the PATRIOT Act vital to our national security, as is our responsibility to protect the rights of U.S. citizens. So mostly, we applaud the forum that you've provided for the public debate and discussion of these very, very important issues, and we look forward to working with you further in this discussion.

[The prepared statement of Ms. Baginski follows:]

PREPARED STATEMENT OF MAUREEN A. BAGINSKI

Good morning Mr. Chairman and Members of the Subcommittee. I am pleased to be here today with Barry Sabin, Chief of the Counterterrorism Section, Department of Justice Criminal Division to talk with you about the ways in which the USA Patriot Act has assisted the FBI with its information-sharing efforts. I will address the overall benefits of the information sharing provisions of the Act, including: the relevant amendments to the Foreign Intelligence Surveillance Act; Section 203(b), which authorizes the sharing of foreign intelligence information obtained in a Title III electronic surveillance with other federal officials, including intelligence officers, DHS/DOD/ICE officials, and national security officials; and Section 203(d), which specifically authorizes the sharing of foreign intelligence information collected in a criminal investigation with intelligence officials.

It is important to place the information sharing provisions of the USA Patriot Act in the context of subsequent Congressional action formalizing the FBI Intelligence Directorate in 2004. The Statement of Managers accompanying the Conference Report on H.R. 4818, Consolidated Appropriations Act, 2005 (House of Representatives—November 19, 2004), states:

> ". . . the conference agreement adopts the House report language directing the FBI to create a new Directorate of Intelligence. . . . The need for effective intelligence capabilities cuts across all FBI programs including the counterterrorism, counterintelligence, criminal and cyber crime programs. This new directorate will ensure that intelligence is shared across these programs, eliminate information stove-piping, and allow the FBI to quickly adapt as threats change. . . . It shall also work to improve the FBI's capability to share intelligence, not only within the Bureau and the Intelligence Community, but also with State and local law enforcement."

I am here today to express to you how crucial renewal of the USA Patriot Act provisions related to information and intelligence sharing is to fulfilling the responsibilities of the FBI's new Directorate of Intelligence as envisioned by Congress.

There are two components to this subject: first, the issue of collecting intelligence and the legal authorities and policies that govern that collection; and second, how that information is actually shared once it is collected. I will address both in turn.

I realize that the collection authorities granted under the Patriot Act are of concern to many individuals and organizations. In that regard I want to say two things.

First, the FBI is committed to carrying out its mission in accordance with the protections provided by the Constitution. FBI agents are trained to understand and appreciate that the responsibility to respect and protect the law is the basis for their authority to enforce it. Respect for Constitutional liberties is not optional, it is mandatory for all FBI employees. The FBI could not be effective—and would not exist—without it.

Second, the FBI's authority to collect information is very clearly laid out in law and is directed by the Attorney General—the chief law enforcement officer for the United States. Intelligence collection is only done in accordance with the intelligence priorities set by the President, and is guided at every step by procedures mandated by the Attorney General. As soon as an international terrorism intelligence or counterintelligence case is opened, both Headquarters and the Department of Justice are notified. We are subject to and follow Attorney General's guidelines and procedures for FBI National Security Investigations and Foreign Intelligence Collection (NSIG); and all terrorism-related cases are subject to in-progress review by the Department of Justice (DOJ) Office of Intelligence Policy and Review, the DOJ Criminal Division, and local offices of U.S. Attorneys. We report annually to the Department of Justice on the progress of intelligence cases. The FBI's collection authorities are also controlled by the Federal Courts. Under the USA Patriot Act, a federal judge must still approve search warrants and wiretaps for counterintelligence and counterterrorism investigations and Agents must establish probable cause in order to obtain a FISA warrant. The FBI only collects and disseminates intelligence under guidelines designed specifically to protect the privacy of United States persons, and we are committed to using our authorities and resources responsibly.

After information is legally collected, the issue of how we pool that information arises. Effective intelligence requires skilled analysis and dissemination to meet the requirements of customers inside and outside the FBI. My job as the FBI's Executive Assistant Director for Intelligence is to manage the entire intelligence cycle to ensure that the FBI has the collection, reporting, analysis and dissemination capability it needs to protect the country. Information sharing is vital to that capability.

Effective FBI intelligence capabilities depend, first of all, on the integration of our intelligence collection and criminal investigative operations. During hearings on the 9/11 attacks, Congress heard testimony about meetings between the CIA and FBI where it was unclear what information on a hijacker could be legally shared under the widely-misunderstood set of rules and laws that was known as "the Wall." This wall extended into the FBI itself. Agents pursuing cases involving the Foreign Intelligence Surveillance Act (FISA) could not readily share information with agents or prosecutors working criminal investigations. And the wall worked both ways—without FISA-derived information agents or prosecutors involved in a criminal case might not have any way of knowing what information from the criminal investigation might be useful to an agent working on a parallel international terrorism or counterintelligence investigation. Although there was some legal capability to share information, the law was complex and as a result, agents often erred on the side of caution and refrained from sharing the information. In addition, the wall functioned to discourage criminal and intelligence investigators from talking about their cases, such that investigators on either side might have no idea what might be useful to share with those on the other side of wall.

The Patriot Act tore down those legal walls between FISA-related intelligence and criminal investigations. Law enforcement and intelligence agents were able to coordinate terrorism investigations without fear of running afoul of the law as then interpreted.

Patriot Act Section 203(b) authorizes the sharing of foreign intelligence information obtained in a Title III electronic surveillance with other federal officials, including intelligence officers, DHS/DOD/ICE officials, and national security officials. If Section 203(b) were allowed to expire, FBI Agents would be allowed to share certain foreign intelligence information collected through criminal investigative wiretaps with foreign intelligence services, such as MI–5, but would arguably not be allowed to share that same information with the CIA. This result would be inconsistent with the spirit of the recently enacted Intelligence Reform and Terrorism Prevention Act of 2004, which included many provisions designed to enhance information sharing within the federal government.

An example of information sharing now permitted by section 203 of the USA PATRIOT Act takes place in the National Counterterrorism Center (NCTC) (formerly the Terrorist Threat Integration Center). The NCTC receives foreign intelligence information lawfully collected by its member entities, which includes international terrorism information collected by the law enforcement community. Information provided to NCTC pursuant to section 203 of the PATRIOT act is used in three crucial NCTC missions: the production of all-source terrorism analysis, updating the database used by other federal entities to prevent known or suspected terrorists from entering U.S. borders, and to ensure that agencies, as appropriate, have access to and receive all-source intelligence needed to execute their counterterrorism plans or perform independent, alternative analysis. The FBI, one of the NCTC's key members, relies upon section 203(d) of the USA PATRIOT Act to provide information related to international terrorism to NCTC analysts including intelligence, protective,

immigration, national defense, national security, and other information related to international terrorism (a subset of foreign intelligence and counterintelligence information) obtained as part of FBI criminal investigations. In particular, section 203(d) authorizes law enforcement officers to disclose foreign intelligence or counterintelligence information to various federal officials, notwithstanding any other legal restriction. Without section 203(d), access to such FBI information by non-FBI personnel at NCTC could put us back to the pre 9/11 days of uncertainty about information sharing authorities. A decision by this Congress to allow section 203(d) to sunset would send the message that full information sharing is discouraged and law enforcement and intelligence officials will once again be left with a complex legal regime and err on the side of caution and refrain from sharing terrorism information.

Furthermore, section 203 of the PATRIOT Act facilitates the NCTC's ability to

provide strategic analysis to policy makers and actionable leads to officers within the FBI and the Intelligence Community (including components of the Department of Homeland Security (DHS)), transcending traditional government boundaries.

The NCTC estimates that the number of known or appropriately suspected terrorists intercepted at borders of the United States, based on FBI reporting alone, has increased due to the information sharing provisions of the USA PATRIOT Act. The NCTC maintains TIPOFF, an up-to-date database of known and appropriately suspected terrorists. The NCTC relies upon various agencies, which provide terrorist identity information on an on-going basis. Much of the terrorist identities information the NCTC receives from the FBI is collected in the course of criminal investigations and is shared pursuant to section 203.

Tearing down the wall between criminal and intelligence investigations actually enabled the FBI to conduct intelligence analysis and to integrate intelligence analysis into the Bureau. Our Intelligence Program now crosses all investigative programs—Criminal, Cyber, Counterterrorism, and Counterintelligence. And the Directorate of Intelligence is able to leverage the core strengths of the law enforcement culture—with its attention to the pedigree of sources and fact-based analysis—while ensuring no walls exist between collectors, analysts, and those who must act upon intelligence information to keep our nation safe. As FBI Director Mueller said in a speech to the American Civil Liberties Union (ACLU) in 2003: "Critical to preventing future terrorist attacks is improving our intelligence capabilities so that we can increase the most important aspect of terrorist intelligence information—its predictive value. . . . The global aspect of terrorism creates an even greater need for the FBI to integrate its intelligence program and criminal operations to prevent attacks."

Facing today's threats, it makes no sense not to share information that has been legally collected with those who have a need for it and can maintain proper security and privacy safeguards.

Experience has taught the FBI that there are no neat dividing lines that distinguish criminal, terrorist, and foreign intelligence activity. Criminal, terrorist, and foreign intelligence organizations and activities are often interrelated or interdependent. FBI files are full of examples of investigations where information sharing between counterterrorism, counterintelligence and criminal intelligence efforts and investigations was essential to the FBI's ability to protect the United States from terrorists, foreign intelligence activity and criminal activity. Some cases that start out as criminal cases become counterterrorism cases. Some cases that start out as counterintelligence cases become criminal cases. Sometimes the FBI will initiate parallel criminal and counterterrorism or counterintelligence cases to maximize the FBI's ability to adequately identify, investigate and address a variety of threats to the United States while protecting vulnerable sources and methods. The success of these cases in providing accurate intelligence threat assessments as well as arrests and convictions is entirely dependent on the free flow of information between the respective investigations, investigators and analysts.

Ongoing criminal investigations of transnational criminal enterprises involved in counterfeit goods, drug/weapons trafficking, money laundering and other criminal activity depend on close coordination and information sharing with the FBI's Counterterrorism and Counterintelligence Programs, as well as with other agencies in the intelligence community, when intelligence is developed which connects these criminal enterprises to terrorism, the material support of terrorism or state sponsored intelligence activity.

As an example of benefits from sharing intelligence from such a case, information from a criminal Title III surveillance and criminal investigation was passed to FBI Counterterrorism investigators and intelligence community partners, because the subject of the criminal case had previously been targeted by other agencies. Infor-

mation sharing permitted the agencies to pool their information and resources to uncover the interplay of criminal and foreign intelligence activity.

As an example of sharing from a terrorism intelligence case, a terrorism investigation initiated in Minneapolis was subsequently transferred to San Diego and converted to a criminal case. The investigation focused on a group of Pakistan-based individuals who were involved in arms trafficking, the production and distribution of multi-ton quantities of hashish and heroin, and the discussion of an exchange of a large quantity of drugs for four stinger anti-aircraft missiles to be used by Al Qaeda in Afghanistan. The operation resulted in the arrest, indictment and subsequent deportation of the subjects, Syed Mustajab Shah, Muhammed Afridi, and Ilyas Ali, from Hong Kong to San Diego to face drug charges and charges of providing material support to Al Qaeda. In this case the benefits of immediate disruption by arrest outweighed the need for long-term intelligence coverage of the conspirators.

Another example came in the aftermath of the September 11th attacks. A reliable intelligence asset identified a naturalized U.S. citizen as a leader among a group of Islamic extremists residing in the U.S. The subject's extremist views, his affiliations with other terrorism subjects, and his heavy involvement in the stock market increased the potential that he was a possible financier and material supporter of terrorist activities. Early in the criminal investigation it was confirmed that the subject had developed a complex scheme to defraud multiple brokerage firms of large amounts of money. The subject was arrested and pled guilty to wire fraud. The close interaction between the criminal and intelligence cases was critical both to the successful arrest of the subject before he left the country and to the eventual outcome of the case. Once again, intelligence led to an arrest that was determined to be the most effective means to disrupt a potential terrorist threat.

Criminal enterprises are also frequently involved in, allied with, or otherwise rely on smuggling operations that do not respect jurisdictional lines between types of investigations or intelligence. Alien smugglers frequently use the same routes used by drug and contraband smugglers and do not limit their smuggling to aliens—they will smuggle anything or anyone for the right price. Terrorists can take advantage of these smuggling routes and enterprises to enter the U.S. and are willing to pay top dollar to smugglers. Intelligence developed in these cases also frequently identifies corrupt U.S. and foreign officials who facilitate smuggling activities. Current intelligence, based on information sharing between criminal, counterterrorism, and counterintelligence efforts, has identified smugglers who provide false travel documents to special interest aliens, deal with corrupt foreign officials, and financially support extremist organizations, as well as illegitimate and quasi-legitimate business operators in the United States, who not only use the services of illegal aliens, but are also actively involved in smuggling as well. These transnational criminal enterprises require global intelligence coverage, domestic as well as foreign, that transcends out-dated divisions between national security and criminal law enforcement.

Obviously, considering the cases I've just described, the information sharing provisions are overwhelmingly heralded by FBI Field Offices as the most important provisions in the USA Patriot Act. The ability to share critical information has significantly altered the entire manner in which terrorism and criminal investigations are conducted, allowing for a much more coordinated and effective approach than prior to the USA Patriot Act. Specifically, the Field Offices note that these provisions enable case agents to involve other agencies in investigations, resulting in a style of teamwork that enables more effective and responsive investigations, improves the utilization of resources allowing a better focus on the case, allows for follow-up investigations by other agencies when the criminal subject leaves the U.S., and helps prevent the compromise of foreign intelligence investigations.

From the perspective of the Directorate of Intelligence, the USA Patriot Act information sharing provisions are critical to the effectiveness of the Directorate's Field Intelligence Groups (FIGs) and to the integration of Directorate of Intelligence elements that are embedded in each of our headquarters investigative divisions. As authorized by the Congress, the Directorate now has a Field Intelligence Group in each field office that brings together the intelligence from criminal, counterterrorism, counterintelligence, and cyber investigations. The FIGs also include our language analysts who provide vital support to the full range of FBI investigations and intelligence collection. At headquarters, the Directorate manages intelligence analysis, in coordination with other elements of the intelligence community, to support both national security and criminal law enforcement requirements. Allowing the information sharing provisions of the USA Patriot Act to sunset would re-introduce barriers that would make intelligence sharing more difficult.

The Intelligence Reform Act directs the President to "create an information sharing environment for the sharing of terrorism information in a manner consistent

with national security and with applicable legal standards." It also directs the President to incorporate "protections for individuals' privacy and civil liberties," and further, to incorporate "strong mechanisms to enhance accountability and facilitate oversight, including audits, authentication, and access controls." The Intelligence Reform Act directs the DNI to implement those provisions and provides the DNI with a privacy and civil liberties officer to ensure implementation. The FBI has already implemented Executive Order 12333 in both our privacy systems and in the dissemination of information from our intelligence databases.

Specifically, we use a Privacy Impact Assessment (PIA) process to evaluate privacy in major record systems prior to system implementation. The PIA process requires that the system sponsor/developer conduct a thorough, written analysis of the impact on privacy that will result from the creation of a proposed system prior to the system's implementation. We assess both impacts attributable solely to the proposed system and the cumulative impacts arising from the proposed system's interface with existing systems. The PIA provides senior FBI management officials with a systemic assessment of a major new system's impact on privacy before the system becomes operational. The FBI PIA process includes a review of major systems by the FBI Privacy Council, a group composed of representatives from several FBI divisions, as well as an FBI Senior Privacy Official.

In summary, the information sharing provisions of the USA Patriot Act are vital to our national security. Allowing these provisions to sunset would be inconsistent with the spirit of the recently enacted Intelligence Reform and Terrorism Prevention Act of 2004, which included many provisions designed to enhance information sharing within the federal government. Provisions of the USA Patriot Act are critical to implementing the Congressional mandate for an "information sharing environment." Section 203(b) of the USA Patriot Act specifically authorizes the sharing of foreign intelligence information obtained in a Title III electronic surveillance with other federal officials, including intelligence officers and national security officials, such as DHS and DOD officials. Section 203(d) specifically authorizes the sharing of foreign intelligence information collected in a criminal investigation with intelligence officials. Allowing either of these provisions to sunset could seriously damage our information sharing and coordination efforts with the CIA, other intelligence agencies, and even internally between criminal and intelligence investigations.

Mr. Chairman and Members of the Subcommittee—thank you for your time and for your continued support of the FBI's information sharing efforts. I am happy to answer any questions.

Mr. COBLE. Thank you, Ms. Baginski. We've been joined by our friend, the distinguished gentleman from Massachusetts, Mr. Delahunt. Good to see you, Bill.

Mr. Sabin, good to have you with us.

TESTIMONY OF BARRY M. SABIN, CHIEF, COUNTERTERRORISM SECTION FOR THE CRIMINAL DIVISION, U.S. DEPARTMENT OF JUSTICE

Mr. SABIN. Good to be here. Mr. Chairman, Ranking Member Scott, Members of the Subcommittee, thank you for the opportunity to testify at this important hearing and address sections 203(b) and (d) of the USA PATRIOT Act. Both of these provisions are slated to sunset on December 31, 2005, and both deserve to be made permanent.

I seek to share with you from my perspective as a career prosecutor how critical these provisions have been in addressing terrorist threat information, criminal investigations, and the manner in which our counterterrorism mission has been performed on a daily basis.

Section 203 of the Act authorizes information sharing between law enforcement and the Intelligence Community. As such, it complements, and is complemented by, other provisions of the PATRIOT Act that facilitate such information sharing; most notably, sections 218 and 504. These provisions collectively have knocked down the so-called "wall" between law enforcement and intel-

ligence, a wall that impeded our efforts to combat international terrorism.

Prior to the PATRIOT Act, widespread misunderstandings about the wall hindered the flow of information in two directions: It hindered intelligence information from being passed to prosecutors; and it also hindered prosecutors and criminal investigators from sharing certain types of law enforcement information with the Intelligence Community and other national security officials.

Section 203 of the PATRIOT Act was enacted to deal with the latter problem, and to ensure that valuable foreign intelligence collected by the law enforcement community can be shared with the intelligence and national security communities, under appropriate safeguards.

Director Mueller testified earlier this month that the information sharing provisions are consistently identified by FBI field offices as the most important provisions in the PATRIOT Act. Pursuant to the PATRIOT Act, intelligence emanating from criminal investigations has indeed been routinely shared with other appropriate Government officials.

Some examples of intelligence information developed in a criminal case which was shared with the Intelligence Community under section 203(d) include the following:

Information about the organization of a violent jihad training camp, including training in basic military skills, explosives, and weapons, as well as a plot to bomb soft targets abroad, resulted from the investigation and criminal prosecution in New York of a naturalized United States citizen who was associated with an Al Qaeda related group;

Travel information and the manner that monies were channeled to members of a criminal conspiracy in Portland who traveled from the United States intending to fight, unsuccessfully, alongside the Taliban against U.S. and allied forces;

Information about an assassination plot, including the use of false travel documents and transporting monies to a designated state sponsor of terrorism resulted from the investigation and prosecution in Northern Virginia of a naturalized United States citizen who had been the founder of a well-known United States organization;

Information about the use of fraudulent travel documents by a high-ranking member of a designated foreign terrorist organization emanating from his criminal investigation and prosecution in Washington, D.C., revealed intelligence information about the manner and means of the terrorist group's logistical support network, which was shared in order to assist in protecting the lives of United States citizens;

The criminal prosecutions of individuals from Lackawana, New York, who traveled to and participated in a military-style training camp abroad yielded intelligence information in a number of areas, including details regarding the application forms which permitted attendance at the training camp. After being convicted, one defendant has recently testified in a separate Federal criminal trial about this application process, which assisted in the admissibility of the form and the conviction of those other defendants;

The criminal prosecution in Northern Virginia of a naturalized United States citizen who had traveled to an Al Qaeda training camp in Afghanistan revealed information about the group's practices, logistical support, and targeting information.

Title III information is similarly being shared under section 203(b): Wiretap interceptions involving a scheme to defraud donors and the Internal Revenue Service and illegally transfer monies to Iraq generated not only criminal charges in Syracuse, New York, but information concerning the manner and means by which monies were funneled to Iraq;

Intercepted communications in connection with a sting operation led to criminal charges in New York and Arkansas and intelligence information relating to money laundering, receiving and attempting to transport night-vision goggles, infrared Army lights, and other sensitive military equipment relating to a foreign terrorist organization.

Additionally, last year during a series of high-profile events, the 2004 Threat Task Force used the information sharing provisions under section 203(d) as part and parcel of performing its critical duties. And the FBI relies upon section 203(d), as my colleague just recounted, to provide information obtained in criminal investigations to analysts in the new National Counterterrorism Center; thus assisting the center in carrying out its vital counterterrorism missions.

The information sharing provisions not only promote a culture of teamwork and trust, they provide Government officials certainty in the performance of their duties. If section 203(d) is allowed to sunset, then each law enforcement agency's authority and duty to share foreign intelligence may have to be reevaluated, and this change might lead to unnecessary uncertainty and confusion.

Section 203 fully protects legitimate privacy and civil liberties interests through its controls on disclosure and use and its special protections for information identifying a U.S. person. For example, section 203(b) does not allow carte blanche disclosure of sensitive information. The information itself can only be acquired in the first place pursuant to the strict demands of title III, and section 203(b) does not in any way diminish or minimize those requirements.

Second, the only information that can be shared with intelligence or national security personnel is that which satisfies the statutory definitions of "foreign intelligence," "counterintelligence," or "foreign intelligence information." This requirement acts as a filter to prevent the unnecessary disclosure of extraneous information.

Third, the disclosure can only be to designated Federal officials, and solely for their official use.

And finally, as described above, identifying information about U.S. persons is subject to special restrictions.

For all of these reasons, section 203(b) correctly and appropriately facilitates a unified, cohesive counterterrorism effort, while also safeguarding privacy. Similarly, section 203(d) also protects privacy.

Prior to 9/11, we tied ourselves in knots with misunderstood legal and bureaucratic guidelines that had the effect of constricting the flow of essential information within the United States Government. We dare not, and must not, let this happen again.

Taken together, these provisions are crucial to the Government's efforts to prevent and preempt terrorist attacks. We cannot put artificial barriers between law enforcement agencies and entities such as the new National Counterterrorism Center, when it comes to the sharing of law enforcement information that has foreign intelligence value.

Mr. Chairman, as you debate these issues, we invite your questions, your comments, and your suggestions. We very much want to work with Congress to ensure that we will keep America safe and free. Sections 203(b) and (d) are helping us fight the terrorists in a manner that respects the Constitution and constitutional values.

This Congress should permanently renew sections 203(b) and (d) of the PATRIOT Act. I again thank the Committee for holding this hearing, and I will do my best to answer your questions.

[The prepared statement of Mr. Sabin follows:]

PREPARED STATEMENT OF BARRY M. SABIN

INTRODUCTION

Thank you for the opportunity to testify at this important hearing. Since the attacks of September 11, 2001, Congress and the Administration have made great progress in providing law enforcement and intelligence officials with the tools they need to prevent, disrupt, investigate, and prosecute terrorism. The most notable of these achievements was enactment of the USA PATRIOT Act ("Patriot Act" or "Act") in late 2001, passed with overwhelming and bipartisan support in the House and Senate.

As you know, many sections of that Act are slated to sunset later this year, unless the Congress acts to extend them. Today, I will address Section 203, and in particular, sections 203(b) and 203(d) of the Patriot Act. Both of these provisions are slated to sunset on December 31, 2005, and both deserve to be made permanent. I seek to share with you, from my perspective as a career prosecutor, how critical these provisions have been in addressing terrorist threat information, criminal investigations and the manner in which our counterterrorism mission has been performed on a daily basis.

INFORMATION-SHARING GENERALLY

Section 203 of the Act authorizes information sharing between law enforcement and the intelligence community. As such, it complements and is complemented by other provisions of the Patriot Act that facilitate such information sharing, most notably Sections 218 and 504. These provisions collectively have knocked down the so-called "Wall" between law enforcement and intelligence—a wall that impeded our efforts to combat international terrorism. Prior to the Patriot Act, widespread misunderstandings about the "Wall" hindered the flow of information in two directions: it hindered intelligence information from being passed to prosecutors, and it also hindered prosecutors and criminal investigators from sharing certain types of law enforcement information with the intelligence community and other national security officials. Section 203 of the USA Patriot Act was enacted to deal with the latter problem, and to ensure that valuable foreign intelligence collected by the law enforcement community can be shared with the intelligence and national security communities, under appropriate safeguards.

Mr. Chairman, you do not have to take my word on the importance of keeping that Wall down and allowing the smooth flow of terrorism-related information to appropriate agencies across the Executive Branch. The bipartisan 9/11 Commission not only called for increased information sharing within the Executive Branch, it unanimously recognized that "[t]he provisions in the [Patriot] Act that facilitate the sharing of information . . . between law enforcement and intelligence appear, on balance, to be beneficial."[1] United States Attorney Patrick Fitzgerald has given compelling testimony to Congress on the "bizarre and dangerous" complications that

[1] *The 9/11 Commission Report,* at 394 (authorized ed.).

the "Wall" caused in major terrorism cases prior to 9/11.[2] And Director Mueller testified earlier this month that "the information-sharing provisions are consistently identified by FBI field offices as *the most important provisions in the Patriot Act.* The ability to share crucial information has significantly altered the landscape for conducting terrorism investigations, allowing for a more coordinated and effective approach" (emphasis added).[3]

Indeed, a telling example as to the importance of these information sharing provisions comes from outside the United States. A few weeks ago I met with counterterrorism officials in the law enforcement and intelligence community of one of our foreign partners. After discussing the information sharing provisions under the Patriot Act, these experienced practitioners observed that the provisions result in the following key practical consequences: (1) prosecutors are involved at the earliest stages of national security investigations; (2) the government uses a task force approach, maximizing the utility of the provisions; and (3) the provisions increase the flexibility and types of investigative techniques which can be used in a national security investigation. These developments increase the options available to decision-makers, enable them to make more informed choices and to make those choices in a more timely fashion. Hence, the legislation you have enacted in order to allow United States officials to share information is being studied by many of our partners in the international community and is paving the way for similar information sharing provisions to be incorporated into foreign laws and practices.

THE PATRIOT ACT CHANGES

Let me briefly review the Patriot Act changes contained in Section 203. Section 203(a) of the Patriot Act amended Rule 6(e) of the Federal Rules of Criminal Procedure to authorize the sharing of grand jury information involving foreign intelligence, counterintelligence, or foreign intelligence information, with a Federal intelligence, protective, immigration, national defense, or national security official.

Section 203(b) of the Act authorizes law enforcement officials to share the contents of communications that were lawfully intercepted by a judicially authorized wiretap (commonly known as "Title III information") with a federal law enforcement, intelligence, protective, immigration, national defense, or national security official, to the extent that the communications include foreign intelligence, counterintelligence, or foreign intelligence information. As with grand jury information, the disclosure can only be made to assist the recipient in the performance of his or her official duties, and the recipient may only use the information as necessary in the conduct of those duties.

Section 203(c) of the Act requires the Attorney General to establish procedures for the disclosure of the information pursuant to sections 203(a) and 203(b) when the information identifies an American citizen or other "United States person." The Attorney General has promulgated these procedures, and they require that information identifying a United States person be handled in accordance with special protocols that place significant limitations on the retention and dissemination of such information.[4]

Finally, section 203 also recognizes that criminal investigators may acquire information useful to the larger intelligence and national security communities by the use of other law enforcement techniques apart from grand juries and criminal investigative wiretaps. For example, a member of the public may walk into an FBI office and provide information on the location of an international terrorist, or the FBI may discover such information while conducting an interview or executing a search warrant. Section 203(d) of the Act authorizes the sharing of foreign intelligence, counterintelligence, or foreign intelligence information, that is obtained as part of a criminal investigation, with a federal law enforcement, intelligence, protective, immigration, national defense, or national security official. As with grand jury and Title III information, the disclosure can only be made to assist the recipient in the performance of his or her official duties, and the recipient may only use that information as necessary in the conduct of those official duties.

---

[2] See Testimony of the Honorable Patrick Fitzgerald before the Senate Judiciary Committee (Oct. 21, 2003).

[3] Testimony of FBI Director Robert Mueller before the Senate Judiciary Committee (Apr. 5, 2005).

[4] Memorandum of the Attorney General, Guidelines for Disclosure of Grand Jury and Electronic, Wire, and Oral Interception Identifying United States Persons (Sept. 23, 2002).

PATRIOT ACT RESULTS AND CHANGED GOVERNMENT PRACTICES

Pursuant to the Patriot Act, intelligence emanating from criminal investigations has indeed been routinely shared, and is shared routinely, with other appropriate government officials. Some examples of intelligence information developed in a criminal case which was shared with the intelligence community under Section 203(d) include the following:

- Information about the organization of a violent jihad training camp including training in basic military skills, explosives, and weapons, as well as a plot to bomb soft targets abroad, resulted from the investigation and criminal prosecution in New York of a naturalized United States citizen who was associated with an al-Qaeda related group;
- Travel information and the manner that monies were channeled to members of a criminal conspiracy in Portland who traveled from the United States intending to fight alongside the Taliban against U.S. and allied forces;
- Information about an assassination plot, including the use of false travel documents and transporting monies to a designated state sponsor of terrorism, resulted from the investigation and prosecution in Northern Virginia of a naturalized United States citizen who had been the founder of a well-known United States organization;
- Information about the use of fraudulent travel documents by a high-ranking member of a designated foreign terrorist organization emanating from his criminal investigation and prosecution in Washington, D.C., revealed intelligence information about the manner and means of the terrorist group's logistical support network which was shared in order to assist in protecting the lives of U.S. citizens;
- The criminal prosecution of individuals from Lackawana, New York, who traveled to, and participated in, a military-style training camp abroad yielded intelligence information in a number of areas including details regarding the application forms which permitted attendance at the training camp; after being convicted, one defendant has testified in a recent separate federal criminal trial about this application practice, which assisted in the admissibility of the form and conviction of the defendants;
- The criminal prosecution in Northern Virginia of a naturalized U.S. citizen who had traveled to an al-Qaeda training camp in Afghanistan revealed information about the group's practices, logistical support and targeting information.

Title III information is similarly being shared. The potential utility of such information to the intelligence and national security communities is obvious: suspects whose conversations are being monitored without their knowledge may reveal all sorts of information about terrorists, terrorist plots, or other activities with national security implications. Furthermore, the utility of this provision is not theoretical: the Department has made disclosures of vital information to the intelligence community and other federal officials under section 203(b) on many occasions, such as:

- Wiretap interceptions involving a scheme to defraud donors and the Internal Revenue Service and illegally transfer monies to Iraq generated not only criminal charges in Syracuse, New York but information concerning the manner and means by which monies were funneled to Iraq;
- Intercepted communications, in conjunction with a sting operation, led to criminal charges in New York and Arkansas and intelligence information relating to money laundering, receiving and attempting to transport night-vision goggles, infrared army lights and other sensitive military equipment relating to a foreign terrorist organization.

Last year, during a series of high-profile events—the G–8 Summit in Georgia, the Democratic Convention in Boston and the Republican Convention in New York, the November 2004 presidential election, and other events—a task force used the information sharing provisions under Section 203(d) as part and parcel of performing its critical duties. The 2004 Threat Task Force was a successful inter-agency effort involving robust sharing of information at all levels of government.

And the FBI relies upon section 203(d) to provide information obtained in criminal investigations to analysts in the new National Counterterrorism Center, thus assisting the Center in carrying out its vital counterterrorism missions. The National Counterterrorism Center represents a strong example of section 203 information sharing, as the Center uses information provided by law enforcement agencies to produce comprehensive terrorism analysis; to add to the list of suspected terrorists

on the TIPOFF watchlist; and to distribute terrorism-related information across the federal government.

The information sharing provisions not only promote a culture of teamwork and trust they provide government officials certainty in the performance of their duties. In that regard, it should be noted that section 203 must be read in conjunction with section 905 of the Patriot Act, which generally requires that federal law enforcement agencies share foreign intelligence acquired in the course of a criminal investigation with the intelligence community, "[e]xcept as otherwise provided by law. . . ." As the Attorney General pointed out in Guidelines implementing section 905, section 203(d) makes it clear that no other federal or state law operates to prevent the sharing of such information so long as the disclosure will assist the recipients in the performance of their official duties.[5] Thus, under current law, the duty to share information under section 905 is clear. However, if section 203(d) is allowed to sunset, then each law enforcement agency's authority and duty to share foreign intelligence under section 905 may have to be reevaluated and this change might lead to unnecessary uncertainty and confusion regarding the force and effect of section 905.

These changes, and other portions of the Patriot Act, have appropriately led to changes in Department of Justice procedures and guidelines. For example, under the Attorney General's National Security Investigation Guidelines, revised on October 31, 2003, the FBI has an ongoing obligation to share investigative information from national security files with the Criminal Division and relevant United States Attorneys' Offices. In turn, the United States Attorneys and Anti-Terrorism Advisory Council Coordinators must be prepared at any time to discuss the availability of criminal charges in any international terrorism investigation within their district.

These provisions have been used repeatedly and are now a critical tool in our counterterrorism enforcement program. As Attorney General Gonzales noted in his testimony earlier this month, prosecutors in every district have worked with Joint Terrorism Task Forces over the last three years to thoughtfully and painstakingly review historical and current intelligence files to determine whether there was a basis for bringing criminal charges against the subjects of intelligence investigations. Literally, thousands of files were reviewed and criminal matters were pursued. The criminal cases that were filed were brought only after a full discussion as to whether criminal action was more appropriate, at that time, than continuing with covert intelligence collection. Some national security matters have continued as intelligence investigations, thereby protecting critical sources and methods. We collectively understand, and train, that the goal is prevention, not just bringing criminal prosecutions. We seek to preserve a criminal option, if it is possible, and ensure that the threat information is timely and effectively shared.

ADDITIONAL CONGRESSIONAL LEGISLATION

The counterterrorism community needs to pool what it knows. Indeed, that is the fundamental construct underlying many provisions of the Intelligence Reform and Terrorism Prevention Act of 2004, which was enacted by Congress just four months ago. Building upon Section 203 of the Patriot Act, provisions of the Intelligence Reform Act further expanded Federal Rule of Criminal Procedure 6(e)(3)(D) to permit an attorney for the government to disclose any grand jury matter involving international terrorism, a threat of attack or other grave hostile acts. The persons to whom this may be disclosed includes not only United States officials—including federal and state officials—but also foreign government officials "for the purpose of preventing or responding to such threat or activities." The description in the December 2004 legislation of what may be disclosed is modeled after the definition of "foreign intelligence information" used in the Patriot Act three years earlier. In light of these necessary and welcome actions by Congress in the Intelligence Reform Act, it would be incongruous to now remove the foundations from which these recent changes arise.

Similarly, after the enactment of the Patriot Act, the Homeland Security Act added two information sharing provisions to Title III. One provision (codified at 18 U.S.C. 2517(7)) authorizes the sharing of Title III information with a foreign investigative or law enforcement officer to the extent that such disclosure is appropriate to the performance of official duties. Therefore, were section 203(b) allowed to expire, United States law enforcement officers would be allowed to share certain foreign information collected through criminal investigative wiretaps with foreign intelligence services, such as MI–5, but would arguably not be allowed to share that

[5] Memorandum of the Attorney General, Guidelines Regarding Disclosure to the Director of Central Intelligence and Homeland Security Officials of Foreign Intelligence Acquired in the Course of a Criminal Investigation (Sept. 23, 2002).

same information with the CIA. And the second provision (codified at 18 U.S.C. 2517(8)) authorizes disclosure of Title III information to any appropriate federal, state, local or foreign government official to prevent or respond to a threat of attack, international terrorism, or other grave hostile acts. All of these provisions reflect Congress' continuing efforts to ensure information sharing between federal law enforcement officials and other appropriate officials.

PROTECTING PRIVACY AND CIVIL LIBERTIES

Section 203 fully protects legitimate privacy and civil liberties interests through its controls on disclosure and use, and its special protections for information identifying a U.S. person. For example, section 203(b) does not allow carte blanche disclosure of sensitive information. The information itself can only be acquired in the first place pursuant to the strict demands of Title III, and section 203(b) does not in any way diminish or minimize those requirements. Second, the only information that can be shared with intelligence or national security personnel is that which satisfies the statutory definitions of "foreign intelligence," "counterintelligence," or "foreign intelligence information."[6] This requirement acts as a filter to prevent the unnecessary disclosure of extraneous information. Third, the disclosure can only be to designated federal officials, and solely for their official use. And finally, as described above, identifying information about U.S. persons is subject to special restrictions. For all these reasons, section 203(b) correctly and appropriately facilitates a unified, cohesive counterterrorism effort while also safeguarding privacy.

Section 203(d) also protects privacy. Although historically grand jury and Title III information have been treated as more sensitive than other types of law enforcement information, section 203(d) disclosure is circumscribed in much the same way as disclosure of grand jury and Title III information under sections 203(a) and 203(b). In particular, disclosure is only authorized if: (1) the information consists of foreign intelligence, counterintelligence, or foreign intelligence information; (2) the recipient is another federal law enforcement, intelligence, protective, immigration, national defense, or national security official; and (3) the disclosure is meant to assist the recipient in the performance of his or her official duties. Moreover, as with grand jury and Title III information, the recipient may only use the information as necessary in the conduct of those official duties.

CONCLUSION

No one should be lulled into a sense of complacency by al Qaeda's inability—so far—to mount another catastrophic attack on the U.S. homeland. Prior to 9/11, we tied ourselves in knots with misunderstood legal and bureaucratic guidelines that had the effect of constricting the flow of essential information within the United States Government. We dare not, and must not, let this happen again. Taken together, these provisions are crucial to the government's efforts to prevent and preempt terrorist attacks. We cannot put artificial barriers between law enforcement agencies and entities such as the new National Counterterrorism Center when it comes to the sharing of law enforcement information that has foreign intelligence value.

Mr. Chairman, as you debate these issues, we invite your questions, your comments, and your suggestions. We very much want to work with Congress to ensure that we will keep America safe and free. Sections 203(b) and 203(d) are helping us fight the terrorists in a manner that respects the Constitution and constitutional values. This Congress should permanently renew Sections 203(b) and 203(d) of the Patriot Act, as well as other essential provisions of the Act.

---

[6] "Foreign intelligence" means information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. "Counterintelligence" means information gathered, and activities conducted, to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.

"Foreign intelligence information" means

(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against (I) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (II) sabotage or international terrorism by a foreign power or an agent of a foreign power; or (III) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to (I) the national defense or the security of the United States; or (II) the conduct of the foreign affairs of the United States.

I again thank the Committee for holding this hearing. I will do my best to answer your questions.

Mr. COBLE. Thank you, Mr. Chairman. We have been joined by our friends from California, Ohio, and Texas: Mr. Lungren, Mr. Chabot, and Mr. Gohmert. Good to have you all with us.

Mr. Edgar.

TESTIMONY OF TIMOTHY H. EDGAR, NATIONAL SECURITY POLICY COUNSEL, AMERICAN CIVIL LIBERTIES UNION

Ms. EDGAR. Thank you very much, Mr. Chairman, Ranking Member Scott, Members of the Subcommittee. I am very pleased to be here at this hearing on information sharing and sections 203(b) and (d) of the PATRIOT Act.

We are here today at the tenth anniversary of the terrible bombing of the Oklahoma City Federal Building, a horrendous crime that was one reason I sought a career in the national security field, grappling with the very difficult questions involved in protecting ourselves against terrorism, while keeping our basic rights and freedoms.

While the PATRIOT Act passed by wide margins, Members on both sides were right to worry about civil liberties, and wisely included a sunset clause. The sunset allows us to go look back at the PATRIOT Act, and try to do a better job. Whatever powers Congress authorizes we're going to need to live with for a long time. Terrorism, whether home-grown or international, is certainly not going away.

This hearing is about two provisions that sunset. They allow sharing of information—criminal wiretap information under 203(b), and general criminal information under 203(d)—with both U.S. Government intelligence agencies and foreign government agencies. The ACLU supports information sharing to ensure investigators connect the dots, but with appropriate safeguards to protect civil liberties.

Without oversight, uncontrolled sharing of criminal information with intelligence agencies poses a real risk that Federal agents will use search warrants, wiretaps, and subpoenas to chill freedom of speech and association, with a criminal probe serving merely as a pretext for an intelligence investigation.

Let me explain. A series of raids in Northern Virginia in March 2002 of non-profit organizations and private homes sent shock waves through a community and targeted some of its prominent Muslim American organizations and leaders. The warrants were extremely broad. They sought all information, correspondence, pamphlets, leaflets, booklets, video and audio tapes "referencing in any way" anyone designated as a terrorist—a warrant which the ACLU of Virginia was right to challenge as reminiscent of the general warrants that contributed to the American Revolution.

It is no surprise that agents seized thousands of documents and other items of first amendment value. No charges have been brought against these organizations; nor have their assets been frozen. The property has now been returned, and the attorney for the organizations has been told her clients are no longer under investigation for terrorism financing at all.

A Federal civil rights case has been filed alleging serious abuses of constitutional rights, including that the search warrant affidavit included fabricated facts, and that the warrants were executed without regard for constitutional rights.

Some Federal officials have characterized this investigation as an intelligence probe designed to gather information, rather than to enforce the law. This justification strongly suggests that the material has been copied and shared with intelligence agencies, under section 203(d) of the PATRIOT Act, and that they also have been shared with the intelligence agencies of foreign governments.

Possible sharing of this information with foreign governments is particularly troubling, given the dissidents involved with these organizations; for example, Dr. Jamal Barzingi, an Iraqi-American leader who was invited to advise the Iraqi governing council.

The raids did not affect only the Muslim American community. The warrants also included a rural Georgia chicken processing company with 1,200 employees, as a result of the PATRIOT Act's nationwide search power.

We agree that Congress should use the 9/11 Commission's test for PATRIOT Act powers: A, that the power actually materially enhances security and, B, that there is adequate supervision of the Executive's use of these powers to ensure protection of civil liberties.

If Congress is satisfied that these provisions, section 203(b) and (d), meet that first test of enhancing security, it still must consider checks and balances on the Executive Branch, to better protect civil liberties.

The Justice Department says civil liberties are protected by Attorney General guidelines. As I explain in my written statement, it is not clear what, if any, real protection the guidelines provide, because they authorize the sharing of exactly that kind of information which the statute itself authorizes to be shared.

We propose that the notice requirement of section 203 should be broadened from just grand jury information to include all criminal investigative information shared with intelligence agencies, and that notice should be beefed up. We're proposing that notice should include a statement of the good-faith basis for the criminal investigation, and provide some update as to its progress. If no charges are filed, a notice should be filed with the court, explaining why. Court-filed notice, we believe, could serve as a check on the abuse of the criminal process for intelligence gathering fishing expeditions.

We also urge that notice should be provided to Congress, as well; and that Congress should consider reauthorizing some of the provisions of the PATRIOT Act, including sections 203(b) and (d), for some additional temporary period of time, so they can have additional reporting and consider again how these are being used, rather than making them permanent.

Stronger safeguards may be needed to protect privacy. I'd like to refer to the Committee an article written by my colleague Kate Martin, director of the National Security Studies Center, in an ABA series called "Patriot Debates," that suggests some further ideas.

I thank you for this opportunity to testify. And since I have 40 seconds remaining, one of the——

Mr. COBLE. Mr. Edgar, you actually have more than that, because we were late. So you have about a minute and a half remaining.

Mr. EDGAR. Well, I may be the only witness not to use all of that. I do want to say that I agree with the witnesses for the Government that the wall was largely the result of widespread misunderstandings about the wall. And I certainly want to make sure that Government agents have a clear understanding of their ability to share this information.

But I do think that we can work together to create appropriate safeguards that will allow us a check against the misuse either of the criminal process for intelligence ends, or of the intelligence process for criminal ends. Thank you very much.

[The prepared statement of Mr. Edgar follows:]

PREPARED STATEMENT OF TIMOTHY H. EDGAR

Chairman Coble, Ranking Member Scott and Members of the Subcommittee:

I am pleased to appear before you today on behalf of the American Civil Liberties Union and its more than 400,000 members, dedicated to preserving the principles of the Constitution and Bill of Rights, at this important oversight hearing concerning information sharing and sections 203(b) and (d) of the USA PATRIOT Act of 2001.[1]

The Patriot Act was passed by Congress in 2001 just six weeks after the terrorist attacks of September 11. Although the act passed by wide margins, members on both sides of the aisle expressed reservations about its impact on fundamental freedoms and civil liberties. As a result, Congress included a "sunset clause" providing that over a dozen provisions will expire on December 31, 2005, if Congress does not act to renew them.

This hearing addresses two provisions of the Patriot Act that will expire if they are not renewed—sections 203(b) and (d). These provisions authorize sharing of information acquired in criminal investigations with intelligence agencies. Section 203(b) specifically authorizes sharing of criminal wiretap information, while section 203(d) provides general authority to share information acquired in criminal investigations "notwithstanding any other provision of law."

The ACLU supports information sharing concerning terrorism to ensure investigators can and do "connect the dots" to prevent terrorist attacks, with appropriate safeguards required to protect civil liberties. The National Commission on Terrorist Attacks Upon the United States ("9/11 Commission") found that, prior to September 11, 2001, intelligence and security agencies did not properly share information in a number of key instances. In most cases, there appears to have been no legal barrier preventing such sharing.

Nevertheless, uncontrolled sharing of criminal investigative information with intelligence agencies poses real risks to civil liberties. The most acute danger is that federal prosecutors and law enforcement agents will be transformed from law enforcement officials concerned with preventing and punishing criminal activities into a domestic spy network directed at unpopular religious and political organizations.

Using criminal search warrants, wiretaps, and subpoenas, federal investigators can severely chill constitutionally-protected freedom of speech and association if they aggressively probe religious and political organizations on the basis of a criminal probe that is really only a pretext for an intelligence investigation.

Federal law gives the FBI and other agencies wide latitude in conducting criminal investigations. Those who have been mistakenly investigated by the federal government can attest that the investigation alone, even without any formal charges or accusations, can lead to the loss of a job, business, and reputation.

The intense focus of criminal money laundering and terrorism financing investigations on Muslim organizations, think tanks and charities since September 11 illustrates both the benefits and the dangers of wider information sharing. The Justice Department, in its recent report on the Patriot Act, states it has used section 203(b)

[1] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107–56, 115 Stat. 272.

"on many occasions . . . to track terrorists' funding sources and identify terrorist operatives overseas."[2] The danger is that intensive criminal investigations, if undertaken without a good faith basis for bringing criminal charges, will severely chill legitimate political, religious and academic activities.

A series of raids in Northern Virginia in March 2002 of non-profit organizations and private homes terrorized a community and targeted some of the most prominent and well respected Muslim organizations and citizens of the United States. No money laundering or terrorism financing charges have been brought against these organizations or their officers in over three years. Some federal officials have characterized the investigation as an "intelligence probe" designed to gather information rather than to enforce the law.

More meaningful judicial oversight could help preserve the benefits of information sharing while providing greater protection for civil liberties. Currently, the only protection for civil liberties for most criminal investigative information consists of Attorney General guidelines that provide little, if any, real protection against abuse.

NORTHERN VIRGINIA RAIDS: CRIMINAL INVESTIGATION OR INTELLIGENCE "FISHING EXPEDITION"?

In a series of raids in March 2002 in Northern Virginia, federal agents seized confidential files, computer hard drives, books, and other materials from some of the most respected Islamic think tanks and organizations in the United States and raided the homes of many of the leaders involved in those organizations.

The search warrants targeted two entities whose main purpose involves activities at the core of the First Amendment: the Graduate School of Islamic Thought and Social Sciences (GSITSS), an institute of higher education, and the International Institute of Islamic Thought (IIIT), an Islamic research institute and think tank, as well as the private homes of a number of their employees and scholars.

The warrants sought a number of First Amendment-protected materials that clearly lack any apparent connection to an investigation of money laundering or terrorism financing. These include:

- Any and all information or correspondence "referencing in any way" any individual or entity designated as a terrorist by the President of the United States, the United States Department of Treasury, or the Secretary of State,
- "Pamphlets, leaflets, booklets, video and audio tapes related to" any such individual or entity, and
- *"All* computers" and related equipment and software.[3]

Given the breadth of the search warrants, it is no surprise the agents seized thousands of documents and other items of First Amendment value, including books, binders, computer disks, scholarly manuscripts, audio and videotapes, and mail delivered while the search warrant was being executed. Agents even seized "Sunday school emergency forms."[4]

Indeed, as the ACLU of Virginia pointed out in its amicus filing in this case, given the magnitude of the terrorism problem and its effect on the Islamic world, it would extremely surprising *not* to find documents "referencing in any way" terrorist organizations (such as by, for example, condemning the attacks of September 11) at any American institution studying contemporary Islam or engaging in advocacy on behalf of Muslim Americans.

A federal civil rights action filed by the family of Dr. Unus, an employee of the IIIT, includes several serious changes of wrongdoing during the simultaneous raid of their home. The complaint alleges that agents demanded entry with weapons drawn and without immediately identifying themselves as federal agents, did not allow Dr. Unus' wife to review the search warrant, took items not specified in the warrant, handcuffed Dr. Unus' wife and daughter for hours, and did not allow them to cover themselves as required by their faith.[5]

The raids sent shock waves through the Northern Virginia Muslim American community. The institutions targeted included some of the most established and well-respected Muslim American organizations and leaders, citizens of the United States

---

[2] United States Dep't of Justice, *USA PATRIOT Act: Sunsets Report* (April 2005)

[3] *See* Brief Amicus Curiae of the American Civil Liberties Union of Virginia, Inc., In Support of Motion for Return of Property and to Unseal the Search Warrant Affidavit, *In the Matter of the Search of 750A Miller Drive et al.,* No. 02–MG–122 (E.D. Va. 2002) (emphasis added), attached to this testimony as appendix A.

[4] *Id.*

[5] *See* Complaint in *Aysha Nudrat Unus and Hanaa Unus v. David Kane and Rita Katz,* Civ. No. 04–312–A (E.D. Va. filed Nov. 9, 2004) ¶¶ 47–63.

who have lived in this country since the 1970's. Would indictments soon show that established organizations like the GSITSS or the IIIT were really fronts for terrorism financing?

In a word: no. More than three years following the raids, there have been no criminal charges brought against the GSITSS, the IIIT, or any of their officers or directors. The GSITSS and the IIIT have not had their assets seized or funds frozen. No evidence has emerged that any of their assets were ever used to fund terrorism. All the files, computers and other property seized in the raids has been returned, although the government retains copies of them. The attorney for the GSITSS and the IIIT, Nancy Luque, has been told by the FBI that her clients are no longer under investigation for any terrorism financing or other terrorism-related charges.

The complaint in the civil rights action says the affidavit in support of the search warrants contained fabricated material facts regarding non-existent overseas transactions. The complaint also says the search warrant affidavit was drafted with the help of private author and self-styled "terrorist hunter" Rita Katz, who was paid $272,000 for her advice by the federal government and has made much more in a book deal and as a consultant for news organizations.[6] According to federal investigators, Katz "lost the trust of some investigators from the FBI and Justice Department" as a result in part of the "reckless conclusions" she drew in her book.[7]

According to the *Washington Post,* federal officials have sought to justify the raids "as an 'intelligence' probe, designed not necessarily to yield criminal charges but to track possible terrorist activity."[8] This justification strongly suggests that the material seized in the March 2002 raids has been copied and shared with intelligence agencies under section 203(d) of the Patriot Act. As a result of amendments made to section 203(d) of the Patriot Act by the Homeland Security Act,[9] the material may also have been shared with the intelligence agencies of foreign governments. As a result, it is at least possible the intelligence agencies of Syria, Saudi Arabia, or Egypt have been given some or all of the confidential files of the IIIT or the GSITSS, whose officers, directors and scholars have included prominent dissidents and scholars who seek to integrate Islam with an agenda for democratic reform. For example, Dr. Jamal Barzingi, a member of the board of the IIIT, prominent Muslim scholar and Iraqi-American, is a leading advocate of democratic reform. Dr. Barzingi was invited to advise the Iraqi Governing Council following the toppling of Saddam Hussein's regime in 2003.

The raids in Northern Virginia did not affect only the Muslim community. The search warrants also included authorization to search the offices of Mar-Jac Poultry, Inc., a Gainesville, Georgia chicken processing company that produces halal chicken—chicken prepared under Islamic law. The search warrants were approved in the Eastern District of Virginia under the new nationwide search warrant power authorized by section 219 of the Patriot Act. Mar-Jac Poultry is a longstanding poultry business founded in 1948. It currently employs 1200 workers. No charges have been brought against Mar-Jac or any of its employees in over three years, but its reputation in the community has suffered a severe blow as a result of the raids and attendant publicity.[10]

In a landmark case in 1965, the Supreme Court considered a criminal search warrant allowing the seizure of "any books, records, pamphlets, cards, receipts, lists, memoranda, pictures, recordings, or any written instruments concerning the Communist Party of Texas and the operations of the Communist Party of Texas."[11] The Supreme Court struck down the warrant, saying search warrants should be "accorded the most scrupulous exactitude when the 'things' are books, and the basis for their seizure is the ideas they contain."[12]

---

[6] *See id.* ¶¶ 12–34.

[7] *See* Marc Perelman, *Muslim Charities Sue CBS, Investigator,* The Forward, June 13, 2003.

[8] Jerry Markon, *Affidavit Unsealed From Muslim Probe,* Washington Post, Aug. 1, 2003, at A6.

[9] Homeland Security Act of 2002, § 897, Pub. L. No. 107–296, 116 Stat. 2135, 2257–58 (codified at 50 U.S.C. § 403–5d). Section 897 amends the general authority for sharing of criminal investigative information, such as the fruits of the search warrants executed in Northern Virginia, to include "any appropriate Federal, State, local, or *foreign government official*" *See id.* (emphasis added). The standards are somewhat narrower than for disclosure to United States intelligence agencies. Other provisions of the Homeland Security Act extend sections 203(a) and (b) to authorize the sharing of grand jury information and the fruits of criminal electronic surveillance with the intelligence agencies of foreign governments. *See id.* at §§ 895, 896.

[10] *See* Bill Torpy, *Poultry Company Sues CBS over Terrorism Story,* Atlanta Journal-Constitution, July 6, 2003.

[11] *Stanford v. Texas,* 379 U.S. 476, 486 (1965).

[12] *Id.* at 485.

As the Supreme Court has observed, "The Bill of Rights was fashioned against the background of knowledge that unrestricted power of search and seizure could also be an instrument for stifling liberty of expression."[13] The use of criminal investigative powers for intelligence-gathering "fishing expeditions" poses real dangers to civil liberties.

SHOULD CONGRESS REAUTHORIZE SECTION 203(B) AND (D)?

Before re-authorizing any expiring power, this subcommittee should require the Executive Branch to meet the standard articulated by the bipartisan 9/11 Commission:

- First, Congress should examine the provisions to determine whether the government can show "(a) that the power actually materially enhances security and (b) that there is adequate supervision of the executive's use of the powers to ensure protection of civil liberties."[14]
- Second, "[i]f the power is granted, there must be adequate guidelines and oversight to properly confine its use."[15]

Only an intensive and painstaking process of examining the facts regarding the use of these powers can answer these questions.

Until now, the government has fallen short on specifics. For example, the discussion of sections 203(b) and (d) in the Justice Department's "sunsets reports" does not describe any specific cases.[16] Just last week, Senate Judiciary Chairman Arlen Specter expressed frustration at the Justice Department's inability to provide specific facts about the Patriot Act even in a classified setting. "This closed-door briefing was for specifics," Senator Specter explained. "They didn't have specifics."[17]

The Justice Department claims civil liberties are adequately protected by Attorney General guidelines governing the sharing of criminal grand jury and wiretap information mandated by section 203(c) of the Patriot Act (a provision not subject to the sunset provision).[18] These guidelines require information concerning United States persons to be labeled and treated in accordance with Executive Order 12333, which authorizes the intelligence community to "collect, retain or disseminate" information about U.S. persons where such information meets the definition of "foreign intelligence or counterintelligence" as well as for a host of other reasons.[19] As section 203 of the Patriot Act authorizes sharing specifically of foreign intelligence and counterintelligence information, it is not clear what, if any, additional protection the Attorney General guidelines provide.

If the government can show that sections 203(b) and (d) "actually materially enhance[] security," the danger to free expression from the misuse of criminal powers points to the need for stricter supervision of the Executive Branch than is provided by the guidelines.

Section 203(a) of the Patriot Act permits sharing of otherwise confidential "matters occurring before the grand jury" with intelligence officials, but also requires notice to the court "[w]ithin a reasonable time after such disclosure. . . ." Section 203(a) is not subject to the sunset clause.

The notice requirement of section 203(a) should be broadened from grand jury information to include all criminal investigative information shared with intelligence agencies, and notice should be made more meaningful. For example, notice to the court should include a statement of the good faith basis for the criminal investigation and provide some update as to the progress of that investigation. The notice should also be supplemented with a report on the disposition of the criminal investigation if no charges are brought. Such a requirement will serve as a valuable check on abuse of the criminal process for intelligence "fishing expeditions."

A stronger notice requirement could also aid in Congressional oversight. Congress should consider reauthorizing some provisions of the Patriot Act, including sections 203(b) and (d), for some additional period of time, rather than making them perma-

---

[13] *Marcus v. Search Warrants of Property at 104 East Tenth St.,* 367 U.S. 717, 729 (1961).

[14] Final Report of the National Commission on Terrorist Attacks Upon the United States ("The 9/11 Commission Report") 294–95 (2004) (boldfaced recommendation)

[15] *Id.*

[16] *See* sunsets report, *supra* n. 2.

[17] Eric Lichtblau, *Specter Voices Frustration Over Briefing on Patriot Act,* N.Y. Times, Apr. 13, 2005.

[18] Memorandum of the Attorney General, Guidelines for Disclosure of Grand Jury and Electronic, Wire and Oral Interception Information Identifying United States Persons, Sept. 23, 2002, available at: *http://www.usdoj.gov/olp/section 203.pdf*

[19] Exec. Order 12333, 46 Fed. Reg. 59941 (Dec. 4, 1981) (set out as a note following 50 U.S.C.A. § 401), at § 2.3

nent. Congress could include reporting requirements that would provide it with the same information a stronger notice requirement would provide to the federal courts.

CONCLUSION

This subcommittee's review of the Patriot Act and related legal measures in the ongoing effort to combat terrorism is needed to ensure continued public support for the government's efforts to safeguard national security. The controversy over the Patriot Act reflects the concerns of millions of Americans for preserving our fundamental freedoms while safeguarding national security. To date, resolutions in opposition to parts of the Patriot Act and other actions that infringe on fundamental rights have been passed in in 377 communities in 43 states including five state-wide resolutions. These communities represent approximately 56.9 million people who oppose sections of the Patriot Act.

Such widespread concern, across ideological lines, reflects the strong belief of Americans that security and liberty need not be competing values. Congress included a "sunset provision" precisely because of the dangers represented by passing such far-reaching changes in American law in the aftermath of the worst terrorist attack in American history. Now is the time for Congress to complete the work it began when it passed the Patriot Act, by bringing the Patriot Act back in line with the Constitution.

I thank you for this opportunity to testify and look forward to taking any questions you may have.

Mr. COBLE. Thank you, Mr. Edgar. And we have been joined by our friend from California, the gentlelady Ms. Waters. Good to have you with us.

Now, folks, as I said to you all earlier, we have the 5-minute rule against us, as well, so if you all could keep your answers as terse as possible.

Mr. McCaul, in your experience in the Western District of Texas, how have sections 203(b) and (d) affected the wall between law enforcement agencies and the Intelligence Community, A? And, B, if we don't authorize these two sections, what is your response to that?

Mr. MCCAUL. Thank you, Mr. Chairman. As I said in my testimony, when the wall came down it opened up the sharing of information between the Intelligence Community and the criminal division and the prosecutors. It has facilitated a nationwide effort to protect this country, because it's opened up information from all jurisdictions in the United States so we can freely share information.

In fact, the FBI was, in my view, somewhat compartmentalized before this wall came down. Now the FBI is able to e-mail, for instance, to itself, and fully communicate, and then fully communicate with the prosecutors, as well.

To answer your question, "What would happen?", if these two provisions are not reauthorized, in my view, it will resurrect, or erect, the wall again; which I believe would be the most disastrous thing that could happen to this country, given the examples that I talked about in my testimony between the Osama bin Laden investigation and the Wen Ho Lee investigation, the investigation into China, and other cases that I've illustrated in my testimony.

In addition, I think the President's National Counterterrorism Center would be severely damaged by the—if this is not reauthorized; in the sense that this information could not freely flow within the Federal Government.

Mr. COBLE. I thank you, sir. Ms. Baginski, do you believe the need to share information between criminal investigators and intelligence investigators is likely to end soon, or do you believe these provisions will be needed for some extended time and should be

made permanent? And by the way, I think you could make convincing arguments for permanent and sunset. But let me hear from you.

Ms. BAGINSKI. Sir, yes, I believe this will be around for some time, and that's because of the nature of the threat. And I would just offer up an example of looking at the situation in Spain, for example. You had radical Moroccans who entered Spanish society; made their living through drug trafficking and counterfeiting compact discs; bought the telephones from a known criminal international enterprise; bought the explosives from a local known criminal enterprise; stole a truck; and blew up passenger trains in Madrid. And my question is: Is that a criminal activity, or a terrorist activity?

Mr. COBLE. I thank you. Mr. Sabin, Mr. Edgar in his testimony, in his written testimony, referred to a series of raids in Northern Virginia in 2002, early 2002, that targeted prominent Muslim organizations and citizens. And he further indicated that no money laundering or terrorism financing charges have been brought against these organizations or their officers in over 3 years. What do you say to that? Or are you familiar with that?

Mr. SABIN. Yes, I am familiar with it. I would respectfully suggest that that is not an accurate representation of the investigation. There have been two defendants convicted in matters arising from that investigation.

Specifically, two search warrants were executed at the American Muslim Council and the American Muslim Foundation. The founder and president of those raided organizations, Mr. Alamoodi, was indicted, prosecuted, and convicted of terrorist financing related charges; specifically, violations of the International Emergency Economic Powers Act, immigration charges, and financial transactions involving state sponsors of terrorism, specifically Libya and Syria. He has pled guilty, and is cooperating with law enforcement.

Second, Soliman Biheiri was prosecuted on two occasions and convicted for false statements in application for naturalization; received a sentence in the Eastern District of Virginia; and then was prosecuted again relating to false statements relating to passport, obtaining that by fraud, as well as material false statements in violation of 1001; and was convicted and sentenced for those crimes.

In the search warrants, it related to his involvement in Hamas and the Palestinian Islamic Jihad, arising out of the racketeering indictment in Tampa, Florida, relating to Sami AlArian [ph] and others. That case is pending, and awaiting trial next month in Tampa, Florida. So there are two specific prosecutions that resulted from information from those searches.

With respect to the argument that Mr. Edgar made, I would suggest that it's not related to why we are here today—information sharing under section 203, but the fact that they made allegations regarding the predicate for obtaining those warrants. And I underscore that warrants were obtained through criminal process, at an article III court, by a United States District Judge, both for locations in Eastern District of Virginia and in Georgia. So——

Mr. COBLE. My red light is on, Mr. Sabin. Mr. Edgar, I'll examine you subsequently. I think we'll probably have a second round here.

Mr. SCOTT. Did you let Mr. Edgar respond to the question?

Mr. EDGAR. I would like to respond.

Mr. COBLE. Well, my red light's on. Without objection, I'll hear from you, Mr. Edgar.

Mr. EDGAR. Yes, I just wanted to make very clear that, as my written statement makes clear, I'm discussing the raids of two different organizations, the Graduate School for the Institute of the Study of Islamic Social Sciences, and the International Institute of Islamic Thought, and their officers and directors. That's the only case in which the ACLU of Virginia intervened. It's the one in which we were concerned about the over-breadth of the search warrants and the first amendment materials seized.

And I am advised by their attorney that there is no connection between their organization and the cases that were mentioned. You know, I think that there's no question that there have been cases where the Government has found some useful information, but I don't believe this was one of them.

Mr. COBLE. All right. I thank the gentleman.

The gentleman from Virginia, Mr. Scott.

Mr. SCOTT. Thank you, Mr. Chairman. I wanted to follow up on that kind of over-breadth issue, because we've heard the word "intelligence," and Ms. Baginski said that it involves those who would do us harm, and you need probable cause for a FISA warrant. That kind of implies that you need probable cause of a crime. And the Attorney General tried that out, too, the last time he was here, suggesting that you need probable cause for a crime for a FISA warrant. That's not actually true; is it?

Ms. BAGINSKI. No, sir. And if I made that suggestion, that was not what I intended.

Mr. SCOTT. Okay. Now, what do you need probable cause of to get a FISA warrant?

Ms. BAGINSKI. What do you need? That you have an agent of a foreign power that is intended to do you some harm.

Mr. SCOTT. Well, no, it's not trying to do you harm.

Ms. BAGINSKI. In the sense of, from my perspective—and pardon me if the phrase has caused us some concern——

Mr. SCOTT. Well, the phrase causes concern because what you need is probable cause that you can get some foreign intelligence.

Ms. BAGINSKI. Yes, sir.

Mr. SCOTT. Doesn't have anything to do with a crime. You're negotiating a trade deal——

Ms. BAGINSKI. From my perspective——

Mr. SCOTT. This is spying. I mean, if you're negotiating—from your perspective, but, you know, this is the over-breadth part.

Ms. BAGINSKI. No, I take your point, sir. The point——

Mr. SCOTT. If you have information that the agent of a foreign government that you're doing a trade deal with—you can tap his phone.

Ms. BAGINSKI. The point that I would make relative to FISA is that foreign intelligence is actually governed by a series of priorities that are set by the President. They emanate from the President. They are turned into foreign intelligence collection priorities. And those priorities outline his national security concerns.

Mr. SCOTT. When we're talking about over-breadth, you can get a FISA warrant if you've got probable cause that the guy's an agent of a foreign government, and you can get foreign intelligence which includes——

Ms. BAGINSKI. That's correct, sir.

Mr. SCOTT. —things that have nothing to do with crimes, nothing to do with terrorism.

Ms. BAGINSKI. That's absolutely correct, sir.

Mr. SCOTT. And that's the over-breadth part. And then, when you get all this information, without any probable cause of any criminal activity, then you can start passing it out all over town.

You had Mr. Edgar's clients—how many people, Mr. Edgar, do you think have seen information that has first amendment implications, and possibly embarrassing information, on which the information was gathered without any connection with a crime?

Mr. EDGAR. Well, I don't know. I think that's a really serious question that we need to look at.

Mr. SCOTT. Now, what checks and balances were there to oversee who was sharing what of that information?

Mr. EDGAR. Well, I think there are two problems, Mr. Scott. I mean, the first problem is the FISA problem, the use of intelligence authorities that don't need probable cause of crime to investigate for criminal purposes.

Mr. SCOTT. Well, the Attorney General kind of implied that when we asked could we change the law on how you get a FISA warrant, that the significant purpose had to be foreign intelligence, not even the purpose.

Mr. EDGAR. Right.

Mr. SCOTT. Which kind of invites the question, "If the purpose wasn't foreign intelligence, what was it?" And he blurted out "criminal investigation"; which suggests that you're trying to do a criminal investigation without probable cause of a crime.

Mr. EDGAR. Well, I think that's right, Mr. Scott. Under section 218, I think that's a real danger. I think that under section 203, which is kind of the reverse section—this is the section about sharing crime information with intelligence agencies—you know, I do think that the FBI and DOJ make a fair point, that they have to get probable cause of crime for search warrants when they're doing criminal search warrants, criminal wiretaps.

Mr. SCOTT. Okay, now, this thing goes two ways. You're talking about a criminal investigation, where you had to get the information with probable cause of a crime, going to foreign intelligence. The other is foreign intelligence information that you got——

Mr. EDGAR. Right.

Mr. SCOTT. —without any criminal investigation, without any probable cause at all, just on curiosity. If you've got the agent of a foreign government, curiosity is about the only standard you need to get their phone, and to have the tap all over town with a roving wiretap. So that you really—the real problem is that kind of rumor and innuendo going into the criminal investigation.

Mr. EDGAR. Well, I think they're both problems, Mr. Scott. I mean, I think that the problem that you're addressing may be even more serious. The problem I'm concerned about here was at issue

in the Northern Virginia raids; really is the use of a criminal investigation for really an intelligence-gathering investigation.

Now, these are not, you know, my words. This is what agents were quoted in the "Washington Post" as saying as the reason why our clients—or the clients, I should say, in the case we intervened in, you know, weren't facing any freezing of their assets, any charges after 3 years.

And I really think that it's wrong for the Government to essentially smear all of these people, these organizations, as having some connection with each other; when there really isn't that connection. I think that that's casting a broad brush.

Now, there's no question that there have been people in Northern Virginia who were tried and convicted for some of these offenses that they're talking about. I'm concerned about casting such a broad net that we bring in legitimate academic institutions, or legitimate other institutions or think tanks, seize all their information, and then share it with U.S. Government intelligence agencies, or even foreign government intelligence agencies, when some of these Muslim-American leaders are in fact dissidents and are opposing their own government's policy. And I think that that shows the need for greater safeguards for sharing in both directions.

Mr. SCOTT. Let me—I just have a couple of seconds left. I think we have ascertained, have we not, Ms. Baginski, that you can get a FISA warrant without any allegation of a crime?

Ms. BAGINSKI. Without any allegation of a crime, but driven by foreign intelligence priorities that——

Mr. SCOTT. You can get a foreign—a FISA warrant without any allegation of a crime. Can you tell me what the status of the Levy guidelines is now?

Ms. BAGINSKI. The Levy guidelines, the Attorney General guidelines that have been updated most recently, and they are still in effect and being followed.

Mr. SCOTT. Do you need to be investigating a crime to infiltrate organizations, or can you do it without looking at a crime?

Ms. BAGINSKI. Sir, I think that's a relatively broad statement, so can you give me a little bit more specific—what kinds of organizations?

Mr. SCOTT. Well, the Levy guidelines before said you can't infiltrate somebody's organization unless you're actually investigating a crime. Now there's some suspicion that that practice, which has been the policy for years, since the 1960's, is no longer in effect; so that the FBI and CIA and everybody can go infiltrate somebody's organization without a criminal investigation going on.

Ms. BAGINSKI. No, all investigations have to be predicated—and I've been at the FBI for 2 years, and that has been drilled into me, and that's what I've seen. The Attorney General guidelines are followed. They are overseen by the Justice Department. And if I'm not answering your question, I'll take it for the record.

Mr. SCOTT. Mr. Chairman, could I—I just want to be very clear. So you are saying that you will not infiltrate an organization just to be gathering information? You will actually—if you infiltrate an organization, there actually is suspicion of a crime?

Ms. BAGINSKI. I think that, again, is a very broad statement. The FBI has an investigative mission that is a criminal investigative

mission; but it also has an intelligence-gathering mission. And I don't know which you are asking me about in this case. Or if I'm not being clear, I'm be happy to take this for the record.

Mr. SCOTT. Are we going to have another round?

Mr. COBLE. The gentleman's time has expired. Recognizing the gentlemen and the witnesses—or the Members in order of appearance, the gentleman from Ohio is recognized for 5 minutes.

Mr. CHABOT. Thank you, Mr. Chairman. Ms. Baginski and Mr. Sabin, if I could address my first question to you, could you tell us your views on the ACLU's notice proposal? In his written testimony, Mr. Edgar suggested that law enforcement should be required to notify a judge whenever criminal investigation—the investigative information is shared with the Intelligence Community, regardless of how it's collected, and should also be required to supplement that notice with a report on the disposition of the criminal investigation.

So for example, investigators would be required to notify a judge even if they wished to share with the Intelligence Community foreign intelligence collected through a voluntary interview with a witness in a criminal case.

As a practical matter, would such a requirement inhibit information sharing? And would such a requirement possibly reduce the flow of information provided to the National Counterterrorism Center?

Mr. SABIN. Congressman, yes, it would inhibit the flow of information and restrict abilities of the Counterterrorism Center to robustly attempt to achieve its mission.

For example, the key in this post-9/11 world is prevention. And that task force model, where people have certainty and trust and the ability to address the information in whatever form it comes, allows us to manipulate the information, exploit the information, and figure out for recommendations and decision makers what options, in terms of a national strategy, we can achieve in achieving the mission.

So to specifically address section 203, section 203(a) involves court involvement relating to the grand jury information sharing process. Section 203(b) does not, relating to the title III information. But you have the predicate of going to an article III judge, seeking that wiretap, before you collect that information, as Ms. Baginski referred to earlier, and then specific reporting requirements regarding the obtaining and collection of the information relating to the title III wiretap.

To impose that burden of judicial notification or other kind of good-faith recommendations that Mr. Edgar proposed fundamentally misunderstands the way section 203(d) is being undertaken on a daily basis by the folks both on the criminal and intelligence realms. That is the manner and means by which the executive is understanding the information we have, so that we can pool the information and make thoughtful and appropriate decisions in executing our strategies.

Mr. CHABOT. Thank you. Ms. Baginski, could you weigh in on that, too?

Ms. BAGINSKI. I think Mr. Sabin has actually covered this very, very well. It's the removal of the ambiguity that—I think as Mr.

Sabin has described—that people in the room know that affirmatively they are to share this information. Some of the misunderstanding about the wall was the lack of an affirmative obligation to share in a law. And I think that this is—I think it would greatly inhibit the operations of the NCTC, and even the JTTFs.

Mr. CHABOT. Thank you. Mr. Edgar, to be fair, if you'd like to comment, I'd be happy to hear.

Mr. EDGAR. Sure. I mean, I certainly don't want to impose any unreasonable burdens on the Government. I think that we're talking about not a permission requirement, you know. I wanted to work with the Congress to address some of the serious issues, I think, that are posed by having physical search warrants, grand jury subpoenas, all this information shared.

In the grand jury context, they already have to provide these notices. And so all I'm suggesting is that in the area of title III wiretaps, physical search warrants—maybe other information, maybe not—we can talk to about what kinds of things should be covered, or shouldn't; that there should be notice, and that it should provide a good-faith basis for the criminal investigation. It doesn't have to be an elaborate report.

And I really—you know, it alarms me a little bit to—I just don't see how that's such a huge burden. We're not saying that it has to be done beforehand, you know. I think that information does have to be shared, you know, more quickly. And, you know, Congress can look at this, if we set another sunset date, look at it again, see if that's working, and adjust it then.

Mr. CHABOT. Okay. Thank you. Mr. Chairman, I want to thank you for holding this very important hearing. I know the yellow light has been on there for quite a while. So rather than overstay my time, I'll yield back the balance of this time.

Mr. COBLE. I thank the gentleman.

The gentleman from Massachusetts, Mr. Delahunt.

Mr. DELAHUNT. Thank you, Mr. Chairman. In response to Mr. Edgar's observation about doing it post as opposed to a prerequisite, what's your response, Mr. Sabin?

Mr. SABIN. With respect to 203(b), that's something we could take under consideration and have a discussion about. With respect to 203(d), relating to that sharing of information, I think that would put an unreasonable burden in terms of how we seek to exchange the information in a task force approach, and to do that efficiently and quickly.

So that you have, for example, information gleaned from an interview that an FBI agent does, and then share that information with a colleague in the task force. You would then, according to 203(d) suggested recommended changes, go to a court, in order to have the court, the judiciary, involve itself in that purely executive investigative function—I think takes that kind of notice too far——

Mr. DELAHUNT. Mr. Edgar?

Mr. EDGAR. Well, again, it's a notice requirement that basically just says, "This is what we shared with the Intelligence Community, this is the good-faith basis of our criminal inquiry," that would help to provide some kind of check against the use of——

Mr. DELAHUNT. You're suggesting this now in post?

Mr. EDGAR. Right. And, you know, I think that we can talk a little bit about how extensive that should be. I'm hesitant to say that it should only be for wiretaps because, of course, in the raids I described, I don't believe there were wiretaps.

Mr. DELAHUNT. You've answered my question.

Mr. EDGAR. Okay.

Mr. DELAHUNT. Because I think the problem that the Government has here is a widespread concern. And I think that was articulated in the September 11th Commission, in that second piece of the—that was referred to, I think, by Ms. Baginski, if I'm sure. So I mean, you know, this isn't just simply only about protecting those freedoms that we speak of; but also, reassuring the American people that there are sufficient checks and balances and notifications so that nothing untoward or unsavory is happening.

And given the history, or given the level of misconduct, for example, that has been noted in a variety of different venues and forums by those in Government, I think that's something that really has to be entertained seriously by the Government. There has to be a larger, if you will, mission here: transparency.

And I would suggest that every effort be made by the Government to take this concept of transparency as far as possible, to maximize it. Because with all due respect, that has not been my experience with the Department of Justice.

I served on a Subcommittee—rather, a full Committee—at the invitation of the Chairman. It was a Government Reform Committee looking into the misconduct of the FBI in the Boston office. It was difficult getting information for the Committee relevant to incidents that occurred in the 1980's, the 1970's, and the 1960's.

Finally, there was agreement, a consensus worked out through negotiations by Mr. Burton. And one could, I think, fairly describe him as a rather conservative Member of this Congress. He certainly—it's clear that he's a Member of the majority party. But it took, if you will, a unanimous vote, bicameral—rather, bipartisan—of the Committee, to issue a citation, a contempt citation, before the cooperation I think that was necessary—before that was forthcoming.

So let's think in larger terms. I think this is a very interesting panel. I think some good points have been made. And I'm keeping an open mind. But I think, Mr. Edgar, why don't you draft kind of a white paper, you know? You're not as busy as these other folks. [Laughter.]

And come up with some ideas and suggestions.

Mr. EDGAR. All right, for PATRIOT Act——

Mr. DELAHUNT. Yes, for and against. I think you have a very balanced presentation.

Mr. EDGAR. Thank you.

Mr. DELAHUNT. And the ACLU has credibility among, you know, certain segments of the American population; rather remarkably now, from the National Rifle Association and groups that are commonly described more progressive.

And, you know, maybe it's time, Mr. Chairman, for some thoughtful discussion among all of the parties involved.

Mr. EDGAR. I appreciate that, and we'll undertake to get that to you, Mr. Delahunt.

Mr. COBLE. I thank the gentleman from Massachusetts. Mr. Edgar, I'm sure you're welcoming this assignment of additional homework that's been leveled upon you.

The gentleman from California, Mr. Lungren.

Mr. LUNGREN. Thank you very much, Mr. Chairman. I want to thank you and members of the staff for putting together this panel. These are serious issues. But I can't help but reflect back on a previous experience I had where I served as the vice chairman of the national commission that looked at the way we treated Japanese Americans and Japanese nationals during World War II; and recall the response of the Federal Government at that time, in face of a true national security concern, and the overreach and the, in hindsight, wrongheaded reaction of the Federal Government at that time.

So while I am pleased, and share the concerns everybody does that we not abuse powers given to the Executive Branch, I just might say that it strikes me that this is a far better conversation to have post-9/11 than the discussions that were had and decisions that were made by the Federal Government post-Pearl Harbor, with the treatment of an identified ethnic group.

That's not to suggest that those people that you've mentioned, Mr. Edgar, ought not to be concerned and ought not to look for indications of proper concern and proper sensitivity on the part of those serving in the Federal Government at the present time.

The gentleman from Virginia mentioned some issues of over-breadth, but his description of the law basically was just a description of the law, and not a description of over-breadth. The decision was made by the Congress to include sections 203 and 218 in the PATRIOT Act precisely because we had a wall, and precisely because we thought it interfered with the proper exercise of Executive Branch activity in the area of both criminal law and national security intelligence issues.

So a question I have for you, Mr. Edgar, is this. It seems to me, some of your complaint was really directed more to 218 than to 203(b) and (d). And in the absence of amendment of either 203(b) or 203(d), do you individually, or your organization, support the sunsetting, permanent sunsetting, of those provisions?

Mr. EDGAR. Well, Mr. Lungren, I really hope we don't have to do that. I mean, I think that the whole point of the sunset provision was to give Congress a chance to have these hearings and to talk about what provisions needed to be kept or sunsetted or changed.

You know, I think that, you know, I have a sort of a top five or so provisions of the PATRIOT Act that I'm most concerned about. I'm not sure 203 would be on it. It's an important provision, one that we think needs to be fixed. And, you know, we've suggested ways to fix it here. You know, I'm happy to get back to you about all of the 16 provisions.

Our suggestion is to use the 9/11 Commission test. You know, first, does it materially enhance security? You know, we've heard a lot more detail today about the use of 203(b) and (d) than I've heard ever before, including in the sunset report. So we should study that. And then secondly, are there guidelines—are there other protections we can include? And I've suggested a few here for you.

Mr. LUNGREN. Okay. Let me ask you a question on 203(d) with respect to the subsequent notification that you were suggesting. Would you tell me exactly how that would work? Exactly how, under section 203(d), where information that's obtained through a criminal investigation, that is shared with foreign intelligence—within the foreign intelligence activity of the Federal Government, or investigation of the Federal Government—how your notification would work?

What exactly would the Government be required to do, and at what stage would they be required to do it? And how often would they be required to do it in a continuing criminal investigation?

Mr. EDGAR. Well, that's a great question. I think that if you look at 203(a) as somewhat of the model, which is for grand jury information, they say within a reasonable time notice has to be provided to the court. You know, I think that's a reasonable basis for all criminal information.

It has to be—already, under the guidelines that I mentioned, it already has to be labeled as U.S. person specific foreign intelligence information, when it's shared and treated in accordance with Executive Order 12333. So they're going to already know what this is; you know, what the notice would apply to.

Mr. LUNGREN. But I guess my question would be this.

Mr. EDGAR. Yes.

Mr. LUNGREN. If you're sharing the information on day 13——

Mr. EDGAR. Right.

Mr. LUNGREN. —and then more information develops in the criminal investigation on day 45, and then on day 60, is there a requirement for continued—I'm just asking for your idea. Would there be a——

Mr. EDGAR. Yes, well, I think there would have to be some kind of reasonable requirement, that's not overly burdensome, to keep the court currently informed on what's going on, and to provide the good-faith basis for the investigation. And that's something that could be worked out with guidelines; we could work on legislative language; however you would see fit to work on it.

Mr. LUNGREN. Okay. Mr. Sabin—and I know we're asking you to talk sort of off the top of your head, here—but in what way would that interfere with the proper functioning of your office in the sharing of information?

Mr. SABIN. I just don't see how that recommendation could work in the real world on a practical basis so that information can be timely shared between the law enforcement and national security officials. Indeed, I think probably the judiciary would be concerned about the imposition of all their resources and their involvement from their perspective in the ongoing Executive Branch prosecutorial investigation.

Mr. LUNGREN. Okay. Well, that's kind of a conclusionary statement you made. Tell me why.

Mr. SABIN. Well, it goes to——

Mr. COBLE. Mr. Sabin, wrap up rather quickly, because the time has expired and we've got to move along. But go ahead, sir.

Mr. SABIN. Because it would develop uncertainty. It would undermine the ability to timely and specifically share that information

so that we can act upon it in an aggressive and appropriately thoughtful manner.

Mr. COBLE. The gentleman's time has expired.

The gentlelady from California, Ms. Waters.

Ms. WATERS. Thank you very much, Mr. Chairman. And I, too, appreciate this hearing, and other hearings, because our Country is now in a position where we must decide how to make sure that we're offering the security to our Nation that all Americans should have. At the same time, how do we respect the Constitution and our civil rights and our civil liberties? And this is a debate that has been long in coming.

Having said that, I'm going to take just one little portion here of the Congressman's testimony, the written testimony, that refers to the fact that the PATRIOT Act simply authorizes the use of roving wiretaps. And my question is, is this an over-simplification of section 206 of the PATRIOT Act? Isn't it more accurate that under the Act the FISA court can authorize wiretaps or intercepts on any phones or computers that any target may use; thus eliminating the particularity requirement to obtain warrants under the fourth amendment of the Constitution?

I'm concerned because, I guess, in tearing down the wall under surveillance or investigation, any information that law enforcement wishes to share, it can share. And I'm not so sure whether or not the person sharing the information is ever involved in the court—a court action for prosecution, where they would determine how they got the information, what they really heard, and be sworn to tell the truth.

And I'm also concerned that this roving wiretap, it just roves everywhere. It follows you for how long? For 1 year, 2 years, 3 years, 10 years? For the rest of your life? It follows you to the athletic club; follows you to school, where you are a principal using the telephone? What are the restraints, what are the constraints? Why do you think it's not that important; it's just another security measure that is important to helping to secure the nation?

Mr. MCCAUL. And I do appreciate your concerns. Maybe I can clarify some of them. One is that in the—I'd say for the last quarter of a century, in drug cases and organized crime cases, law enforcement has had the ability to wiretap not just one particular line, but the individual, themselves. So in other words, whatever phones they have access to, we can wiretap those phones.

In answer to your question about the period of time, it's 90 days. Under FISA, they are active for 90 days. Then we have to repetition to renew that FISA.

Now, the standard for a FISA, as Mr. Scott pointed out, is: Is this person, is this individual an agent of a foreign power? Are they a foreign power, are they an agent of a foreign power? And, you know, there is a fine line, also, between someone who's in this country for clandestine purposes, and the criminal area, as well.

In fact, the definition—to maybe clarify it for Mr. Scott—the definition of "foreign intelligence information" includes—and this is in the Foreign Intelligence Surveillance Act—includes crimes such as espionage, sabotage, or terrorism.

When the PATRIOT Act was passed in 2001, Senator Leahy, who was Judiciary Committee Chairman in the Senate, stated, "This

bill breaks down traditional barriers between law enforcement and foreign intelligence. This is not done just to combat international terrorism, but for any criminal investigation that overlaps a broad definition of foreign intelligence."

And I think Mr. Sabin probably has examples. I do, as well. This is not just for fun and games. These are people in this country who because of security——

Ms. WATERS. May I interrupt you for 1 second? Because my time is going to be up in just a second. I want to be clear. Someone is under criminal investigation, or they're on surveillance for some reason—maybe not criminal investigation. They pick up some information, law enforcement, I suppose. Do they go to court prior to sharing that information with the Intelligence Community? Or do they just share that information with the Intelligence Community? Then after 90 days, are you telling me it is then the Intelligence Community that goes to court to be able to continue to place that person under roving surveillance? How does it work?

Mr. MCCAUL. Well, really, the best I can do is to try to simplify it. There are basically two ways to obtain a wiretap in this country. One is under title III, which involves an article III judge, a Federal district judge. The other way to obtain a wiretap, under the Foreign Intelligence Surveillance Act, is to go to the FISA court. It's a three-member court that presides in the Department of Justice. Those are intelligence cases. And the standard is different for obtaining wiretaps.

In a criminal case it's: Is there a probable cause that a crime is being committed? In a FISA intelligence—usually terrorist—case it's: Is this person—is there probable cause that they're an agent of a foreign power? If they are, that's the legal standard that you can obtain the wiretap.

Prior to the FISA, interestingly, there was no restriction. The President had absolute authority for warrantless searches, with respect to national security. So that's sort of a history of it.

When the—typically, if we had a wiretap in a criminal case and we wanted to share that, typically we would just amend the FCI, foreign counterintelligence, agents to our 6(e) list, our rule 6(e) list, and file that with court.

Ms. WATERS. I think I need some more time, but I won't try and take it now.

Mr. COBLE. We'll have a second round, Ms. Waters.

Ms. WATERS. All right. Thank you.

Mr. COBLE. The gentleman from Texas, Mr. Gohmert.

Mr. GOHMERT. Thank you, Mr. Chairman. Like the other folks here, I really appreciate your having this hearing. This is important. On the other hand, it's not often we get a chance to cross examine under oath colleagues with whom we went through orientation, and perhaps explore some of their secret feelings under oath.

I am curious. The sentence, "The confrontation that we are calling for with the apostate regimes does not know socratic debates, platonic ideals, nor Aristotle diplomacy." Who wrote that?

Mr. MCCAUL. This is—I think it's disturbing language. And the first time I read this, you know, when I realized the source, it is—it's very shocking, and it kind of—I think it demonstrates why we're here today. It says, "Islamic governments have never, and

will never be established through peaceful solutions and cooperative councils. They are established, as they always have been, through pen and gun, by word and bullet, and by tongue and teeth."

The words that Mr. Gohmert introduced, and that I finished, is the preface to the Al Qaeda training manual. And I think it gives great insight as to who the enemy is. It gives great insight into their thinking process and what they intend to do.

And again, I think it demonstrates why the question is not if, but when and where the next attack will occur. That's why I believe reauthorization of this act is so important.

Mr. GOHMERT. Well, let me ask—and I'm not sure who would be the best to respond; perhaps the Department of Justice rep, or FBI rep. But with regard to the information sharing—and pardon my ignorance, but I'm not afraid to embarrass myself by asking silly questions; but I've got to ask. Who, specifically, is doing the analysis to determine what information is important and useful to the mission that may be shared?

Ms. BAGINSKI. That work is actually done in a combination of my intelligence analysts with agents. It is all directed by firmly established national intelligence requirements, where we are charged with responding to and producing information on very specific information areas that are defined by, currently, the Director of Central Intelligence and, in the future, the Director of National Intelligence.

Mr. GOHMERT. Well, what specifically is done to determine whether it's something that should be shared?

Ms. BAGINSKI. There are senior intelligence analysts, who are called "reports officers." They review the sum total of the investigative product against those requirements. They put reports together, and those reports are approved by a chain of command that flows through my organization in the Intelligence Directorate.

Mr. GOHMERT. Okay. And then, are the reports entered into the data system that others with appropriate security clearance can access?

Ms. BAGINSKI. That's correct, sir.

Mr. GOHMERT. Are there forms that are filled out with personal information about individuals? Or is it just the report? I mean, how detailed is the information?

Ms. BAGINSKI. It is the information, and in every respect what we do is separate the information from the source and minimize the U.S. person information.

Mr. GOHMERT. Okay. When we talk about analysts and senior analysts, what type of educational background do these people have, and what type of clearance?

Ms. BAGINSKI. Our analysts are all cleared to the top secret code word, and then they have a few compartments, depending on the areas in which they're working. But the generic clearance would be that.

The general background for our analysts now is, we have about 60 percent of the population of 1,922 to date that have advanced degrees. Many of them are lawyers; many of them are political scientists; many of them are linguists. They come from a very broad

background, because what we're really looking for is their ability to think and make judgments based on information.

Mr. GOHMERT. Well, quickly—my time is running out——

Ms. BAGINSKI. Yes, sir.

Mr. GOHMERT. —but is there any routinely scheduled review after this information is shared, to determine whether it was appropriate to share it or not?

Ms. BAGINSKI. Yes, sir. Many of those things are done actually under the intelligence oversight processes that are in place, Foreign Intelligence Oversight Board, the HPSCI and the SSCI especially, with regard—and OIPR, of course, looks at that from our perspective.

Mr. GOHMERT. Do they look at specific cases of information sharing to determine if it was appropriately done? I know you said it flows through you, but I'm curious about oversight after the fact, to see if there was abuse.

Ms. BAGINSKI. Yes, there is oversight on both sides of that, through the intel committees and, of course, through our Office of Intelligence and Policy Review. But I would like to actually gather some more information. It's a very lengthy answer. So if you wouldn't mind receiving a written response to that, I could go through the various components.

Mr. GOHMERT. I would greatly appreciate that, very much. Thank you.

Ms. BAGINSKI. Okay.

Mr. GOHMERT. Thank you, Mr. Chairman.

Mr. COBLE. I thank the gentleman. We'll start a second round now, and we'll move this along. Ms. Baginski, this may have been touched upon, but let me put my oars in these waters. If section 203 were allowed to expire, would the FBI be unable to share some foreign intelligence that it collects with the National Intelligence Director?

Ms. BAGINSKI. Actually, not with the National Intelligence Director himself, because if you go back to the National Security Act, that provision has always been in there to actually share foreign intelligence that comes from criminal investigations with the DCI, and that has been amended now to be the DNI.

Where you would have the problem is in a setting like the NCTC, where that sharing would be far less clear. You would not have the affirmative—the affirmative guidance to share that information more broadly than the DNI, who is just one person.

Mr. COBLE. So I take it that you believe that if it did expire it would hamper the effectiveness of the National Intelligence Director?

Ms. BAGINSKI. I do think so, in practice, yes, sir.

Mr. COBLE. Mr. Edgar, can you cite any examples, other than the Virginia incident you mentioned, that were not—where 203 was not properly utilized or used?

Mr. EDGAR. Well, I think what we would need to do to look at that, Mr. Chairman, is to look at some of the ways in which some of the DOJ's criminal investigations have been very wide ranging after 9/11. One example I didn't include in my testimony—and maybe I can supplement it—there was an investigation including—I believe it was just the threat of a criminal subpoena that may

have been withdrawn. But it involved an Ohio peace group at an Ohio university, where there was a lot of discussion about that.

I think those are the kinds of things we're worried about, is that, you know, some of the criminal powers—you know, certainly, some of them require probable cause; some of them don't. And the law rightly gives these investigators wide latitude. So I could look at that Ohio case, and maybe some others as well.

Mr. COBLE. Yes. And you may supplement that, and we'll keep the record open for at least 7 days. When it was your belief that it was improperly approached, Mr. Edgar, did you report that to the Inspector General?

Mr. EDGAR. Well, I just have, you know, at your invitation, recently started to look at this whole issue, 203.

Mr. COBLE. Okay.

Mr. EDGAR. I can talk to the attorneys involved and see what they've done in terms of reporting. They have filed, actually, a civil rights lawsuit, so I think they've gone even further than that.

Mr. COBLE. Mr. McCaul, you were responding to Ms. Waters when the time expired. I have about two more minutes to go. Do you want to pick up on where you were?

Mr. MCCAUL. Well, again, I think what the PATRIOT Act attempted to do is update to the modern age of technology, provide for a national system of search warrants; which is extremely effective, instead of having to go to each multiple jurisdiction. And the case I highlighted in my opening statement I think was a good example of that. And then, lastly, to apply some of these laws that we've been able to use against organized crime and drug dealers against terrorists and in these intelligence cases. Certainly, the roving, you know, wiretap is an example of one of those techniques that's been used for quite some time in those types of cases.

And I have to emphasize that nothing is done without judicial review. It's not an abrogation of judicial authority. Everything that is done, whether it's a search warrant, a wiretap, an arrest warrant, is always done with judicial review; whether it's in the criminal side under, you know, article III, or in the FISA arena.

Mr. COBLE. I thank you. And you know, we've said nothing about this at this hearing, and this may not be the appropriate forum, but I have grave concerns about the connection between drug trafficking and terrorism. And that may be for another day.

Does anybody want to weigh in on that now? That's not the topic at hand, but anybody want to? I've got about 50 seconds to go.

Mr. SABIN. Chairman, I would, because I believe it emphasizes the manner in which information sharing needs to be robust. Because narco-trafficking, or narco-terrorism, is not when the information comes in relating to groups such as the AUC or the FARC down in Colombia, in and of itself, identified in some special package as foreign intelligence information. But you can have generating from narcotics investigations, from alien smuggling and human trafficking cases, from cyber crime, manners in which foreign intelligence, foreign intelligence information, or counterintelligence aspects are implicated.

And that's why it's so crucial to be able to share the information to pursue those so that we can, in appropriate circumstances, in a

transparent way, as Mr. Delahunt suggests, bring and use the criminal processes to achieve what we're trying to achieve.

Mr. COBLE. I thank you. My time has expired.

The gentleman from Virginia, Mr. Scott.

Mr. SCOTT. Thank you. As we've established, a lot of this FISA does not require a crime as a predicate; just foreign intelligence which includes the conduct of foreign affairs, whatever that means. That could mean negotiating a trade deal or anything else, you can get information. And everybody has kind of alluded to terrorism as a—show the need for all this information sharing.

So I'd just ask Ms. Baginski, would you agree to limit this just to terrorism, and not to trade deals and other things that don't have anything to do with a crime?

Ms. BAGINSKI. Not as an intelligence professional, no, sir.

Mr. SCOTT. Okay.

Ms. BAGINSKI. Counter-espionage, I think, espionage, is another very good example of why you wouldn't limit it to terrorism. But I think the more important part is that on the collection end, a priori, you actually can't make a judgment about the reason that you collected it and the information that comes out the other end.

Mr. SCOTT. Okay. Well, the answer is you don't want to limit it to terrorism. And just kind of the problem is, as the gentleman from Texas kind of pointed out, that there are essentially no outside checks and balances. Everybody that checks and balances is subject to the same chain of command. When the chain of command says, "Do it," there's no judicial oversight or anything else. You just have to—have to do it.

And when you start sharing this information, it's just not, you know—when it says sharing, which may not have been a crime to begin with, you can share this information with law enforcement, intelligence, protective, immigration, national defense, or national security. How many people exactly—by the time you've done all that how many people get to look? If you've got something embarrassing—not criminal, just embarrassing—how many people get to look at that information? Dozens? Hundreds? Thousands? I mean, how do you share it? Post it on the Internet? I mean, how do you—there is no limit.

And when you start talking about getting this FISA, we've already—like I said, people keep talking about terrorism and all that. You can get the FISA warrants without a crime. All you have to do is show the probable cause it's an agent of a foreign government. How many people qualify under that "agent of a foreign government?" What kind of category is that? Does Osama bin Laden count as somebody you can get a FISA warrant against?

Mr. SABIN. To answer your question, yes. Let's be clear regarding the use of the terms. As the FISA appellate court opined and specifically decided, the best use, often the best use of the FISA statute is through the criminal process. So I would respectfully disagree with you, Ranking Member Scott, that you cannot act as a predicate in order to seek a FISA warrant.

Mr. SCOTT. No, I didn't say you could not use crime. You do not have to have crime.

Mr. SABIN. Correct.

Mr. SCOTT. You can get a FISA warrant, no crime even alleged or suspected.

Mr. SABIN. Correct.

Mr. SCOTT. Thank you.

Mr. SABIN. But as part of the FISA appellate court——

Mr. SCOTT. Oh, you may have a crime. May be terrorism.

Mr. SABIN. Correct.

Mr. SCOTT. Osama bin Laden, I mean, he's going to blow something up—it may be a crime; may not. That's the over-breadth part of it. And we've already determined you don't want to limit it to terrorism. So you're including all of this other stuff. And then once you get—again, try to help me out. Who can you get a FISA warrant against? Who can be a target?

Mr. SABIN. A foreign power, or an agent of a foreign power. But your analysis goes to the sharing——

Mr. SCOTT. What foreign power is Osama bin Laden?

Mr. SABIN. It would—related to Al Qaeda. Specifically, foreign terrorist organization, as determined under the Immigration and Nationality Act. There are present 40 foreign terrorist organizations that the Secretary of State, in consultation with the Attorney General and the Secretary of Treasury, have designated.

Mr. SCOTT. They put your name on a list.

Mr. SABIN. Correct. And that's why it's transparent, to go back to Mr. Delahunt's point; is that there is for all that interact between the individuals that are under the direction and control of the foreign terrorist organizations and those associate members.

Mr. SCOTT. Can you do a "lone wolf?"

Mr. SABIN. Yes. That is what Congress provided in the Intelligence Reform Act 4 months ago in the December legislation. But that goes to the sharing——

Mr. SCOTT. So the——

Mr. SABIN. If I could finish——

Mr. SCOTT. Well, let me just say this. If the Department of Defense designates somebody as a lone wolf, then you can start listening in.

Mr. SABIN. No, it's not the Department of Defense. It's the Secretary of State, but——

Mr. SCOTT. Okay, Secretary of Defense names somebody, and then they are the target of a FISA warrant.

Mr. SABIN. That's not accurate.

Mr. SCOTT. Okay.

Mr. SABIN. Sir, you're talking about the sharing from the intelligence side, under sections 218 and 504, to the law enforcement side. This—sections 203(b) and (d) go the other way with respect to the sharing from the criminal law enforcement, to the national security officials. So that there is a reciprocal exchange of information sharing.

So while the provisions of 218 and 504 complement and integrate with respect to the information sharing, they are separate from the sunset provisions relating to 203(b) and (d).

Mr. SCOTT. Okay. Let me—let's get straight, then. Can you share FISA information with law enforcement?

Mr. SABIN. Yes, pursuant to sections 218 and 504.

Mr. SCOTT. Okay. And once you get the information from FISA—once you get a target, you can do a roving wiretap, as the gentlelady from California indicated?

Mr. SABIN. Correct. Because we have seen that individuals use cell phones and are quick to avoid detection.

Mr. SCOTT. And once the Secretary of State has designated that target and you get this roving wiretap, you can put a tap on every phone they use?

Mr. SABIN. No. It has to be particular to the individual; not to the facility. That's the difference between a title III and a FISA wiretap. In terms of a title III, you have to have probable cause relating to—that a criminal activity is occurring——

Mr. SCOTT. Well, no, we're talking about a roving FISA wiretap.

Mr. SABIN. Correct. But that's the difference between the——

Mr. SCOTT. Roving FISA wiretap. What can you put a bug on?

Mr. SABIN. It depends on what the facility is used. You can do it for oral. You can do it for electronic. You can do it for a wire. But it has to be determined that—through the FISA court process; which is an article III judge.

Mr. SCOTT. Once you get a FISA roving wiretap against somebody, you can put a bug on every phone they use.

Mr. SABIN. If you establish the requisite reasons that they would seek to be using it to avoid detection and surveillance.

Mr. SCOTT. Now, the Attorney General refused to agree to the suggestion that I made that you ought to ascertain, after you've gotten the bug there, that the target is actually in the building, using the phone. An ascertainment, you know, so that once you got a bug on the phone, on the pay phone on the corner, you want to make sure that it's actually the target using the phone, and not somebody else just using the phone.

Mr. SABIN. Yes, but in the application and the affidavit sworn to by an officer, they have set forth the probable cause why that individual is an agent of a foreign power. So that's in the determination by the court.

Mr. SCOTT. You have to list every phone they use in the warrant?

Mr. SABIN. No. Because you don't know——

Mr. SCOTT. That's right.

Mr. SABIN. —what they're going to use and what——

Mr. SCOTT. And so, without checks and balances, you put the bug on the corner telephone. And then the guy leaves the corner, and you don't stop listening.

Mr. SABIN. Yes, but implicit in that assumption is the fact that you didn't make that showing to the article III FISA court judge. And if you can make that requisite showing, so that the judge has the confidence that the Government is appropriately seeking to use that investigative technique, then that is something that should be pursued.

Mr. SCOTT. Once you have alleged that it's an agent of a foreign government, and you want the roving wiretap, does a judge have any discretion as to whether to issue the warrant or not?

Mr. SABIN. Yes. You have to seek——

Mr. SCOTT. Once you have made that—once you have stated that representation, that it's an agent of a foreign government and you

want the roving wiretap because you're going to get some foreign intelligence, does the judge have discretion to say "No?"

Mr. SABIN. Yes. The judge can say that there's insufficient probable cause, that the Government has not met that standard. And so he can say "No"—he or she can say "No." Absolutely.

Mr. DELAHUNT. Would the gentleman yield for a moment? Bobby?

Mr. SCOTT. I yield whatever time——

Mr. COBLE. The gentleman's time has expired, but you'll do this very quickly.

Mr. DELAHUNT. Yes. I think what the Ranking Member is alluding to is, is there minimization?

Mr. SCOTT. Right.

Mr. SABIN. Yes.

Mr. DELAHUNT. Okay?

Mr. SABIN. She wrote me a note—Ms. Baginski wrote me a note about minimization. And she can talk——

Mr. DELAHUNT. Well, let me put my questions then to Miss——

Mr. COBLE. Well, gentlemen, if I may—let me get to the gentleman from Texas. Then I'll get with you next.

The gentlelady from California, Ms. Waters, had to go to another meeting, and she has requested that her opening statement be made a part of the record. And with unanimous consent, it will be made a part of the record.

The gentleman from Texas is recognized.

Mr. GOHMERT. Thank you, Mr. Chairman. Just quickly, you know, we do live in extraordinary times. And the type of weapons available, the terrorists, so exceed what there was available 200-plus years ago, it just couldn't have been foreseen. I understand we need additional investigative powers just to protect ourselves, but I am concerned about the level of supervision, and perhaps outside analysis. And for lack of a better term, what we used to say in the Army is there needs to be a pucker factor somewhere along the way, where people are actually worried.

And I was trying to glean earlier what kind of pucker factor, or concern, would there be by an employee for their job, for their, you know, violating the law, going too far, if they put inappropriate information into the system, viewable by those that shouldn't see it, or pursue something that shouldn't have been?

Mr. SABIN. This Congress passed section 223 of the PATRIOT Act, which provides for both administrative discipline for violation of the information sharing rules contained in title II, as well as the potential for a civil lawsuit.

Also, under title XVIII, United States Code, relating to the wiretap provisions, I believe that would relate to section 203(b), that if there is an improper disclosure there are also the potential for civil lawsuits or administrative discipline. So it's taken very seriously, with respect to potential consequences, for a willful violation of the statute and the provisions.

Mr. GOHMERT. A willful violation is what it has to be?

Mr. SABIN. I believe so, sir.

Mr. GOHMERT. Yes. Mr. Edgar?

Mr. EDGAR. Yes, I was just going to say, the problem we see with section 223 is that it really requires the person to have found out about the surveillance.

Mr. GOHMERT. Well, in fact, you were going to my next question, if I could ask Mr. Sabin. You mentioned the lawsuits, the administrative action. But as Mr. Edgar says, someone's got to find out about that before they do it. And in my earlier questions, I was pursuing that.

If there is no outside entity that has an independent objective look-see and files a routine report on anything that's inappropriate, then how would an individual find out that there was an actionable conduct?

Mr. SABIN. What comes to mind is, first, if I'm not mistaken, under the Intelligence Reform and Prevention Act, that set up a civil liberties board in the Executive Branch, as well as the potential for referrals to the Inspector General relating to violations of the PATRIOT Act. So——

Mr. GOHMERT. And that's all within the Executive Branch, correct?

Mr. SABIN. I believe that's correct, sir.

Mr. EDGAR. Well, in the civil liberties board, subpoenas can be blocked by the Attorney General, under a provision of that law, you know, that we objected to, but was enacted. One thing that I think would be helpful about the notice I'm talking about is, it's to the judiciary. And it's something that would provide that kind of pucker factor that you're talking about, you know, to say, "Am I really going to file this notice?" you know, "Is this notice correct? Is it stating a good-faith basis?"

Mr. GOHMERT. And I mentioned this to Attorney General Gonzalez. I'll mention it to you. You surely have an appreciation of history. You understand, nothing personal in these kinds of questions. Because I know so many people very well that have absolute confidence in Attorney General Gonzalez, that I have complete confidence in him. I have complete confidence, and I admire and respect and appreciate President George W. Bush.

My current concern is that we had a president in the early '70's that was not so concerned with honesty. We had an Attorney General under that Administration that had the same problem, and his general counsel. And then you look into the '90's, and we had an Administration that was so abusive that there were a thousand or so files in the White House.

So if the oversight is the Executive Branch, I'm not concerned about this President; but I'm concerned about Presidents in the future that could be, their general counsels, their Attorneys General; and whether or not the Executive Branch at that point will be capable of slapping itself silly for having a thousand files and maybe sending some people to prison, as I've kind of felt like somebody should have investigated and pursued back in the '90's.

So nothing personal. I'm sure you understand that. All right, thank you, Mr. Chairman.

Mr. COBLE. I thank the gentleman.

The gentleman from Massachusetts, Mr. Delahunt, now you're recognized.

Mr. DELAHUNT. I thank the Chair. A lot of what Congressman Gohmert articulated, I agree with. You know what I think might be worthwhile, Mr. Chairman, I think what we really need, because this is—some of this is esoteric and arcane, and unless you really understand the mechanics, it's difficult to comprehend.

You know, we might want to consider doing a field trip. Remember those good old days? An afternoon? And actually walk through the process itself, so that it can—many of us learn visually, many of us learn by touching it, etcetera. But it does become arcane.

But, you know, the point that Congressman Gohmert makes about, you know, who's there to review your analysis, your analysts, in terms of their examination of whether the sharing was appropriate or not—and again, he's correct; this is not directed—this is not ad hominem, but it's institutional. Because our history is replete, you know, with situations where that power has been abused. It goes to the system of checks and balances.

And I don't know what the answer is to that, but I think you've got to come up with something. You know, maybe it's Congress that exercises that oversight. Are you collecting data on that information now? Do you have a system so that you could do a full report to the Committee on the Judiciary?

Ms. BAGINSKI. I could certainly report the information that has been shared with the Intelligence Community in the form of reports.

Mr. DELAHUNT. What about have you had any experiences, whether it's inadvertent or otherwise, where information should not have been shared?

Ms. BAGINSKI. I have not, in my experience through the intelligence reports, no. And there is, I think, as you know, HPSCI and SSCI do considerable oversight on both the collection side, the appropriateness of how information was actually collected, and how do you share——

Mr. DELAHUNT. How do you feel about the guidelines becoming statutory, with a discussion among Members of Congress about incorporating criminal sanctions?

Ms. BAGINSKI. The Attorney General guidelines?

Mr. DELAHUNT. Uh-huh.

Ms. BAGINSKI. I haven't even given it any thought. But I think, on the face of it, I wouldn't have any problem with it. They're a very good framework.

Mr. DELAHUNT. Mr. Sabin?

Mr. SABIN. To get back to the pucker factor, there are career people that—and one of the lessons learned is the idea that we shouldn't tie ourselves and hamstring ourselves. While we would be receptive to analyzing that, I would be concerned that that may swing the pendulum too far, and people will have a concern about robustly sharing information.

So while there needs to be the checks and balances and the transparency, I think that that might be too harsh a sanction. But we can sit down and talk about it.

Mr. DELAHUNT. You know, I think it was Mr. Lungren that referenced the issues surrounding, you know, the mistreatment of Japanese Americans during World War II. And I think it was you,

Mr. Edgar, that, you know, presented a case that you distinguished from those cases that were described by Mr. Sabin.

Mr. EDGAR. That's right.

Mr. DELAHUNT. About the Islamic community here and the Arab American community here. I think everybody's sensitive to that. Maybe this is just a problem attendant toward the nature of investigations, period. But when you do a search, and that search receives considerable media attention, and who knows where it comes from—but there was one in my home city. I happened to be walking by. I live there. CBS was there and, Jesus, there was cameras and stuff going on. It was three or four years ago. And you know, nothing's happened. The business has gone out of existence, and reputations have been, you know, tarnished.

If we're talking about the confidence of the American people in the integrity of the system, in how this democracy works, I think you've got to start to seriously consider a way, once an investigation concludes, to announce and to exonerate and, if need be, to apologize.

I was a prosecutor a long time ago for a lot of years. You know, on different occasions, I had to stand up and say that, "We unintentionally erred, and we charged people with crimes that were innocent." But there's been a history of the Federal Government, the Department of Justice, through the years to subscribe to this, "We can't comment."

Of course, it appears in the paper anyhow, and there are leaks. And we know how all—we all know how that game is played. But we hurt innocent people. And we diminish ourselves, and we diminish our liberties, and we diminish the confidence of the American people in the integrity of the system. Mr. Sabin?

Mr. SABIN. Yes, Mr. Delahunt. And I fully agree that that is a valid objective. And I think I'm familiar with the matter that you're referring to in Boston. And I would refer your attention to the United States Attorney's Manual, sort of the bible of how we conduct our businesses. And there is a provision by which the U.S. Attorney can make a public announcement regarding the cessation or declination of a particular matter, if it's an appropriate set of circumstances.

I would respectfully disagree that the Northern Virginia charities matter and that investigation is such an example. I can provide you the court decisions from Georgia and from the Eastern District of Virginia whereby——

Mr. DELAHUNT. I think you're talking about different cases.

Mr. SABIN. No, it's the same case, sir. With respect to the number of search warrants that were executed on the same day, there was a civil lawsuit brought, that he has referred to, against the case agent and a Government consultant. The Eastern District of Virginia dismissed the case against those individuals, finding that there was sufficient probable cause for the search warrant affidavits and that there was extensively detailed information accurately presented in those search warrant affidavits. That's transparent; that's public; that's on the record; and we can provide that.

So with all due respect, not only have there been criminal prosecutions emanating from that investigation, but that there was appropriate use of the search warrants; that that is an ongoing inves-

tigation that has been previously publicly disclosed; and that the allegations relating to the Government case agent and to the Government consultant were dismissed by the court.

Mr. DELAHUNT. I'm not suggesting—I'm not going to give you an opportunity to answer, because he's going to bang that gavel on me really soon. I'm just going to extend it.

But I'm not even talking about those cases. And I'm not talking necessarily cases implicating terrorism and the PATRIOT Act. I'm talking about a wide, you know, variety of cases, that all too often, reputations are tarnished. And maybe it's time for Justice to examine the U.S. Attorney's Manual, understand—to expand that provision in there that allows for public statements. Because I think it would go a long way to restore confidence in the DOJ and the process itself. Because it lingers out there, and it causes great harm to people.

And I would just add one other thing. We're talking about sharing of information and the need to break down a wall. Again, I was a State prosecutor, Mr. Chairman, for a long time. And there still exist serious problems with the sharing of information by certain Federal agencies with local and State law enforcement officials in non-national security cases, but in traditional cases implicating violent crime; which obviously is a concern to all of us. Thank you, Mr. Chairman.

Mr. COBLE. And I didn't gavel you down, Mr. Delahunt.

Mr. Sabin, I know you're on a short leash, and I know you have to get back to Justice soon. I'm going to recognize Ms. Waters right now. But before I do, as a follow-up to Mr. Scott, you're not suggesting, are you, Mr. Sabin—well, strike that. Are you suggesting that the State Department can designate a person as a lone wolf?

Mr. SABIN. No.

Mr. COBLE. Okay.

Mr. SABIN. No.

Mr. SCOTT. How do you get designated as a lone wolf?

Mr. SABIN. There are different mechanism by which you can be designated, that sort of makes you radioactive, to trigger violations of the material support statutes under 2339(a) or (b), or the International Emergency Economic Powers Act, under title 50, section 1705.

Mr. SCOTT. The question was, how do you get designated a lone wolf for the purpose of a FISA warrant, that you can be the target of a FISA warrant?

Mr. SABIN. That is information that is provided to the FISA court judges. I was talking about the invocation of criminal process in order to trigger those criminal statute violations. But in terms of the probable cause that is set forth in determining someone is a lone wolf, that's the factual information that is contained within the application and the affidavit to the court.

Mr. COBLE. We're on Ms. Waters' time. Let me recognize the gentlelady from California.

Ms. WATERS. Thank you very much, Mr. Chairman and Members. This subject interests me greatly because of what I learned about COINTELPRO. I don't know if any of you are familiar with COINTELPRO. Are any of you familiar with COINTELPRO?

Mr. EDGAR. Yes, Congresswoman. And I think that that is really the concern we have. It was a massive domestic spy operation throughout the '60's, '70's, about investigating peace groups.

I mean, I do want to respond, again, about this Northern Virginia case. I want to make clear, I'm talking about the searches of the Graduate School of Islamic Thought and the institute—International Institute for Islamic Thought. I am informed that no charges are pending or have been made against any of those institutions. Their attorney was informed by the Government that they're not under investigation any more for terrorism financing. None of their assets have been frozen.

And I do think that it's wrong to talk about all of these search warrants as if they're all involving all the same people. There are a lot of different groups and different individuals that were involved. And you know, if charges are going to be brought, fine. But I think that the concern we have is the breadth of those warrants were directed really to first amendment activities of those institutions. They were directed to any and all books, papers, pamphlets. It went through a whole list—if they referenced someone designated as a terrorist.

And I think that, you know, it's important that our criminal investigative powers be used aggressively to stop and prevent crime. But when you're talking about those kind of over-broad warrants directed at people that at least for 3 years have not been charged with anything, have not had their assets frozen, against those people, that we need to be careful about that.

And we need to be careful about sharing that information with intelligence agencies, and with foreign Government intelligence agencies, without any kind of judicial supervision. That's the point I was making.

Ms. WATERS. Well, yes. Well, let me just say that there are victims of the COINTELPRO operation, some of whom are still alive today in other countries, who have never gotten justice from the operation of the Justice Department; and in the way that the intelligence agencies basically undermined them, their privacy, and basically identified them as something—terrorists, or enemies of the state, you name it. I've always been concerned about that. And I just feel that maybe even some day we'll be able to bring that back to the Congress of the United States.

But having said that, let me just ask a broad question. Some of us visit Cuba all the time. Some of us like going to Cuba. And some of us spend hours with Fidel Castro; talking with him; getting to know him; asking him questions about the revolution; talking about what he refers to as the blockade; on and on and on and on. And we learn an awful lot.

Recently, I learned in the hearings that are taking place in the Senate that Mr. Bolton had tried to get the Intelligence Community to confirm that there were biological weapons being developed by the Cuban Government—which turns out not to have been true; but there was some attempt to get that done.

Now, if I'm visiting Cuba, or Members of Congress are visiting Cuba, we're meeting with Fidel Castro; we're talking with him. And an investigation is going on about the development of biologi-

cal weapons, etcetera. Are we then under investigation, also? How does it work?

Mr. SABIN. Well——[Laughter.]

Want me to take a stab at that? [Laughter.]

Ms. WATERS. Ha-ha-ha-ha. Yeah. How does it work?

Mr. SABIN. I mean, I think that's not directly related to the information-sharing provisions, and I think we are——

Ms. WATERS. Well, that's okay, you——

Mr. SABIN. And our scope——

Ms. WATERS. You are supposed to know these things.

Mr. SABIN. Well, actually, having come from South Florida, where I was the criminal chief and the first assistant, I am familiar with espionage cases that were brought against agents of the Fidel Castro regime that worked down in South Florida, for which we invoked the criminal process and obtained convictions against a group of spies that had infiltrated certain locations in South Florida.

So Congress has passed a specific series of statutes that you cannot undertake certain transactions with certain particular designated foreign nations. And there are exceptions to those broad restrictions. And it would depend upon the specific factual circumstances, as to who was going, whether you obtained a license from the office——

Ms. WATERS. We're going. We're legal. We go through the Treasury Department. They know we are there. We go down; we have dinner; we smoke a cigar with Fidel; we talk to him. Are we under surveillance?

Mr. EDGAR. Congresswoman, can I——

Mr. SABIN. I'm not looking at your activities, Congressman Waters. I can't speak for others.

Mr. EDGAR. I, obviously, can't answer that question; other than to say that, you know, what you're describing is, under the definition of the statute that we've been talking about, foreign intelligence. It's not just—like we said, it's not just criminal. Foreign intelligence means—I'm reading from Justice Department's testimony here—information relating to the capabilities, intentions, or activities of foreign governments, or elements thereof, foreign organizations, or foreign persons.

So certainly, anything about, not just Fidel, but any Cuban, would be a foreign person, and information about his intentions or capabilities. So, you know, it's certainly something that would be foreign intelligence information. So if it was acquired in a criminal investigation, it could be shared, under 203(d), 203(b), if it was acquired in a—you know, and it could be the basis, possibly, for a FISA wiretap.

Mr. MCCAUL. If I could comment—and I'm quoting from the FISA court of review's opinion. It's the only opinion, appellate opinion, from the FISA court. It says the definitions of agent of a foreign power and foreign intelligence information are crucial to understanding the statutory scheme.

And this is where I think we need to really focus on, because I think we're getting off track. It's information that relates to the ability of the United States to protect against actual or potential attack, or other grave hostile acts of a foreign power. That's one.

Ms. WATERS. Well, that fits my question.

Mr. MCCAUL. Sabotage or international terrorism. Number three, clandestine intelligence activities. And it further provides, this information necessary to the national defense or security of the United States.

Ms. WATERS. It all fits my question. I just—I set it up for you. And I told you about the suspicion that there were biological weapons that were being made. That's under investigation—let's say it's under investigation. We're traveling down there; we're meeting with him; we're talking with him. So what happens? Are we under surveillance? Are we under—do we become a part of that investigation?

How far does the roving wiretap extend? Does it extend from the person who is the subject of the investigation to other people who the subject is in contact with on an ongoing basis, on an official basis? How does all this stuff work?

Mr. COBLE. Ms. Waters, would you suspend for just a moment?

Ms. WATERS. Yes.

Mr. COBLE. I promised Mr. Sabin I'd get him back to Justice. Would you object, Ms. Waters, if they responded in writing?

Ms. WATERS. Yeah—but I'm going to let him go, because I know he knows. I can see that look on his face. [Laughter.]

He knows.

Mr. SABIN. [Laughs] Just read that look, Congressman.

Mr. COBLE. Well, I thank the gentleman.

Ms. WATERS. Okay, we'll have to excuse him. All right.

Mr. COBLE. Folks, it's been a good hearing.

Mr. SCOTT. Mr. Chairman?

Mr. COBLE. Yes, sir?

Mr. SCOTT. I just wanted to read the definition of "foreign intelligence information." It has a lot of clandestine activities, but information relating to the national defense or security of the United States. But it also says "or the conduct of the foreign affairs of the United States"; which could be anything. I mean, that could be a trade deal, trying to get somebody's bottom price on steel. That's the conduct of foreign affairs of the United States. And if that's your predicate for getting this roving wiretap, listening to everybody's information, that's a fairly casual——

Ms. WATERS. It's big.

Mr. COBLE. Well, this will be ongoing. I want to thank all of you. Mr. McCaul, this is a case of first impression. I just told Mr. Scott, you're the first Member I've ever known to give his testimony and stay until the last dog is hanged. [Laughter.]

So I thank you for that.

Mr. MCCAUL. I was asked to do so. And thank you, Mr. Chairman.

Mr. COBLE. Folks, we thank you all for your testimony. The Subcommittee very much appreciates it.

In order to ensure a full record and adequate consideration of this important issue, the record will be left open for additional submissions for 7 days. Also, any written questions that a Member wants to submit should be submitted within the same 7-day period.

This concludes the oversight hearing on "The Implementation of the USA PATRIOT Act, the Effect of sections 203(b) and (d) on In-

formation Sharing." Thank you for your cooperation, and the Subcommittee stands adjourned.

And Mr. Sabin, I hope you get back in time.

[Whereupon, at 5:10 p.m., the Subcommittee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

PREPARED STATEMENT OF THE HONORABLE ROBERT C. SCOTT, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF VIRGINIA, AND RANKING MEMBER, SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

Thank you, Mr. Chairman. I am pleased to join you in convening this hearing on subsections 203(b) and (d) of the USA PATRIOT Act. We sunsetted those provisions, along with a number of other provisions, where we were exposing the public to extraordinary federal government police powers to pry into and individual's private activities and spread information collected all over town without direct court supervision and oversight.

Our country's founders were leery of government power, particularly in the area of the criminal law. So, checks and balances were made an integral part of the criminal justice system to ensure citizens would be secure against unwarranted government intrusion into their private properties and affairs, and that the government could not easily prove crimes against accused persons, or accomplish a similar result by use of government powers to harass or smear a citizen.

Today, with the cost of legal representation and a contingent of the media eager to exploit sensationalism, mere suspicion or investigation of crime can result in much of that from which our founders sought to protect us. We will hear of an example of this type use of extraordinary government powers from one of our speakers today.

Mr. Chairman, as a compromise on not getting the level of judicial supervision and oversight many of us felt warranted in connection with the extension of these extraordinary powers, by unanimous vote of the full Committee, we voted to sunset these provisions after 2 years. This would allow us to exercise Congressional oversight of these extraordinary powers on a short leash. However, against the might of the Administration and the Senate, we ended up with a 4 year sunset. While I expect we will hear testimony about how useful the provisions have been, we will still not know much about the great bulk of information that is being shared, what percentage of it is useful, what use is made of it and what is being done with the information collected, that which is used and unused.

I look forward to the testimony of our witnesses and the light they will shed on these issues. Thank you.

PREPARED STATEMENT OF THE HONORABLE MAXINE WATERS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Mr. Chairman, the overwhelmingly tragic events of 9/11, demonstrated the need for better communication between law enforcement and the intelligence communities. The USA Patriot Act was enacted in response to those events in an atmosphere of fear. The Act was passed just six weeks after the September 11th attacks. Because Members of both parties recognized the potentially huge impact of the Patriot Act on civil liberties and basic constitutional protections, the Act included a "sunset" clause that provided that over a dozen of the Act's provisions will expire, unless Congress acts to renew them.

Mr. Chairman, I believe that the Patriot Act is a lopsided response to the events of 9/11 that requires significant correction. While the Act does encourage increased information sharing between law enforcement and intelligence agencies, it does not provide adequate safeguards to protect the constitutionally guaranteed rights of American citizens, including the rights to privacy. The lawful activities of innocent Americans are being swept up within the authorities created by the Act because we have failed to require a need before particularized showing of wiretaps are allowed.

Mr. Chairman, section 203 (b) and section 203 (d) of the Patriot Act provide no safeguards to protect our rights to privacy or our civil liberties. Neither section ensures proper oversight by judges of the sharing of information between law enforcement and intelligence agencies, or of the monitoring of the information obtained. More specifically, these sections 203 (b) and 203 (d) allow law enforcement agencies to share intercepted telephone and Internet conversations with intelligence agencies, but do not require a court order by a judge to authorize the sharing of this information. Furthermore, the CIA is not prohibited from providing this information freely-even to foreign intelligence operations.

Mr. Chairman, this Act has made our Federal Judiciary Branch a bystander and has relegated Federal judges to the sidelines. The Act and allows the Federal government to conduct investigations and to determine how to the handle any information obtained through such investigations, without any oversight. As a result, law enforcement and intelligence agencies may secretly spy on Americans and freely share the sensitive information gained through their investigative efforts with whomever they deem fit. There are absolutely no specified limitations on how the information gained was obtained and how it can or cannot be used or disseminated.

Mr. Chairman, as we consider whether to reauthorize the provisions of the Patriot Act that will sunset at the end of this year, we cannot be content to rest on simple assurances of good faith by the law enforcement and intelligence communities. We must restore a role for our judiciary that will allow them to protect the constitutional rights of all of our people.

Therefore, I look forward to hearing from our witnesses today to determine what steps are required to protect the civil liberties and privacy rights of all Americans, while still preserving the very important role of the Judicial Branch.

I yield back the balance of my time.

PREPARED STATEMENT OF THE HONORABLE SHEILA JACKSON LEE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

SHEILA JACKSON LEE
18TH DISTRICT, TEXAS

COMMITTEES:
SELECT COMMITTEE ON HOMELAND SECURITY
SUBCOMMITTEES:
INFRASTRUCTURE AND BORDER SECURITY
CYBERSECURITY, SCIENCE, AND RESEARCH & DEVELOPMENT

JUDICIARY
SUBCOMMITTEES:
CRIME
RANKING MEMBER
IMMIGRATION AND CLAIMS

SCIENCE
SUBCOMMITTEE:
SPACE AND AERONAUTICS

MEMBER
DEMOCRATIC CAUCUS POLICY AND STEERING COMMITTEE

TEXAS CHAIR
CONGRESSIONAL BLACK CAUCUS

Congress of the United States
House of Representatives
Washington, DC 20515

WASHINGTON OFFICE:
2435 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-3816

DISTRICT OFFICE:
1919 SMITH STREET, SUITE 1180
THE GEORGE "MICKEY" LELAND FEDERAL BUILDING
HOUSTON, TX 77002
(713) 655-0050

ACRES HOME OFFICE:
6719 WEST MONTGOMERY, SUITE 204
HOUSTON, TX 77019
(713) 691-4882

HEIGHTS OFFICE:
420 WEST 19TH STREET
HOUSTON, TX 77008
(713) 861-4070

Statement

By

Congresswoman Sheila Jackson Lee

Judiciary Subcommittee on Crime, Terrorism, and Homeland Security
"The Implementation of the USA Patriot Act Effect of Section 203 (b) and (d) on Information Sharing

Tuesday, April 19, 2005

2141 Rayburn House Office Building

3:00 p.m.

The attacks of September 11, 2001, demonstrated the need for more effective information sharing and coordination between law enforcement and the Intelligence Community agencies. The attacks also demonstrated the need to integrate the analysis of foreign and domestic intelligence information. Sections 203(b) and (d) of the USA PATRIOT Act responded to the need to improve information sharing and are scheduled to expire on December 31, 2005 unless Congress reauthorizes them.

As most of you are aware, Section 203(b) allows law enforcement to share foreign intelligence, counterintelligence, or foreign intelligence information obtained through a criminal wiretap with law enforcement, intelligence, protective, immigration, national defense, or national security personnel.

Further, Section 203(d) permits law enforcement officials to share foreign intelligence, counter intelligence, or foreign intelligence information obtain through a criminal investigation. It goes without saying that timely and accurate information about the activities, capabilities, plans and intentions of foreign powers, organizations and persons and their agents, is essential to the national security of the U.S. All reasonable and lawful means must be used to ensure that the U.S. will receive the best intelligence available. To this end, I look forward to hearing the testimony of our distinguished panel.

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
(Alexandria Division)

IN THE MATTER OF THE SEARCH OF:	)	
	)	
750 A Miller Drive Leesburg, VA	)	
	)	
1101 and 1105 Safa Street Herndon, VA	)	Case No. 02-MG-122
	)	
1514 Church Hill Place Reston, VA	)	
	)	
12528 and 12607 Rock Ridge Road Herndon, VA	)	
	)	
12541 Brown's Ferry Road Herndon, VA	)	
	)	
9034 Swift Creek Road Fairfax Station, VA	)	
	)	
305 Marjorie Lane Herndon, VA	)	
	)	
	)	
	)	

BRIEF *AMICUS CURIAE* OF THE AMERICAN CIVIL LIBERTIES UNION OF VIRGINIA, INC. IN SUPPORT OF MOTION FOR RETURN OF PROPERTY AND TO UNSEAL THE SEARCH WARRANT AFFIDAVIT

The American Civil Liberties Union of Virginia, Inc., *amicus curiae*, hereby files this brief in support of the movants' Motion for Return of Property and to Unseal the Search Warrant Affidavit.

INTEREST OF *AMICUS*

The American Civil Liberties Union of Virginia, Inc. ("ACLU of Virginia"), the Virginia affiliate of the American Civil Liberties Union, has approximately 5,000 members in the

Commonwealth of Virginia. Its mission is to safeguard and advance the individual rights of Virginia residents under the federal and state constitutions and civil rights statutes. Since its founding, the ACLU of Virginia has been a forceful advocate for the protection of the Fourth Amendment right to be free from unreasonable search and seizure and the First Amendment right to freedom of expression. The ACLU of Virginia has frequently appeared before this Court and the United States Court of Appeals for the Fourth Circuit both as *amicus curiae* and as direct representative for plaintiffs in civil rights and constitutional cases.

The ACLU of Virginia endorses wholeheartedly the movants' contention that the searches at issue violated their rights under the Fourth Amendment. In this brief, *amicus* focuses on one especially egregious aspect of this unconstitutional search: the wholesale seizure of books, pamphlets, scholarly works and other materials protected by the First Amendment.

FACTS

The movants' memorandum of law fully sets forth the facts. Of those facts, the following are most relevant to the First Amendment arguments herein:

1. In March 2002, federal agents searched three Islamic entities and ten Muslim homes pursuant to a warrant supported by a sealed affidavit.

2. Two of the entities that were searched have as their primary purpose activities protected by the First Amendment, i.e., the Graduate School of Islamic Thought and Social Sciences (GSISS), an institution of higher education, and the International Institute of Islamic Thought (IIIT), a non-profit academic and cultural institution concerned with general issues of Islamic thought.

3. The warrants authorized the seizure of, among other things:

- Any and all information referencing in any way [various individuals and organizations] and any other individual or entity designated as a terrorist by the President of the Untied States, the United States Department of Treasury, or Secretary of State;
- Any and all correspondence referencing in any way [various individuals and organizations] and any other individual or entity designated as a terrorist by the President of the Untied States, the United States Department of Treasury, or Secretary of State;
- Pamphlets, leaflets, booklets, video and audio tapes related to [various individuals and organizations] and any other individual or entity designated as a terrorist by the President of the Untied States, the United States Department of Treasury, or Secretary of State; and
- All computers and network equipment and peripherals, the software to operate them, and related instruction manuals.

4. The warrants did not specify which particular books, pamphlets, computer files, tapes or other written or recorded material were to be seized.

5. The agents executing the searches seized thousands of documents and other items presumptively protected by the First Amendment, including books, binders, computer disks, scholarly manuscripts, audio and videotapes, and mail delivered during the execution of the warrants.

6. Many of the seized items were written or recorded in Arabic. As far as the movants know, none of the agents participating in the search spoke or read Arabic.

7. The government inventories of the searches do not provide sufficient information to determine whether the things seized were within the scope of the search warrant, describing most items in general terms such as "cassette tapes," "photographs," "documents in Arabic," "video tapes," "folder with memos," "faxes, emails, memos, letters," "binders with information written in arabic," "folder of documents," "miscellaneous file folders," "contents of filing cabinets," "documents" "miscellaneous books and binders," "desk items."

8. The government inventories refer to some constitutionally protected material that is manifestly outside the scope of the warrants, e.g., "Sunday school emergency forms," and "one box of correspondences, *some* referring to Hamas" [implying correspondence not referring to Hamas was also seized].

7. Almost none of the seized items have been returned to the movants.

8. The affidavits supporting the search warrants remain sealed, and none of the movants has seen the affidavits or has any idea as to their contents.

ARGUMENT

The Supreme Court has long recognized that the inherent restraint on liberty imposed by any search or seizure is magnified when the items to be seized are written materials protected by the First Amendment. This principle reflects the historical fact that "the struggle for freedom of speech and press in England was bound up with the issue of the scope of the search and seizure power." *Marcus v. Search Warrants*, 367 U.S. 717, 724 (1961). In *Marcus*, the Court traced this history in some detail, beginning with the incorporation of the Stationers' Company in 1557, which was authorized to enter any building and seize all printed material that was "contrary to the form of any statute, act, or proclamation, made or to be made." 367 U.S. at 725 (quoting 1

Arber, Transcript of the Registers of the Company of Stationers of London, 1554-1640 A.D., p. xxxi). Broad search and seizure powers to suppress dissident writings were repeatedly reaffirmed by the Star Chamber and later during Oliver Cromwell's rule. *Id.* at 725-26.

After the Restoration, a new licensing act was enacted, under which government officials issued warrants for the seizure of persons and paper. "These warrants, while sometimes specific in content, often gave the most general discretionary authority," for example, "to search any house, shop, printing room, chamber, warehouse, etc. for seditious, scandalous or unlicensed pictures, books, or papers, to bring away or deface the same . . . " *Id.* at 726.

The use of such "general warrants" in England was finally overturned by Lord Camden in *Entick v. Carrington*, 19 How.St.Tr. 1029 (1765). Entick, a publisher of an opposition paper, was charged with seditious libel, and a warrant was issued for the seizure of all of his papers. Camden condemned the general warrant:

> This power so assumed by the secretary of state is an execution upon all the party's papers, in the first instance. His house is rifled; his most valuable secrets are taken out of his possession, before the paper for which he is charged is found to be criminal by any competent jurisdiction, and before he is convicted either of writing, publishing, or being concerned in the paper.

Marcus, 367 U.S. at 728, quoting *Entick v. Carrington*. In another warrant case, Lord Camden noted that a general warrant "is a discretionary power given to messengers to search wherever their suspicions may chance to fall. If such a power is truly invested in a secretary of state, and he can delegate this power, it certainly may affect the person and property of every man in this kingdom, and is totally subversive of the liberty of the subject." *Wilkes v. Wood*, 19 How.St.Tr. 1153 (1765), quoted in *Marcus*, 367 U.S. at 728-29. In a similar vein, a London pamphlet published in 1764 decried such warrants: "[W]here there is even a charge against one particular

paper, to seize all, of every kind, is extravagant, unreasonable and inquisitorial. It is infamous in theory, and downright tyranny and despotism in practice." 367 U.S. at 729 n. 22.

The Court concluded that "[t]he Bill of Rights was fashioned against the background of knowledge that unrestricted power of search and seizure could also be an instrument for stifling liberty of expression." *Id.* at 729.

After presenting the historical background, the Court in *Marcus* turned to the facts of the case, which involved a warrant authorizing police to seize all "obscene publications" from a bookstore. The search resulted in the seizure, and removal from the market, of hundreds of titles, two-thirds of which were ultimately held not to be obscene. *Id.* at 732. The Court faulted the warrant's broad grant of discretion, which left "to the individual judgment of each of the many police officers involved in the selection of such magazines as in his view constituted 'obscene . . . publications.'" *Id.* at 732. Search warrants pertaining to expressive writings are different from other search warrants, and "a State is not free to adopt whatever procedures it pleases for dealing with obscenity as here involved without regard to the possible consequences for constitutionally protected speech." *Id.* at 731.

These principles were reaffirmed in *Stanford v. Texas*, 379 U.S. 476 (1965), a case that strikingly resembles the case at bar. There, the Supreme Court struck down a search warrant that authorized the seizure of "any books, records, pamphlets, cards, receipts, lists, memoranda, pictures, recordings, or any written instruments concerning the Communist Party of Texas and the operations of the Communist Part in Texas." 379 U.S. at 486. Government officials searched the petitioner's home, from which he operated a mail order book business, and seized material sold by the business as well as the petitioner's personal books and pamphlets. *Id.* at 479. As in this case, they also seized "many of the petitioner's private documents and papers,

including his marriage certificate, his insurance policies, his household bills and receipts and the files of his personal correspondence." *Id.* at 480.

The Court found that "the warrant was of a kind which it was the purpose of the Fourth Amendment to forbid -- a general warrant." *Id.* The Court once again explained the Fourth Amendment's roots in the "history of conflict between the Crown and the press," concluding that

> what this history indispensably teaches is that the constitutional requirement that warrants must particularly describe the "things to be seized" is to be accorded the most scrupulous exactitude when the "things" are books, and the basis for their seizure is the ideas which they contain. No less a standard could be faithful to First Amendment freedoms.

Id. at 485 (citations omitted). Since *Marcus* and *Stanford*, the courts have repeatedly affirmed the need for the "most scrupulous exactitude" when warrants or subpoenas are issued for constitutionally protected materials. *See, e.g., Fort Wayne Books, Inc. v. Indiana*, 489 U.S. 46 (1989); *Lo-Ji Sales, Inc. v. State of New York*, 442 U.S. 319 (1979); *In re Grand Jury Subpoena*, 829 F.2d 1291 (4th Cir. 1987).

The present case parallels *Stanford* in that large numbers of books, pamphlets, tapes, and other items protected by the First Amendment were seized based on a suspicion of "subversiveness." As in *Stanford*, the warrants executed in this case were "general warrants." Indeed, the warrants' inclusion of all items "referencing in any way" the proscribed organizations here is virtually identical to the *Stanford* warrants.[1] The broad sweep of the warrants encompasses constitutionally protected materials that are irrelevant to any type of criminal activity, e.g.:

---

[1] The *Stanford* warrants: "books, records, pamphlets, cards, receipts, lists, memoranda, pictures, recordings, or any written instruments concerning the Communist Party of Texas and the operations of the Communist Part in Texas."
The warrants at issue here: "Pamphlets, leaflets, booklets, video and audio tapes related to" ; "Any and all correspondence referencing in any way"; and "Any and all information referencing in any way" various individuals and organizations.

- scholarly works about terrorist organizations,
- a biography of Osama bin Laden,
- books or pamphlets dealing with the history of the Islamic world for the last thirty years,
- books, letters, or pamphlets *condemning* terrorist activity,
- pamphlets describing reli ination against Muslims in America post-9/11.

Given the magnitude of the Septemb and their effect on the Muslim-American community, it would be surprising *not* to find documents "referring in any way" to terrorist organizations at any American entity engaged in the study of Islam or advocacy on behalf of Muslim-Americans. Such documents not only are not evidence of any crime, but are entitled to the highest First Amendment protection.

As in *Stanford*, "[t]he constitutional impossibility of leaving the protection of those freedoms to the whim of the officers charged with executing the warrant is dramatically underscored by what the officers saw fit to seize under the warrant in this case." 379 U.S. at 485. The agents here made no attempt to limit the scope of their search to potential evidence of a crime or to respect the boundaries of the First Amendment. Instead, they went so far as to seize large numbers of documents, books and pamphlets in Arabic, without any way of knowing whether they were within the scope of the warrant.[2]

The danger posed to the United States from terrorism is a serious matter of legitimate concern to law enforcement agencies. However, the particular dangers of the times does not justify the abandonment of fundamental First and Fourth Amendment freedoms, as the Supreme Court has repeatedly made clear. For example, in *United States v. United States District Court*, 407 U.S. 297 (1972), the Court forcefully rejected the Government's contention that they were

[2] The breadth of the search is aggravated by the fact that the affidavits supporting the warrants were, and still are, sealed. "An affidavit may provide the necessary particularity for a warrant if it is either incorporated into or attached to the warrant." *U.S. v. Washington*, 852 F.2d 803, 805 (4th Cir. 1988), quoting *Rickert v. Sweeney*, 813 F.2d 907, 909 (8th Cir. 1987).

not required to obtain warrants for electronic surveillance in domestic security matters. The Court noted that "[n]ational security cases . . . often reflect a convergence of First and Fourth Amendment values not present in cases of 'ordinary' crime. Though the investigative duty of the executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech." 407 U.S. at 313. Justice Douglas, concurring, made the point by invoking the same historical background cited in *Marcus* and *Stanford*:

> That 'domestic security' is said to be involved here does nto draw this case outside the mainstream of Fourth Amendment la. Rather, the recurring desire of reigning officials to employ dragnet techniques to intimidate their critics lies at the core of that prohibition. For it was such excesses as the use of general warrants and the writs of assistance that led to the ratification of the Fourth Amendment.

Id. at 327 (Douglas, J., concurring). His concluding sentence rings true today as it did thirty years ago: "We have as much or more to fear from the erosion of our sense of privacy and independence by the omnipresent . . . Government as we do from the likelihood that fomenters of domestic upheaval will modify or form of governing." *Id.* at 333.

CONCLUSION

As the movants have persuasively argued, the search warrants at issue here lack sufficient particularity as to all of the items to be seized. Even were this not the case, however, the warrants most certainly fail to provide the "most scrupulous exactitude" required for the seizure of things protected by the First Amendment.

For the foregoing reasons, *amicus* respectfully urges this Court to grant the Motion to Return Property and to unseal the search warrant affidavit.

Respectfully submitted,

_____
Rebecca K. Glenberg (VSB No. 44099)
American Civil Liberties Union
Foundation of Virginia, Inc.
6 North Sixth Street, Suite 400
Richmond, Virginia 23219
(804) 644-8080
(804) 649-2733 (FAX)

Attorney for Amicus American Civil Liberties Union of Virginia, Inc.