AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

IMPLEMENTATION OF THE USA PATRIOT ACT: SECTIONS OF THE ACT THAT ADDRESS THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA)

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 26 AND APRIL 28, 2005

Serial No. 109–17

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

20–875 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

HEARING DATES

	Page
Tuesday, April 26, 2005	
PART I	1
Thursday, April 28, 2005	
PART II	39

OPENING STATEMENT

APRIL 26, 2005

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
The Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan, and Ranking Member, Committee on the Judiciary	3

APRIL 28, 2005

The Honorable Howard Coble, a Representative in Congress from the State of North Carolina, and Chairman, Subcommittee on Crime, Terrorism, and Homeland Security	39
The Honorable Robert C. Scott, a Representative in Congress from the State of Virginia, and Ranking Member, Subcommittee on Crime, Terrorism, and Homeland Security	40
The Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan, and Ranking Member, Committee on the Judiciary	41

WITNESSES

APRIL 26, 2005

The Honorable Mary Beth Buchanan, United States Attorney, Western District of Pennsylvania, U.S. Department of Justice	
Oral Testimony	5
Prepared Statement	7
Mr. James A. Baker, Counsel for Intelligence Policy, U.S. Department of Justice	
Oral Testimony	13
Prepared Statement	15
Ms. Suzanne Spaulding, Managing Director, The Harbour Group, LLC	
Oral Testimony	19
Prepared Statement	20

APRIL 28, 2005

Mr. Kenneth L. Wainstein, interim U.S. Attorney, District of Columbia	
Oral Testimony	43
Prepared Statement	46

Page

Mr. James A. Baker, Counsel for Intelligence Policy, U.S. Department of Justice
Oral Testimony 55
Prepared Statement 57
Mr. Robert S. Khuzami, former Assistant U.S. Attorney, Southern District of New York
Oral Testimony 61
Prepared Statement 63
Mr. Gregory T. Nojeim, Associate Director/Chief Legislative Counsel, American Civil Liberties Union
Oral Testimony 67
Prepared Statement 69

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

APRIL 26, 2005

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 109
Prepared Statement of the Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan, and Ranking Member, Committee on the Judiciary 109
Letter from Jamie E. Brown, Acting Assistant Attorney General, U.S. Department of Justice, dated April 30, 2003, to the Honorable Orrin Hatch, Chairman, Committee on the Judiciary, United States Senate 111
Letter from Jamie E. Brown, Acting Assistant Attorney General, U.S. Department of Justice, dated March 5, 2003, to the Honorable Orrin Hatch, Chairman, Committee on the Judiciary, United States Senate 120
Letter from Daniel J. Bryant, Assistant Attorney General, U.S. Department of Justice, dated July 31, 2002, to the Honorable Bob Graham, Chairman, Select Committee on Intelligence, United States Senate, and the Honorable Richard C. Shelby, Vice-Chairman, Select Committee on Intelligence, United States Senate 121

APRIL 28, 2005

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 126
Prepared Statement of the Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan, and Ranking Member, Committee on the Judiciary 126
Redacted document ACLU received in response to a request under the Freedom of Information Act to disclose activity related to Transactional Records National Security Letters issued since October 26, 2001 128
Letter from William E. Moschella, Assistant Attorney General, U.S. Department of Justice to the Honorable Richard B. Cheney, President of the Senate, United States Senate 134
Letter from William E. Moschella, Assistant Attorney General, U.S. Department of Justice to L. Ralph Mecham, Director, Administrative Office of the United States Courts 136
Form National Security letter from the U.S. Department of Justice 138
Illustrations to show the implications of the PATRIOT Act and *Doe v. Ashcroft* on Section 2709 of the Electronic Privacy Act 140

IMPLEMENTATION OF THE USA PATRIOT ACT: SECTIONS OF THE ACT THAT ADDRESS THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA)

Part I

TUESDAY, APRIL 26, 2005

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

The Subcommittee met, pursuant to call, at 10 a.m., in Room 2141, Rayburn House Office Building, the Honorable Howard Coble (Chair of the Subcommittee) presiding.

Mr. COBLE. Good morning, ladies and gentlemen. This week the Subcommittee on Crime, Terrorism, and Homeland Security will continue to review its review of the USA PATRIOT Act by conducting three hearings.

These hearings will examine the provisions that affected the Foreign Intelligence Surveillance Act of 1978, popularly known as FISA. Today we will hear testimony on sections 204, 207, 214, and 225 of the PATRIOT Act.

Additionally, we have asked the witnesses to address sections 6001 and 6002 of the Intelligence Reform and Terrorism Prevention Act of 2001, which amended FISA. These sections are similarly set to expire on December 31 of this year.

The witnesses will discuss each provision in depth. With that in mind I will keep my comments brief and just mention the history of the Foreign Intelligence Surveillance Act of 1978. The Congress enacted the first Federal wiretap statute to prevent disclosures of Government secrets during World War I. Today, except under limited circumstances, it is unlawful to intercept oral, wire and electronic communications, access stored electronic communications, or use a pen register or trap and trace device.

It is furthermore unlawful to abuse electronic surveillance authority under the FISA. Today the U.S. Courts tend to use a two-pronged expectation of privacy analysis to determine whether the fourth amendment has, in fact, been violated.

This language is from Justice Harlan's concurrence in *Silverman* v. *United States,* in which he stated, and I quote, my understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first, that a person have exhibited

an actual or subjective expectation of privacy, and second, that the expectation be one that society is prepared to recognize as reasonable, close quote.

Consistent with the fourth amendment, the Congress created statutory procedures to allow limited law enforcement access to private communications and communication records. Today under title III of the Omnibus Crime Control and Safe Streets Act of 1968, it is a Federal crime to intercept wire, oral, or electronic communications of another without court approval, unless one of the parties consents.

It is also a Federal crime to disclose any information illegally obtained. The Crime Control Act did not cover national security cases, however. In 1978, the Foreign Intelligence Surveillance Act was enacted to set standards for foreign intelligence investigations.

FISA authorized the Government to collect intelligence within the United States on foreign powers and agents of foreign powers. FISA also established a special court to review and authorize or deny wiretapping and other forms of electronic eavesdropping for purposes of foreign intelligence gathering in domestic intelligence cases.

While the PATRIOT Act updated the FISA, it did not change the procedures against abuse. Before and after the enactment of the PATRIOT Act, FISA still requires advanced judicial approval for electronic surveillance and physical searches with limited exceptions.

FISA still requires a high-ranking Government official to sign and certify each FISA application. FISA still requires the Attorney General or his or her deputy to personally sign and approve every FISA application. FISA still requires that the Government must have probable cause to believe that a FISA target is an agent of a foreign power as defined by the statute.

And, if the target is also a U.S. Citizen, FISA still requires the Government to show that the target is engaged in criminal activity, such as international terrorism, sabotage or espionage, in addition to being an agent of a foreign power.

With this background on FISA, I look forward to hearing the testimony from the witnesses, and now recognize the distinguished gentlemen from Virginia, the Ranking Member, Mr. Bobby Scott, for his statement.

Mr. SCOTT. Thank you, Mr. Chairman, for holding this hearing on the issues before us today, in the context where we have actually broken down the wall that existed between foreign intelligence gathering, particularly foreign intelligence, and criminal proceedings, to give the Government broad authority to collect and share information, mostly secret.

I am concerned that we have also blurred the traditional line of protection for freedoms and privacy. While I agree that some lifting of traditional restrictions in this area may be justified in order to induce Government to better use the authorities it already has, I am also mindful that those restrictions were placed there for good reason.

We have seen in the past the COINTELPRO, Watergate, FBI spying on Martin Luther King, Jr., and other incidents as an exam-

ple of what can occur if we do not keep tight enough rein on Government's use of extraordinary power.

We should not have to experience those problems again in order to ensure that such abuses do not occur. Some of the provisions today reflect a trend that is troubling, the trend of Government to justify an ever-increasing extension of extraordinary powers based on convenience. We are considering time frames for surveillance operations that have been extended even more since the PATRIOT Act extensions, all because the Government says it is too costly for it to have to justify extensions in court, even under the low burden of the FISA court.

If we can commit to speed to spend billions of dollars in prisons and other law enforcement costs just to codify sound bites urged by the Department, we can certainly spend time and expense that it takes to ensure our privacy and freedoms are not unduly abridged.

And, Mr. Chairman, I believe it is important that we be safe and maintain our privacy and freedoms, and I don't think we should have to operate under the premise that we have to give up one in order to get the other.

So, Mr. Chairman, I look forward to the testimony by witnesses on the provisions before us today, to learn how they are being used and how these extraordinary powers can be authorized, whether or not the sufficient oversight is being undertaken, and whether the powers are used in a way to protect our safety as well as privacy and freedoms. And I thank you again for calling the hearing.

Mr. COBLE. I thank the gentleman from Virginia. We have been joined by the distinguished gentleman from Michigan, the Ranking Member of the full Committee. Mr. Conyers, do you have an opening statement?

Mr. CONYERS. Just a comment. Thank you, Chairman Coble. We have three Members and three witnesses, so we all get a chance to make a comment.

I come here in support of expiration. There are three areas that I would like to see expire and not be renewed. One is section 207, one is section 214, and the other is the Lone Wolf provision, and I would like everybody to try to make it as clear as they can why they agree with me, hopefully.

Section 207 allows secret surveillance up to a year. The justification for allowing the extraordinary intrusions under the Foreign Intelligence Surveillance Act is the extensive judicial oversight by the FISA court. This section takes that reasonable oversight away and gives the Justice Department authority to surveil suspects long after the relevant issues, the facts have expired, and I think that is not good.

I look forward to hearing why section 214 should be reauthorized. Pen register and trap and trace orders no longer are needed to be aimed at an agent of a foreign power under this provision and are available under the vague standard of relevance. This is even more troublesome in light of how the PATRIOT Act has permanently expanded these orders to allow the Government to record the websites a person visits, and addresses and subject headings of the e-mails that are sent and received.

And, finally, I hope that we examine the Lone Wolf provision, also set to expire this year, where a person need not be required to be connected with a terrorist organization.

FISA allows the secret surveillance, search and seizure, only because it is necessary to protect us from foreign powers. To expand FISA to apply to those who by definition have no connection to a foreign power starts law enforcement down a very obvious slippery slope.

And those are my comments, Chairman Coble. I thank you for this opportunity.

Mr. COBLE. I thank the gentleman from Michigan.

Ladies and gentleman, it is the practice of the Subcommittee to swear in all witnesses appearing before us. 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.

You may be seated. Today we have three distinguished witnesses. Our first witness is Mary Beth Buchanan, United States Attorney for the Western District of Pennsylvania.

Ms. Buchanan has this distinction of being the first woman in Pennsylvania's history for this presidentially appointed position. Prior to her appointment as U.S. Attorney, Ms. Buchanan was an Assistant U.S. Attorney.

From 1992 to 2001, Ms. Buchanan served in the Criminal Division representing the United States in the prosecution of both financial and violent crimes. Ms. Buchanan is a graduate of the California University of Pennsylvania and the University of Pittsburgh School of Law.

Our second witness is Mr. James A. Baker. Mr. Baker has been a Counsel For Intelligence Policy in the Office of Intelligence Policy and Review at the Department of Justice since 2002.

He served as Acting Counsel from May 2001 until January of 2002. Prior to that he was OIPR's Deputy Counsel for Intelligence Operations. Prior to joining OIPR, he served as a Federal prosecutor handling numerous international white collar crimes for the Criminal Division of the Department of Justice.

Mr. Baker was awarded his undergraduate degree from the University of Notre Dame and his J.D. And M.A. From the University of Michigan.

Our final witness today is Ms. Suzanne Spaulding, the Managing Director at the Harbour Group. Recently Ms. Spaulding worked as the Executive Director of the two Congressionally mandated Commissions, the National Commission on Terrorism and the Commission to Assess the Organization of the Federal Government to Combat the Proliferation of Weapons of Mass Destruction.

Ms. Spaulding received her undergraduate and law degrees from the University of Virginia.

Now, ladies and gentlemen, as you all have previously been told, we operate by the 5-minute rule here. Your testimony has been reviewed and will be rereviewed. So if you could comply with that 5-minute rule. We impose the same 5-minute rule against us when questioning you all. So when we examine you, if you can be as

terse as possible that will speed matters along. I do not mean to hold a stopwatch on you, but we have things to do today.

So, Ms. Buchanan, you will start off. When the amber light appears that will advise you that you have a minute to go, and when the red light appears that indicates that the ice on which you are skating has become very thin.

Just a minute. If you will suspend, Ms. Buchanan, we have been joined by our friend from Massachusetts, Mr. Delahunt.

Ms. Buchanan, you are recognized for 5 minutes.

TESTIMONY OF THE HONORABLE MARY BETH BUCHANAN, UNITED STATES ATTORNEY, WESTERN DISTRICT OF PENNSYLVANIA, U.S. DEPARTMENT OF JUSTICE

Ms. BUCHANAN. Thank you, Mr. Chairman, Ranking Member Scott, Members of the Subcommittee. I am Mary Beth Buchanan, the United States Attorney for the Western District of Pennsylvania, and also the Director of the Executive Office for United States Attorneys.

It is an honor to appear before you today to discuss the necessary provisions of the USA PATRIOT Act. As you know, there are three main themes of the PATRIOT Act: First, to facilitate the sharing of information between law enforcement and the intelligence communities; second, to modernize our legal tools to keep pace with technology; and, third, to create parity between the criminal law and the national security laws.

My remarks today will focus primarily on this third theme. Section 214 of the PATRIOT Act deals with the use of pen registers and trap and trace devices under FISA. A pen register is a device that can track dialing, routing, addressing, and signaling information about a telephone or Internet communication.

For example, which numbers are dialed from a particular telephone. A trap and trace device gathers the telephone numbers which call a particular telephone. In neither situation is content information collected. These devices are commonly used in the early stages of a criminal investigation to reveal who is talking to whom, and they can only be used upon certification to a judge that the information is relevant to an ongoing criminal investigation.

The information obtained often forms the building blocks supporting the issuance of search warrants and wiretap orders, and may also be very valuable at trial to show the connection between coconspirators.

The process for obtaining authorization for pen register or trap and trace from the FISA court is similar under section 214. The Government must show that the FISA court—or must show the FISA court that the information sought is relevant to an intelligence investigation. The FISA law, however, prohibits investigations of United States persons which are based solely upon activities that are protected by the first amendment.

Let me give you two examples of how pen registers have been used in criminal cases in my district. The first example is a domestic terrorism case in which David Wayne Hull, a self-declared imperial wizard of the Ku Klux Klan was convicted and sentenced to 12 years in prison for illegal possession of firearms and destructive devices.

In that case, the use of pen registers and trap and trace devices showed that Hull was in frequent telephone contact with other members of a white supremacist organization, not only in Pennsylvania but in four other States. These tools eventually helped to obtain search warrants and title III orders and to convict Hull for those offenses.

Pen register information was also very essential to develop probable cause for a wiretap in a large multi-year drug investigation. Fifty-one defendants, responsible for bringing thousands of kilograms of cocaine and heroin into the Western District of Pennsylvania were convicted on money laundering, drug and firearm charges.

The pen registers helped to develop the probable cause to establish that these individuals were communicating with one another in order to transact their drug trafficking business. This information led to wiretaps and ultimately resulted in the conviction of all 51 defendants. In fact, most of the defendants pled guilty because they realized they had no defense to the charges.

More importantly, this case had a substantial impact upon the Western District of Pennsylvania. The availability of heroin and cocaine was dramatically reduced. In fact, the heroin overdose deaths declined from 138 in 2001 to 46 in 2003.

These are just a few examples to show how important these tools can be in criminal investigations. The same tools must be available in national security investigations. Prior to the passage of the PATRIOT Act, FISA required the Government to certify that the facilities to be monitored had been used or were about to be used to contact a foreign agent or an agent of a foreign power.

Thus, this was a much higher standard and a much higher showing than was ever required under the criminal law to obtain a pen register or a trap and trace order. I hope that you will agree that terrorism investigations should be on equal footing with criminal investigations.

Section 214 of the PATRIOT Act does just that. We must continue to pursue the terrorists with every legal means available. We need the important tools of the PATRIOT Act to keep our Nation safe from terror attack.

I thank the Committee for its continued leadership and support, and I would be glad to answer your questions. Thank you.

[The prepared statement of Ms. Buchanan follows:]

PREPARED STATEMENT OF MARY BETH BUCHANAN

MARY BETH BUCHANAN

UNITED STATES ATTORNEY

WESTERN DISTRICT OF PENNSYLVANIA

PREPARED REMARKS FOR THE

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

COMMITTEE ON THE JUDICIARY

UNITED STATES HOUSE OF REPRESENTATIVES

APRIL 26, 2005

INTRODUCTION

Mr. Chairman, Ranking Member Scott, Members of the Subcommittee, thank you for asking me here today. I am Mary Beth Buchanan, the United States Attorney in the Western District of Pennsylvania and the Director of the Executive Office for United States Attorneys. It is an honor to appear before you today to discuss how the Department has used the important provisions of the USA PATRIOT Act to better combat terrorism and other serious criminal conduct. I will specifically focus today on two of the provisions that are the subject of today's hearing – Section 214 and Section 225 of the USA PATRIOT Act – since those are two provisions that harmonized tools used in terrorism investigations with tools that have been used routinely and effectively in criminal prosecutions long before the passage of the USA PATRIOT Act.

Section 214 of the USA PATRIOT Act allows the government to obtain a pen register order in national security investigations where the information likely is relevant to an international

terrorism or espionage investigation. This provision is similar to the 1986 criminal pen register statute (18 U.S.C. § 3121) that has been frequently used by criminal prosecutors to obtain pen registers and trap and trace devices in a variety of criminal investigations. A pen register is a device that can track dialing, routing, addressing, and signaling information about a communication – for example, which numbers are dialed from a particular telephone. Pen registers are not used to collect the content of communications. Similarly, a trap-and-trace device tracks numbers used to call a particular telephone, without monitoring the substance or content of the telephone conversation. Both devices are routinely used in criminal investigations where, in order to obtain the necessary order authorizing use of the device, the government must show simply that the information sought is relevant to an ongoing investigation.

Pen registers and trap and trace devices have long been used as standard preliminary investigative tools in a variety of criminal investigations and prosecutions. In many instances, these tools are used as one of the first steps in a criminal investigation with the information gathered used to determine if more intrusive forms of surveillance, such as search warrants or wiretaps, are justified. Use of these tools may oftentimes lead investigators and prosecutors to additional suspects or targets in an investigation because of their important ability to allow prosecutors to link defendants or "connect the dots" in a conspiracy or other type of criminal offense.

To obtain a pen register or trap and trace device under 18 U.S.C. § 3121 *et seq.*, a criminal prosecutor must certify that the information sought is relevant to an ongoing criminal investigation, and upon that certification, the court enters an *ex parte* order authorizing the installation and use of a pen register or a trap and trace device. There is no requirement that the

court make a probable cause finding. Under long-settled Supreme Court precedent, the use of pen registers does not constitute a "search" within the meaning of the Fourth Amendment. As such, the Constitution does not require that the government obtain court approval before installing a pen register. The absence of a probable cause requirement is justified because the devices merely obtain information that is voluntarily disclosed to the telephone service provider. Therefore, there is no reasonable expectation of privacy in the information.

Currently under FISA, government officials similarly may seek a court order for a pen register or trap-and-trace device to gather foreign intelligence information or information about international terrorism or espionage. Prior to enactment of the USA PATRIOT Act, however, FISA required government personnel to certify not just that the information they sought was relevant to an intelligence investigation, but also that the facilities to be monitored had been used or were about to be used to contact a foreign agent or an agent of a foreign power, such as a terrorist or spy. Thus, it was much more difficult to obtain an effective pen register or trap-and-trace order in an international terrorism investigation than in a criminal investigation.

Section 214 of the USA PATRIOT Act brought authorities for terrorism and other foreign intelligence investigations more into line with similar criminal authorities by permitting court approval of FISA pen registers and trap-and-trace orders even though an applicant might be unable to certify at that stage of an investigation that the facilities themselves, such as phones, are used by foreign agents or those engaged in international terrorist or clandestine intelligence activities. Significantly, however, applicants must still certify that the devices are likely to obtain foreign intelligence information not concerning a U.S. person, or information relevant to an international terrorism investigation. Section 214 streamlined the process for obtaining pen

registers under FISA while preserving the existing court-order requirement that is evaluated by the same relevance standard as in the criminal context. Now as before, investigators cannot install a pen register unless they apply for and receive permission from the FISA Court. In addition, Section 214 explicitly safeguards First Amendment rights. It requires that any investigation of a United States person not be conducted solely upon the basis of activities protected by the First Amendment to the Constitution. As a result, the Department of Justice must satisfy the FISA Court that its investigation is not solely based upon First Amendment protected activity, which requires the Department to inform the Court of the justification for the investigation.

If Section 214 were allowed to expire, it would be more difficult to obtain a pen register order in an international terrorism investigation than in a criminal investigation, and investigators would have a harder time developing leads in important terrorism investigations.

Section 225 of the USA PATRIOT Act also harmonized the FISA context and criminal prosecutions--in this case extending an important provision used for years in criminal prosecutions to the FISA context. The United States may obtain electronic surveillance and physical search orders from the FISA Court concerning an entity or individual whom the court finds probable cause to believe is an agent of a foreign power. Generally, however, as in the case of criminal wiretaps and electronic surveillance, the United States requires the assistance of private communications providers to carry out such court orders. In the criminal and civil contexts, those who disclose information pursuant to a subpoena or court order are generally exempted from liability. For example, those assisting the government in carrying out criminal investigative wiretaps are provided with immunity from civil liability. This immunity is important because it

helps to secure the prompt cooperation of private parties with law enforcement officers to ensure the effective implementation of court orders.

Prior to the passage of the USA PATRIOT Act, however, while those assisting in the implementation of criminal wiretaps were provided with immunity, no similar immunity protected those companies and individuals assisting the government in carrying out surveillance orders issued by the FISA Court under FISA. Section 225 ended this anomaly by providing immunity to those who assist the government in implementing FISA surveillance orders, thus ensuring that such entities and individuals will comply with orders issued by the FISA Court without delay. This immunity is important because it helps to secure the prompt cooperation of private parties, such as telephone companies, whose assistance is necessary for the effective implementation of court orders. For example, in the investigation of an espionage subject, the FBI was able to convince a company to assist in the installation of technical equipment pursuant to a FISA order by providing a letter outlining the immunity from civil liability associated with complying with the FISA order. Section 225 has been praised for protecting those companies and individuals who are simply fulfilling their legal obligations. If section 225 is allowed to expire, it would be more difficult for the Department of Justice to implement FISA surveillance orders in a timely and effective manner. Because Section 225 simply extends to the FISA context the exemption long applied in the civil and criminal contexts, where individuals who disclose information pursuant to a subpoena or court order generally are immune from liability for disclosure, it should be made permanent.

I thank you for inviting me here and giving me the opportunity to explain in concrete terms how the USA PATRIOT Act has changed the way we fight terrorism. I hope you agree that there is no good reason for investigators to have fewer tools to use in terrorism investigations than they have long used in criminal investigations. Fortunately, the USA PATRIOT Act was passed by Congress to correct these flaws in the system. Now that we have fixed this process, we can't go back. We must continue to pursue the terrorists with every legal means available. The law enforcement community needs the important tools of the USA PATRIOT Act to continue to keep our nation safe from attack.

I thank this Committee for its continued leadership and support. I will be happy to respond to any questions you may have.

Mr. COBLE. Thank you, Ms. Buchanan. Mr. Baker, you are recognized for 5 minutes.

TESTIMONY OF JAMES A. BAKER, COUNSEL FOR INTELLIGENCE POLICY, U.S. DEPARTMENT OF JUSTICE

Mr. BAKER. Thank you, Mr. Chairman. Chairman Coble, Ranking Member Scott and Members of the Committee, I am pleased to be here today to discuss the Government's use——

Mr. COBLE. Mr. Baker, if you will suspend just a minute. We have been joined by the distinguished gentleman from Ohio, Mr. Chabot.

Go ahead, Mr. Baker. I won't penalize you for those 10 seconds, Mr. Baker.

Mr. BAKER. Thank you, sir.

I am pleased to be here today to discuss the Government's use of the authorities granted to it by Congress under FISA, including the amendments to FISA under the USA PATRIOT Act and the Intelligence Reform Act of 2004. Those provisions have made a critical contribution to our ability to protect the national security of the United States consistent with the need to protect the privacy of Americans.

They affect nearly every FISA application that we file, and we ask you to renew them. As the Chairman mentioned, I am the Counsel for Intelligence Policy and the head of Office of Intelligence Policy and Review at the Department of Justice.

OIPR, as we are known, conducts oversight of the intelligence and counterintelligence activities of the executive branch agencies, including the FBI, and my office prepares and presents to the FISA court all FISA applications, and we represent the United States before the FISA court.

I report directly to the Deputy Attorney General. I am a career member of the Senior Executive Service and not a political appointee.

Rather than reading my written statement into the record today, I would just like to make a few observations about FISA that I think will be helpful to our discussion generally today. First, I would just like to mention the overall purpose of FISA. As the Chairman discussed, FISA was enacted in 1978 to provide legislative authorization for and regulation of all electronic surveillance conducted in the United States for foreign intelligence purposes. FISA was not intended to prohibit the collection of important foreign intelligence information, but rather to subject such collection to statutory procedures.

Over the years, Congress has expanded the scope of FISA. In 1994 it was expanded to cover physical searches, in 1998 to provide for separate authorization for pen registers and access to certain business records. In 2001, of course, we have the PATRIOT Act that we are all familiar with and why we are here today.

In addition to that purpose of FISA, I would like to make clear, to describe that FISA established clear standards for who could be a target under FISA. Since 1978, the only authorized targets of full content FISA collection have been foreign powers and agents of foreign powers. Those terms are defined terms under the act. The PATRIOT Act did not change the definition of those terms.

As you know, section 6001 of the Intelligence Reform Act did change one of the definitions of an agent of foreign power to include a non-U.S. Person who engages in international terrorism or activities in preparation therefor. This is the so-called Lone Wolf provision that we will discuss today.

Similarly, FISA only permits the use of other collection activities, such as pen registers, when there is a sufficient nexus between the information that will be collected and a legitimate intelligence investigation. And when the investigation involves a U.S. Person, it cannot be based solely on first amendment activities.

In addition, FISA includes various provisions to ensure accountability for the authorizations that are approved under FISA. It includes mechanisms, several mechanisms to ensure written accountability within the executive branch for the decision to engage in foreign intelligence collection. This serves as a check on executive branch arbitrariness. For example, each full content FISA application must have a certification from a high ranking official and must be signed by the—personally signed by the Attorney General or his Deputy. And FISA's other provisions also include mechanisms to ensure accountability.

In addition, there is judicial oversight of our activities under FISA. Whenever a surveillance or a search for foreign intelligence purposes may involve the fourth amendment rights of any U.S. Person, approval for such collection must come from a neutral and detached Federal judge.

Moreover, even when such fourth amendment rights are not implicated, such as for pen register data, FISA still requires approval by a Federal judge or magistrate before the Government can engage in such collection.

Finally, I would like to highlight some additional privacy protections that are in FISA, and they are known as minimization requirements. The Government may only conduct a full content surveillance or search when there are adequate procedures in place to minimize the intrusion into the privacy of U.S. Persons. Each application that we file for full content collection must include specific minimization procedures that are approved by the Attorney General, are reasonable in their design, and minimize the acquisition, retention and dissemination of information about U.S. Persons, consistent with the need of the Government to obtain, produce, and disseminate foreign intelligence. In each case, the Federal judge orders the Government to follow those procedures.

With these principles in mind, I am happy to answer any questions the Committee may have on our use of FISA and the authorities granted to us by Congress in the PATRIOT Act and the Intelligence Reform Act.

[The prepared statement of Mr. Baker follows:]

PREPARED STATEMENT OF JAMES A. BAKER

Testimony of James A. Baker, Counsel for Intelligence Policy
Office of Intelligence Policy and Review
United States Department of Justice
Committee on the Judiciary, before the
Subcommittee on Crime, Terrorism, and Homeland Security
United States House of Representatives
April 26, 2005

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

I am pleased to be here today to discuss the government's use of authorities granted to it by Congress under the Foreign Intelligence Surveillance Act of 1978 (FISA). In particular, I appreciate the opportunity to have a candid discussion about the impact of the amendments to FISA under the USA PATRIOT Act and how critical they are to the government's ability to successfully prosecute the war on terrorism and prevent another attack like that of September 11 from happening again.

As Counsel for Intelligence Policy in the Department of Justice, I am head of the Office of Intelligence Policy and Review (OIPR). OIPR conducts oversight of the intelligence and counterintelligence activities of the Executive Branch agencies including the FBI. We prepare all applications for electronic surveillance and physical search under FISA and represent the government before the Foreign Intelligence Surveillance Court (FISA Court). OIPR reports directly to the Deputy Attorney General. I am a career member of the Senior Executive Service, not a political appointee.

I. FISA Statistics

First, we would like to talk with you about the use of FISA generally. Since September 11, the volume of applications to the FISA Court has dramatically increased.

- In 2000, 1,012 applications for surveillance or search were filed under FISA. By comparison, in 2004 we filed 1,758 applications, a 74% increase in four years.

- Of the 1,758 applications made in 2004, none were denied, although 94 were modified by the Court in some substantive way.

II. Key Uses of FISA Authorities in the War on Terrorism

In enacting the USA PATRIOT Act, the Intelligence Authorization Act for Fiscal Year 2002, and the Intelligence Reform and Terrorism Prevention Act of 2004, Congress provided the government with vital tools that it has used regularly and effectively in its war on terrorism. The reforms in those measures affect every single application made by the Department for electronic surveillance or physical search authorized regarding suspected terrorists and have enabled the government to become quicker and more flexible in gathering critical intelligence information

on suspected terrorists. It is because of the key importance of these tools to winning the war on terror that the Department asks you to reauthorize the USA PATRIOT Act provisions scheduled to expire at the end of this year. Today, it is my understanding that the Committee wishes to discuss sections 204 and 207 of the USA PATRIOT Act. These provisions are scheduled to sunset at the end of the year. In addition, the Intelligence Reform and Terrorism Prevention Act of 2004 includes a "lone wolf" provision that expands the definition of "agent of a foreign power" to include a non-United States person who engages in international terrorism or in activities in preparation therefor and is not known to be affiliated with a larger group. This provision is also scheduled to sunset at the end of this year, and the Department asks that it be reauthorized as well.

A. Section 204 "Clarification of Intelligence Exceptions from Limitations on Interceptions and Disclosure of Wire, Oral and Electronic Communications"

Section 204 of the USA PATRIOT Act amended Title 18, United States Code, Sec. 2511 (2)(f) in two ways. First, it provides that chapter 206 of title 18, which governs the installation and use of pen registers and trap-and-trace devices, is not intended to interfere with certain foreign intelligence activities that fall outside of the definition of "electronic surveillance" in FISA. Second, section 204 provides that the exclusivity provision in section 2511(2)(f) of title 18 applies not only to the interception of wire and oral communications, but also to the interception of electronic communications. Section 2511(2)(f) reflects Congress's intent, when it enacted FISA and the Electronic Communications Privacy Act of 1986, to make the procedures in chapter 119 of title 18 ("Title III") (regulating the interception and disclosure of wire, electronic, and oral communications), chapter 121 of title 18 (regulating access to stored wire and electronic communications and transactional records), and FISA (regulating electronic surveillance undertaken to acquire foreign intelligence information) the exclusive procedures for conducting electronic surveillance, as defined by FISA, and intercepting certain types of domestic communications.

Section 204 remedies an apparent omission in the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848, which, among other things, amended chapter 119 of title 18 ("Title III") to provide procedures for intercepting electronic communications and added chapter 121 to title 18 to provide procedures for accessing stored electronic communications, but neglected to make a corresponding change to clarify that the exclusivity provisions in section 2511(2)(f) applies to the interception of not only wire and oral, but also electronic, communications.

Section 204 has been criticized by some opponents of the USA PATRIOT Act. For instance, some have argued that the section amended Title III and the Stored Communications Access Act so that stored voice-mail communications, like e-mail, may be obtained by the government through a search warrant rather than through more stringent wiretap orders. These critics, however, confuse section 204 with section 209 of the Act.

In reality, section 204, as the nonpartisan Congressional Research Service has observed, is "essentially a technical amendment" that merely clarifies what Congress had always intended

the statute to mean. In an age when terrorists use electronic communications just like everyone else, it is important to preserve section 204.

B. Authorized Periods for FISA Collection

Section 207 of the USA PATRIOT Act has been essential to protecting the national security of the United States and protecting the civil liberties of Americans. It changed the time periods for which some electronic surveillance and physical searches are authorized under FISA, and in doing so, conserved limited OIPR and FBI resources. Instead of devoting time to the mechanics of repeatedly renewing FISA applications in certain cases -- which are considerable -- those resources can be devoted to other investigative activity as well as conducting appropriate oversight of the use of intelligence collection authorities at the FBI and other intelligence agencies. A few examples of how section 207 has helped are set forth below.

Since its inception, FISA has permitted electronic surveillance of an individual who is an agent of foreign power based upon his status as a non-United States person who acts in the United States as "an officer or employee of a foreign power, or as a member" of an international terrorist group. As originally enacted, FISA permitted electronic surveillance of such targets for initial periods of 90 days, with extensions for additional periods of up to 90 days based upon subsequent applications by the government. In addition, FISA originally allowed the government to conduct physical searches of any agent of a foreign power (including United States persons) for initial periods of 45 days, with extensions for additional 45-day periods.

Section 207 of the USA PATRIOT Act changed the law to permit the government to conduct electronic surveillance and physical search of certain agents of foreign powers and non-resident alien members of international groups for initial periods of 120 days, with extensions for periods of up to one year. It also allows the government to obtain authorization to conduct physical search regarding any agent of a foreign power for periods of up to 90 days. Section 207 did <u>not</u> change the time periods applicable for electronic surveillance of United States persons, which remain at 90 days. By making these time periods for electronic surveillance and physical search equivalent, it has enabled the Department to file streamlined combined electronic surveillance and physical search applications that, in the past, were tried but abandoned as too cumbersome to do effectively.

As the Attorney General testified before the Senate Judiciary Committee earlier this month, we estimate that the amendments in section 207 have saved OIPR approximately 60,000 hours of attorney time in the processing of applications. Because of section 207's success, the Department has proposed additional amendments to increase the efficiency of the FISA process. Among these would be to allow coverage of a non-U.S. person for 120 days initially with each renewal of such authority allowing continued coverage for one year. Had this and other proposals been included in the USA PATRIOT Act, the Department estimates that an additional 25,000 attorney hours would have been saved in the interim. Most of these ideas were specifically endorsed in the recent report of the WMD Commission. The WMD Commission

agreed that these changes would allow the Department to focus its attention where it is most needed and to ensure adequate attention is given to cases implicating the civil liberties of Americans. Section 207 is scheduled to sunset at the end of this year.

C. The "Lone Wolf" Provision

In addition to the USA PATRIOT Act provisions scheduled to sunset at the end of this year, the "lone wolf" provision of the Intelligence Reform and Terrorism Prevention Act of 2004 is also scheduled to sunset. Before passage of this provision, FISA prevented the FBI from obtaining a surveillance order of an international terrorist unless it could establish a connection to a foreign power. However, a lone wolf terrorist seeking to attack the United States may not be connected to a foreign power, or his connection to a foreign power may not be known. This provision applies only to non-U.S. persons engaging or preparing to engage in international terrorism, and FISA Court authorization is still required to monitor lone wolf terrorists.

Senator Schumer stated during the Senate debate on the lone wolf provision: "Right now we know there may be terrorists plotting on American soil. We may have all kinds of reasons to believe they are preparing to commit acts of terrorism. But we cannot do the surveillance we need if we cannot tie them to a foreign power or an international terrorist group. . . . It makes no sense. The simple fact is, it should not matter whether we can tie someone to a foreign power. . . . Engaging in international terrorism should be enough for our intelligence experts to start surveillance."

A lone wolf, or one who appears to be a lone wolf, may have the capacity to cause grievous harm to America and her citizens, and the threat posed by lone wolf terrorists will not disappear at the end of this year. Therefore, the Department requests that this provision be made permanent.

CONCLUSION

It is critical that the elements of the USA PATRIOT Act subject to sunset in a matter of months be renewed. The USA PATRIOT has greatly enhanced the ability of OIPR, as well as prosecutors, the FBI, and the Intelligence Community, to effectively wage the war on terrorism.

I thank the Committee for the opportunity to discuss the importance of the USA PATRIOT Act to this nation's ongoing war against terrorism. I appreciate the Committee's close attention to this important issue. I would be pleased to answer any questions you may have. Thank you.

Mr. COBLE. Thank you, Mr. Baker. Ms. Spaulding.

TESTIMONY OF SUZANNE SPAULDING, MANAGING DIRECTOR, THE HARBOUR GROUP, LLC

Ms. SPAULDING. Chairman Coble, Ranking Member Conyers, and Subcommittee Ranking Member Scott and Members of the Committee, thank you for inviting me to participate in today's hearing.

I understand that this is just one of many hearings the Committee will be holding on the implementation of the USA PATRIOT Act. I commend you for your commitment to undertaking a thorough examination of these significant provisions.

I would like to begin my testimony by emphasizing that I have spent over 20 years working on efforts to combat terrorism, starting in 1984 as Senior Counsel to Senator Arlen Specter of Pennsylvania, who introduced and guided to enactment the first law to provide extraterritorial jurisdiction over terrorist attacks against Americans abroad.

Over the last 2 decades in my work at the Central Intelligence Agency, at Congressional intelligence oversight Committees, and as Executive Director of two independent commissions, I have seen how the terrorist threat changed, from one aptly described in the mid-1980's by Brian Jenkins'famous remark that, quote, terrorists want a lot of people watching, not a lot of people dead, to one that is now more aptly described by former DCI Jim Woolsey's observation that the terrorists of today don't want a seat at the table, they want to destroy the table and everyone sitting at it.

There is no question that today we face a determined set of adversaries bent on destroying American lives and America's way of life. The counterterrorism imperative is to deny the terrorists both of these objectives.

My testimony this morning attempts to assess how well two key provisions, in particular the Lone Wolf amendment and section 214, satisfy this counterterrorism imperative. Let me start with the Lone Wolf amendment to FISA.

The Foreign Intelligence Surveillance Act is an extremely important national security tool. The problem with the Lone Wolf provision is that it needlessly undermines the policy and constitutional justification for this essential authority. The Lone Wolf provision is often referred to as the Moussaoui fix. But, in fact, no fix was needed in the Moussaoui case, because it was not FISA's requirements that prevented the FBI from gaining access to his computer back in August of 2001. The problem was the FBI's misunderstanding of FISA's requirements.

This conclusion is supported by the findings of the Joint Congressional Intelligence Committee inquiry into the 9/11 attacks, an exhaustive Senate Judiciary Committee inquiry, and the 9/11 Commission.

As the Senate Judiciary Committee report explained, the FBI did not have a proper understanding of either the probable cause standard or the legal definition of the agent of a foreign power requirement. Specifically, the Bureau was under the incorrect impression that the statute required a link to an already identified or recognized terrorist organization.

The Senate Judiciary Committee report explains that while a group is not defined in FISA, in common parlance and using other legal principles, including criminal conspiracy, a group consists of two or more persons whether identified or not. And the probable cause standard does not mean more likely than not or an over 51 percent chance, but only the probability and not a prima facie showing.

The report concluded that the Government did have sufficient information to meet the FISA standard and gain access to Moussaoui's computer.

Some would argue that we ought to include the Lone Wolf amendment to FISA anyway, just in case. The problem with this reasoning is that it comes at a high cost. In addition to being unnecessary, the Lone Wolf provision, by extending FISA's application to an individual acting entirely on their own, undermines the policy and constitutional justification for the entire FISA statute.

When Congress enacted FISA, according to the Senate report, it carefully limited its application in order to, quote, "ensure that procedures established in FISA are reasonable and in relation to legitimate foreign counterintelligence requirements and the protective rights of individuals. Their reasonableness depends, in part, upon an assessment of the difficulties of investigating activities planned, directed and supported from abroad by foreign intelligence services and foreign-based international terrorist groups."

The Congressional debate and the court cases that informed and followed it clearly reflect the sense that this limited exception from normal criminal warrant requirements is justified only when dealing with foreign powers or their agents, and was further enforced in the FISA court of review opinion.

Congress should let the Lone Wolf provision sunset. If the Government can make a compelling case that targets have escaped necessary surveillance because the Government has been unable to meet the relatively low probable cause standard for showing that at least one other person is involved, Congress could consider creating a permissive presumption that if there is probable cause to believe that a non-U.S. Person is engaged in or preparing for international terrorist activities they can be considered an agent of a foreign power. However, if it ultimately becomes clear that the target is acting alone a criminal warrant should be sought.

And I would be happy to address sections 214 and 207 in the question and answer period.

[The prepared statement of Ms. Spaulding follows:]

PREPARED STATEMENT OF SUZANNE E. SPAULDING

Mr. Chairman, Ranking Member, and members of the committee, thank you for inviting me to participate in today's oversight hearing on the implementation of certain sections of the USA PATRIOT Act and the Lone Wolf provision, all of which are subject to sunset provisions. I understand that this is just one of many hearings that the committee will be holding on the implementation of USA PATRIOT Act and I commend the committee for its commitment to undertaking a thorough examination of these significant provisions.

I would like to begin my testimony today by emphasizing that I have spent over twenty years working on efforts to combat terrorism, starting in 1984 as Senior Counsel to Senator Arlen Specter of Pennsylvania, who introduced and guided to enactment the first law to provide extraterritorial jurisdiction over terrorist attacks against Americans abroad. Over the last two decades, in my work at the Central Intelligence Agency, at congressional intelligence committees, and as Executive Di-

rector of two different commissions on terrorism and weapons of mass destruction, I have seen how the terrorist threat changed from one aptly characterized by Brian Jenkins famous remark that "terrorists want a lot of people watching, not a lot of people dead," to one better described by former DCI Jim Woolsey's observation that "the terrorists of today don't want a seat at the table, they want to destroy the table and everyone sitting at it." There is no question that today we face a determined set of adversaries bent on destroying American lives and our way of life. The counterterrorism imperative is to deny the terrorists both of these objectives.

My testimony this morning attempts to assess how two key provisions, the Lone Wolf amendment and section 214, satisfy this counterterrorism imperative.

LONE WOLF

The Foreign Intelligence Surveillance Act (FISA) is an extremely important national security tool. The problem with the Lone Wolf provision is that it needlessly undermines the policy and constitutional justification for this essential authority.

The common wisdom—"if it ain't broke, don't fix it"—was ignored when Congress enacted the "lone wolf" amendment to the Foreign Intelligence Surveillance Act (FISA), allowing its use against an individual acting totally alone, with no connection to any foreign power, so long as they are "engaged in international terrorism or activities in preparation therefor."

I think it's important for the committee to separate the true lone wolf from the case of someone who's connection to a terrorist group is simply unclear. If there is a legitimate concern about the ability of the government to show the necessary connection to an international terrorist group—and I am not convinced there is—then there are better ways to address this concern than to extend FISA to someone that we know is acting entirely alone.

Let's start with the case of someone who's connection to an international terrorist group may be unclear. I would urge the committee to carefully consider whether the government has made a compelling case that they need the lone wolf provision to address this concern.

The lone wolf provision is often referred to as the "Moussaoui fix." In fact, no "fix" was needed in the Moussaui case because it was not FISA's requirements that prevented the FBI from gaining access to his computer back in August of 2001. The problem was the FBI's misunderstanding of FISA. This conclusion is supported by the findings of the Joint Congressional Intelligence Committee Inquiry into the 9/11 Attacks, an exhaustive Senate Judiciary Committee inquiry, and the 9/11 Commission.

In order to obtain a FISA order authorizing access to Moussaoui's computer, the FBI needed to show probable cause to believe that Moussaoui was acting "for or on behalf of a foreign power." A foreign power is defined to include a group engaged in international terrorism. As the Senate Judiciary Committee Report explained, the FBI misunderstood the FISA requirement:

> In addition to not understanding the probable cause standard, the (the Unit Chief) did not have a proper understanding of the legal definition of the "agent of a foreign power" requirement. Specifically, he was under the incorrect impression that the statute required a link to an already identified or "recognized" terrorist organization, an interpretation that the FBI and the supervisor himself admitted was incorrect.

FBI Oversight in the 107th Congress by the Senate Judiciary Committee: FISA Implementation Failures, An Interim Report by Senators Patrick Leahy, Charles Grassley, & Arlen Specter (February 2003) at p. 17.

The Judiciary Committee Report, echoing the House Report accompanying FISA in 1978, explained that while "a group" is not defined in FISA, "in common parlance, and using other legal principles, including criminal conspiracy, a group consists of two or more person whether identified or not." Moreover, remember that the FBI does not have to "prove" the target's connection to a terrorist group. They must merely meet the "probable cause" standard, which, as the Judiciary Committee Report points out, does not mean "more likely than not" or "an over 51% chance," but "only the probability and not a prima facie showing." The Report concluded that "there appears to have been sufficient evidence in the possession of the FBI which satisfied the FISA requirements for the Moussaoui application" (p. 23). Thus, no "fix" was required to search Moussaoui's computer.

Even if the FBI had not been able to meet the relatively low "probable cause" standard for showing that Moussaoui was working with at least one other person, the FBI could very likely have obtained a criminal warrant to search Moussaoui's computer. They did not pursue that because they were concerned that doing so

would preclude them from getting a FISA warrant later if they were turned down for the criminal warrant or ultimately did develop what they thought was sufficient information linking him to a terrorist group. This concern was based on the "primary purpose" test—viewed as precluding the use of FISA if the primary purpose was criminal prosecution rather than intelligence collection—which was subsequently changed in the USA PATRIOT Act.

Now that this "primary purpose" test has been eliminated, and particularly in light of a subsequent opinion by the Foreign Intelligence Surveillance Court of Review, this would no longer be a concern and the government today could seek a criminal warrant without concern of precluding future use of FISA.

Nor would the need to use sensitive information in the criminal warrant application be a compelling concern, since the criminal wiretap statute already imposes security requirements upon the judiciary in connection with crimes such as espionage, sabotage, and treason. In addition, classified information already is shared with judges in the context of the Classified Intelligence Procedures Act.

One might argue that we should include the Lone Wolf option in FISA "just in case." The problem with this reasoning is that it comes at a high cost. In addition to being unnecessary, the lone wolf provision—by extending FISA's application to an individual acting entirely on their own—undermines the policy and constitutional justification for the entire FISA statute.

When Congress enacted FISA, according to the Senate Report, it carefully limited its application in order "to ensure that the procedures established in [FISA] are reasonable in relation to legitimate foreign counterintelligence requirements and the protected rights of individuals. Their reasonableness depends, in part, upon an assessment of the difficulties of investigating activities planned, directed, and supported from abroad *by foreign intelligence services and foreign-based terrorist groups.*" Senate Report 95–701, at 14–15 (emphasis added).

The Congressional debate, and the court cases that informed and followed it, clearly reflect the sense that this limited exception from the normal criminal warrant requirements was justified only when dealing with foreign powers or their agents. Most recently, the FISA Court of Review (FISCR) cited the statute's purpose, "to protect the nation against terrorists and espionage threats directed by foreign powers," to conclude that FISA searches, while not clearly meeting "minimum Fourth Amendment warrant standards," are nevertheless reasonable.

The FISA exception to the Fourth Amendment warrant requirement was not based simply on a foreign nexus; it did not apply to every non-US person whose potentially dangerous activity transcended US borders. It was specifically limited to activities involving foreign powers.

Individuals acting entirely on their own simply do not implicate the level of "foreign and military affairs" that justify the use of this extraordinary foreign intelligence tool.

The requirement that the lone wolf must be "engaged in international terrorism or acts in preparation therefore" does not solve this problem. Nowhere in FISA's definition of "international terrorism" is there any requirement for a connection to a foreign government or terrorist group. The definition of international terrorism merely requires a violent act intended to intimidate a civilian population or government that occurs totally outside the United States, or transcends national boundaries in terms of the means by which it is accomplished, the persons it appears intended to coerce or intimidate, or the locale in which the perpetrators operate or seek asylum. This would cover an individual inside the US who uses a gun that was purchased in Mexico to threaten a teacher in a misguided attempt to get the government to change its policies on mandatory testing in schools.

Nor should we rely upon FISA judges to ensure that an overly broad standard is only applied in ways that are sensible, since the law makes clear that they must approve an application if the standards set forth in the statute are met.

Congress should let the lone wolf provision sunset. If the government can make a compelling case that targets have escaped necessary surveillance because the government has been unable to meet the relatively low "probable cause" standard for showing that at least one other person is involved, then Congress could consider creating a permissive presumption that if there is probable cause to believe that a non-US person is engaged in or preparing for international terrorist activities, they can be considered an agent of a foreign power. If it ultimately becomes clear that the target is acting alone, a criminal warrant should be sought.

If nothing else, Congress should seriously reconsider its decision to "fix" FISA by slipping the "lone wolf" into the definition of an "agent of a foreign power." By defining an individual acting totally alone, with no connection to any other individual, group, or government, as "an agent of a foreign power," Congress adopted the logic of Humpty Dumpty, who declared: "When I use a word, it means just what I choose

it to mean." Unfortunately, this legislative legerdemain stretched the logic of this important statutory tool to a point that threatens its legitimacy. If its use against a true lone wolf is ever challenged in court, FISA, too, may have a great fall.

SECTION 214

Section 214 expands the pen register and trap and trace authority under FISA. Prior to this expansion, these orders could be issued only if there was reason to believe that the telephone line or other communication device had been or was about to be used to communicate with an individual involved in international terrorism or spying that may violate US criminal laws or, in the case of an agent of a foreign power, communications that may concern international terrorism or spying that violate criminal laws. The new standard is significantly lower. Now these orders must be issued if it is merely "relevant" to ongoing investigation to protect against international terrorism or spying. This is justified as being consistent with the standard for pen registers and trap and trace authority in the criminal context, which requires that the communications be relevant to an ongoing criminal investigation.

Without addressing the appropriateness of the criminal standard, let me try to explain why I am uncomfortable with the government's argument that whatever powers it has in the ordinary criminal context, it should have for international terrorism investigations—an argument it has made to justify many post-9/11 expansions of power.

The rules that apply in the criminal context require some kind of criminal predicate. Not necessarily that a crime has already been committed, but that the activity that is targeted would violate a criminal statute. Under our constitution, criminal activity must be well defined so that individuals are clearly on notice with regard to whether their actions may violate the law and thus justify government scrutiny.

The language in section 214 and elsewhere drops all references to any criminal predicate, referring instead to "an investigation to protect against international terrorism." These investigations can be based merely on "suspicious activity"—something that has not yet been defined and which any one of us might engage in without even knowing it. The implications of this distinction are potentially profound and have not, I believe, been fully considered.

Beyond this concern, it is also troubling that the only caveat in section 214 with respect to US persons is that the investigation cannot be based "solely" upon activities protected by the First Amendment to the Constitution. Doesn't this mean that the non-First Amendment activity could be extremely minor or insignificant, since even that would take it out of the realm of relying "solely" on First Amendment activity?

Concerns about the new standard in section 214 are similar to concerns expressed about the nearly identical standard provided for Section 215 of the PATRIOT Act, which provides authority for the FBI to compel anyone to produce any tangible thing in their possession as part of a terrorism investigation. I am certain that the committee will spend a great deal of time considering the range of concerns raised by section 215. Thus, I will not go into these concerns in detail but would urge the committee to keep section 214 in mind when it considers the standard in section 215.

The concerns with section 214 are often downplayed because it does not provide authority to intercept the "content" of the communications and, thus, the assumption is that there is no reasonable expectation of privacy. However, as you know, section 216 of the PATRIOT Act, which is not subject the sunset provisions, expanded pen register and trap and trace authority to activity on the Internet, where it is far more difficult to separate content from routing and addressing information. If a pen register served on an ISP requires disclosure of the URL, for example, that will almost always reveal the subject matter. Furthermore, if the government simply looks up the URL on the Internet, they can view the entire content of the page that you visited. This makes it more analogous to section 215's authority for the FBI to find out what books you are reading, and this is another reason that the committee should reconsider section 214 when it considers section 215.

CONCLUSION

Let me close by again commending the committee for its commitment to ensuring that the government has all appropriate and necessary tools at its disposal in this vitally important effort to counter the terrorist threat. We often say that Democracy is our strength. The unique relationship between government and the governed in a democracy is a key source of that strength. These hearings, and your willingness to carefully consider whether these provisions adopted in haste in a time of great fear should be renewed or modified, will contribute significantly to restoring the nec-

essary public confidence that the government is protecting both American lives and America's way of life. Thank you.

Mr. COBLE. Thank you. I commend each of you for not having violated the red light rule. You all came in under the wire.

Folks, our Subcommittee has been blessed, generally, with the appearance of excellent witnesses. Today is no exception. I think we have a very fine panel before us. Mr. Baker, let me start with you.

Why was it necessary to extend the surveillance from 90 days to 120 days and the period of physical searches from 45 to 90 days?

Mr. BAKER. Mr. Chairman, this was an effort to be reasonable in the sense that we were after—especially after 9/11, we were crushed, my office was crushed with the number of FISA applications that were going through. And so we were looking for ways to try to enable us to use our resources more effectively and more efficiently to protect the privacy of Americans.

So what we did by proposing this was to focus, with respect to the 90-day to 120-day and 1-year provisions, to focus on cases involving non-U.S. Persons. And these non-U.S. Persons are individuals who act in the United States as officers or employees of a foreign power or act as a member of an international terrorist group. So it was our assessment that this was an area where the privacy interests at issue for Americans were lower, and, therefore, by allowing us to use resources on the cases where Americans were targeted, that was a better use of our resources. That was where the civil liberties issues were more focused and was a better use of our resources in general there.

Mr. COBLE. So, now, assuming this extension is in fact enacted, could the Government go back to court and request an extension of the orders upon expiration of the time frame; that is, the 120 or the 90 days?

Mr. BAKER. Yes. The expiration—we would obtain authorization for one of these individuals in the first instance, for 120 days, and then the expiration—at the expiration of 120 days, we would seek an extension for 1 year.

Mr. COBLE. Thank you, sir.

Ms. Spaulding, you said you might want to talk about the other sections you did not allude to. So fire away.

Ms. SPAULDING. Thank you, Mr. Chairman. With regard to section 207 and the duration of FISA orders, if the Government is indeed able to make a compelling case to the Committee that it is overly burdensome to file for extensions more frequently, my suggestion would be that at a minimum the Committee consider broadening the discretion of the FISA judge to enter an order for a shorter period of time under certain circumstances.

There are undoubtedly situations which you might consider a slam dunk, to use an unfortunate term, where it is quite clear that you are going to be getting valuable information from a FISA surveillance.

There are other circumstances in which it maybe is not quite so clear, in which a FISA judge ought to have the discretion, as they do apparently, in the extensions of an order, to enter it for up to the period of time. But, in the initial order, the language is not clear as to whether the FISA judge has this discretion to ask the

Government to come in at an earlier point in time, and that would be my suggestion on 207.

Mr. COBLE. I thank you. Ms. Buchanan, let me put a multi-faceted question to you. How are pen registers typically used in criminal investigations, A, and does 214 authorize pen registers for intelligence investigations to obtain the content of a conversation, e-mail or phone call? And, finally, what kind of information does section 214 allow the Government to obtain?

Ms. BUCHANAN. Pen registers are obtained in order to collect the information that is dialed from a telephone, the numbers that are dialed, the routing information. This is not content information. This type of information is collected by the Government to show connections between individuals, to develop probable cause, to further develop a case.

These procedures are utilized early in an investigation. Section 214 permits the Government to obtain this information in intelligence investigations as well as the criminal law. Neither under the criminal law or under section 214 can the Government collect content information. So that is not permissible under either statute.

Mr. COBLE. Well, I think we will probably have a second round because we do not have that many Members here, and this is indeed important. So I will suspend, waiting for the second round.

I recognize the gentleman from Virginia.

Mr. SCOTT. Thank you, Mr. Chairman. Let me follow through on that. On the pen register, trap and trace warrants, you say you cannot get content. That is on the telephone conversations. How do e-mail and websites fare under that standard?

Ms. BUCHANAN. It is really no different, Congressman Scott. Content information is not collected either under a pen register for a telephone or under a pen register of e-mail. Content is not collected. The statute——

Mr. SCOTT. What do you get on e-mail or websites?

Ms. BUCHANAN. The statute is designed to collect just the routing information, who is talking to whom, not the content. The statute specifically deals——

Mr. SCOTT. What do you get on an e-mail?

Ms. BUCHANAN. With an e-mail you just get the routing information, where the e-mail went, who the e-mail was addressed to, not the subject or not any of the content. The statute——

Mr. SCOTT. No subject line.

Ms. BUCHANAN. No subject line. The statute anticipates that in some circumstances there could be inadvertent collection. The statute requires the Government to use the latest technology to prevent that from happening, and in the inadvertent situation when it does happen the Government is required to minimize this information and not to use it.

Mr. SCOTT. What about websites?

Ms. BUCHANAN. The same would apply to a website. This information——

Mr. SCOTT. Do you get to know which website was looked at?

Ms. BUCHANAN. The information that is sought is where the e-mail traffic was routed to.

Mr. SCOTT. What about—website is not an e-mail. Can you find out what websites I have looked at?

Ms. BUCHANAN. I think I am going to defer to Mr. Baker.

Mr. BAKER. Well, this is the——

Mr. SCOTT. I just say that because a website, if you know what website it was you know what I was looking at. If there were dirty pictures that would be embarrassing. Can you find out whether or not I was looking at dirty pictures, or whether or not I just accessed AOL?

Mr. BAKER. There are two issues here. The one issue is what does the technology allow us to do, and then what does the law allow us to do?

In situations where the technology would not sort of by default restrict the—looking down at particular web pages at a particular website, there are internal Department of Justice procedures as recognized by the statute that are in place to try to address the situation that you are describing.

So the law indicates that we are not allowed to collect the content, technology sometimes is not able to do that, to sort of defeat the content, and there are provisions in place in terms of policies to, in effect, minimize that kind of collection for—in other words——

Mr. SCOTT. Well, you recognize the fact that if you have—the website you look at has content implications, if there are certain health care websites, other kinds of websites, you can get some content just because you know what I have been reading.

Mr. BAKER. Yes. But these are communications—well——

Mr. SCOTT. Or what books I bought off of amazon.com. When I go to a website and look at those books, the website, page by page, you can see what I have been doing, what I have been buying.

Mr. BAKER. Well, I mean, business records, books that you purchased from a company, that is not something that is protected by the fourth amendment. And so different standards apply when the Government wants to obtain that kind of information.

So the statute is written a particular way to prohibit the use of a pen register to get content. But, nevertheless, those materials and that example might not be protected by the fourth amendment.

Mr. SCOTT. These FISA warrants, there is reference to not a U.S. Citizen. Can a U.S. Citizen be the target of a FISA wiretap?

Mr. BAKER. Absolutely, yes. The law distinguishes and has different standards for when you want to—when your target is a non-U.S. Person or a foreign power and when your target is a U.S. Person.

Mr. SCOTT. Well, target of the investigation and target of the wiretap——

Mr. BAKER. I am talking about the target of the surveillance in terms of a full content FISA.

Mr. SCOTT. Okay. Well, the target of the wiretap, does that have to be the target of the investigation? Suppose you find that somebody has a lot of information about your target. Can you wiretap that phone to get information about the target?

Mr. BAKER. The target is the person or the entity about whom you want to obtain information. So——

Mr. SCOTT. Suppose a U.S. Citizen has information, and would be—you find out that they are going to be talking about your target, and you can find out where they are going to be, get good information about your target. Can you wiretap—as part of the investigation of the target, can you wiretap somebody else to get information about your target?

Mr. BAKER. No. Only if I could show that that person was an agent of a foreign power. I would have to separately show, or that the other person is using or about—that my target—what I have—two things I have to show under FISA: that the target is an agent of a foreign power, and I have to establish that by probable cause, and the second thing, that the target is going to use the facilities or places of which the surveillance is going to be directed. So a telephone used by an innocent person that is not being used by the target is off limits unless I can make the statutory showing.

Mr. SCOTT. So you can only listen into conversations that involve the target?

Mr. BAKER. It depends what facility I am targeting. If I am surveilling the target's home phone, let's say, and the target—and that is my target, and I can be up on that telephone, if other individuals use that phone, then I can continue my collection, and I deal with that through court authorized and approved minimization procedures.

This is exactly what happens in the title III arena as well. You come up on the telephone——

Mr. SCOTT. Well, that is the home phone. If you got this roving kind of thing and the bug is actually placed at his place where he volunteers a lot, like the National Democratic Headquarters, how do you listen in on other people's conversations there?

Mr. BAKER. Well, again, I am going to have to—I know that the roving positions are going to be the subject of a hearing on Thursday. But succinctly, all of the FISA provisions have within them these minimization procedures that I mentioned earlier, that minimize, that require the Government to minimize the acquisition, retention, and dissemination of the information that is collected.

And those are—and the court orders us to follow those procedures. The court reviews those procedures and orders us to follow them.

Mr. COBLE. I thank the gentleman. The gentlemen from Ohio is recognized for 5 minutes.

Mr. CHABOT. Thank you, Mr. Chairman. Mr. Baker, prior to the enactment of the Lone Wolf amendment, how difficult was it for intelligence agencies to obtain wiretap orders for foreign terrorists who do not belong to any identified terrorist organizations?

Mr. BAKER. Well, it was not authorized by the statute for us to be able to do that. So the answer is we could not do that. We had to find a connection between the target and a foreign power, an international terrorist group or a foreign government, so on.

But it is worth mentioning that from the beginning, from 1978, an international terrorist group could consist of as few as two people. So the difference here really is going, at the minimum, or at the base level, I guess, from a group of two people to a group, if you will, of one person.

Mr. CHABOT. And what must the FISA court find before issuing a surveillance order under the Lone Wolf provision?

Mr. BAKER. That the Lone Wolf, that the target is an agent of a foreign power, meaning in this context that they are a non-U.S. Person, that is critical to remember, non-U.S. Person, who engages in international terrorism or activities in preparation therefor. So this is the Lone Wolf who—an individual who could, I mean, in sort of the doomsday scenario, the things that we are most worried about, an individual who might have access to some kind of a weapon of mass destruction, chemical, biological, nuclear, or radiological weapon, attempt to use a device such as that in the United States, but have no known or apparent connection to another individual or a group or a foreign government.

Mr. CHABOT. And do you believe that real or apparent Lone Wolf terrorists could threaten the safety and security of the American people?

Mr. BAKER. Absolutely. As I have just described, that is what we are very worried about. And it seems to me that, I mean, as the FISA court of review said back in 2002, FISA is constitutional because the searches it authorizes are reasonable.

And it seems to me that targeting an individual such as the one I just described, bringing in a weapon of mass destruction into the United States, under the fourth amendment that is reasonable, and I think therefore that this provision of FISA is certainly constitutional.

Mr. CHABOT. Now, critics of the Lone Wolf provision argue it is a dangerous expansion of authority allowing the application of FISA to individuals lacking any connection to foreign powers.

Do you agree with Mr. Woods who counters this claim on patriotdebates.com when he says, quote, the language actually enacted, however, integrates a definition of international terrorism that preserves a sufficiently strong foreign nexus requirement, unquote?

And if so, could you explain that nexus and why it is important.

Mr. BAKER. Yes, I agree with that comment. Again, to be an agent of a foreign power under this provision, you have to first be a non-U.S. Person and you have to be engaged in international terrorism activities. International terrorism is a defined term under the statute. It includes or covers or applies only to, said differently, violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or would be if committed here, that have a coercive or intimidation factor associated with them, and occur outside the United States or transcend national boundaries, and the perpetrators, the locale that they are going to be taking place in, or the places where the target is going to seek asylum.

And so there is a nexus to international terrorism. You cannot use the Lone Wolf provision to conduct electronic surveillance of a U.S. Person who is engaged in domestic terrorism in the United States. It doesn't apply to that kind of situation.

Mr. CHABOT. Okay. And who determines whether an individual will be classified as a Lone Wolf and what are the criteria used in making such a determination?

Mr. BAKER. Well, at the end of the day it is the FISA court. We have to go before the FISA court before we can get one of those approvals. Prior to that, the Attorney General must sign every application that would use the Lone Wolf provision. Before that, you would have to have a certification from someone, such as the Director of the FBI or another high ranking Government official with national security responsibilities. And my office reviews that, the FBI reviews that and so on.

And, again, the legal foundation is that there is probable cause to believe that the target is an agent of a foreign power under the standard I just articulated, and that they are using or are about to use the facilities at which the surveillance will be directed.

Mr. CHABOT. Finally, has provision alone resulted in a dramatic increase in the use of FISA warrants in situations that do not justify such extraordinary Government power?

Mr. BAKER. Well, I would—I mean I would say, first of all, the number of times that we have used this I believe is still classified, so I can't discuss that today.

But I would say that, I mean certainly, whenever—if we can meet this standard, I think that surveillance of such a person would be justified and would be warranted.

Mr. CHABOT. Thank you. I know that the light is ready to come on. So I yield back the balance of my time.

Mr. COBLE. The gentleman from Michigan, Mr. Conyers.

Mr. CONYERS. Thank you, Mr. Chairman. I remember Attorney Buchanan pointing out how helpful some of the provisions here in the PATRIOT Act were. But the convictions were only criminal convictions. They had nothing to do with terrorism.

Ms. BUCHANAN. That is correct, Mr. Conyers. I was demonstrating how the pen register is used in a criminal case, because, of course, those cases are not classified and the pen register is used in the same manner under FISA.

So I was demonstrating how it can collect noncontent information to show connections between individuals and how that information can be used to later build upon the investigation and ultimately result in convictions.

Mr. CONYERS. Have there ever been any terrorist convictions in the United States?

Ms. BUCHANAN. Well, we just had one last week.

Mr. CONYERS. Well, you had a plea of guilty.

Ms. BUCHANAN. Well, that is a conviction.

Mr. CONYERS. Congratulations. Any others?

Mr. BAKER. Well, I think——

Mr. CONYERS. Can you think of any others, Counsel?

Ms. SPAULDING. No.

Mr. CONYERS. Can you? I am just inquiring.

Mr. BAKER. Mr. Congressman, you are looking for trials, actually where someone was convicted following a trial is what I am gathering from your question.

Mr. CONYERS. Well, there has only been one plea of guilty, and no trials, according to what I know.

Mr. BAKER. Well, I can't remember off the top of my head every conviction. But we have the cases up in Buffalo, the Lackawanna cases, we have the cases in Portland, we have the cases in Virginia

as well, I think the Virginia cases, the so-called Virginia Jihad Group. Those I believe were convictions following a trial before a jury. So I think the answer is yes.

Mr. CONYERS. All right. Let me ask Attorney Spaulding. I am trying to shape this notion, the feeling that I have is that the way these things are written and interpreted that the intelligence community can do just about anything they want anyway.

Can you make me feel better about that and get that out of my system, and really believe that—I mean, I would like to imagine a situation where they are only looking for the phone numbers that you are calling and who you are calling, but they don't want to hear the substance, and they are sitting up there, and I am trying to really keep a straight face and believe that they are not going to listen to substance—I mean, what—this whole area is so general and vague. I remember the former Attorney General refusing court orders flat out. They asked him, I think, to produce something. He said no, he is just not doing it. They can do whatever they want.

Ms. SPAULDING. My sense, from working in the intelligence community and on the staff of the oversight Committees, is that the intelligence community takes its legal obligations very seriously, that in fact they endeavor to stay on the right side of U.S. Law.

Needless to say, espionage is a violation of laws of virtually every country in the world. So they are violating law when they operate overseas. But they take very seriously their obligation to follow U.S. Law.

But it is also the case that law enforcement and intelligence communities will use all of the authority that the law gives them, and they will use it to its fullest to accomplish their mission, which is why it is so important to make sure that the law is clear and appropriate, not overly broad and not vague.

The concern with respect to the potential for section 214 to provide access to content that was illustrated by Mr. Scott's questions, particularly most acute in the Internet context, is a legitimate concern. And it is why I think that it ought to be, that section 214 ought to be reconsidered by this Committee when it looks at section 215. The standards are very similar, and I would hope that 215 will be discussed in that same context.

Attorney Buchanan talked about the standard is parallel to that in the criminal context, "relevant to a criminal investigation for criminal context, and relevant to an international terrorism" or investigation to protect against terrorism in the FISA context, and I would simply urge the Committee to carefully consider the import of that distinction.

Mr. CONYERS. Last question. If Chairman Coble in his usual fairness were to allow us to drop one of these three, Lone Wolf, 214, 207, and we had a quick conference, wouldn't you agree that the Lone Wolf provision is the most troublesome?

Ms. SPAULDING. I would, yes.

Mr. CONYERS. Thank you.

Mr. COBLE. The gentleman from Massachusetts, Mr. Delahunt.

Mr. DELAHUNT. Thank you, Mr. Chairman. Ms. Spaulding, could you comment on the testimony by Mr. Baker, Mr. Baker and his analysis of the necessity of the Lone Wolf provision?

Ms. SPAULDING. Yes.

Mr. DELAHUNT. I sense a nuanced disagreement. And then I will ask you, Mr. Baker, to comment on her response.

Ms. SPAULDING. I think it's important. I believe that FISA—the justification for FISA is not based on the dangerousness of the threat. Clearly a domestic terrorist can wreak just as much havoc as an individual who has transcended international borders in the means by which they carry out their act. So I don't think FISA is just based on that ground. In fact, what the courts and the Congress have said is that FISA is based on a compelling Government need that exists in the context of an international group; that exists in the context where you've got more than one player so that you're likely to get something out of listening to this conversation, and because there is more than one player and it involves an international group, the challenges for the collection of that intelligence and the need for continued secrecy because there are other players involved are what provide the justification of FISA, and this is totally lacking in the context of an individual acting solely on their own. And I think that is a very important distinction because you get caught up in the nature of the threat.

Mr. BAKER. Again, Congressman, I think that the basic answer is that the searches and surveillances that FISA authorizes are constitutional because they are reasonable. And it's our assessment that focusing on somebody like a lone wolf, somebody——

Mr. DELAHUNT. Let me interrupt you for a moment. You use the hypothetical of an individual coming in with weapons of mass destruction. I'm talking about, you know,—I understand the concerns. But by implication, doesn't that qualify as—by inference, isn't there a reasonable inference that there is a group, that there is a conspiracy of some sort just simply because of the acquisition, if you will, the transmission? I'm sure that a weapon of mass destruction just doesn't appear out of thin air on someone's door.

Again, I think, you know, that was the point that I think I heard earlier from Ms. Spaulding. You know, I think there are other means, other than the provision itself to achieve the result you're looking for.

Mr. BAKER. In a situation such as we're describing here, time will be—if we are faced with that, time will be of the essence.

Mr. DELAHUNT. You know, this whole time issue continues rising like there is an immediacy to it. If there is in the possession of the Government and investigatory agencies, I can't imagine a scenario where there is not implicated a co-conspirator. I simply can't.

Mr. BAKER. You might not be able to imagine that, but we have to have some evidence to establish that before the FISA court.

Mr. DELAHUNT. I understand that. But I would think a FISA judge sitting on, you know, being presented an affidavit—included in the affidavit would be some reference to another individual. I mean, there has to be a minimal level of evidence there.

Mr. BAKER. Whether or not I could come up with as a creative lawyer and explain to the FISA court reasonable instances and so on in a particular factual situation is one thing. But the question is, doesn't it make more sense to have a clear standard already in the law that doesn't force us when we are under the gun in terms of time pressure to try to concoct something that may not fly.

Mr. DELAHUNT. This is always going to be the balancing act that, you know, is implicated in our Constitution.

Ms. Spaulding.

Ms. SPAULDING. And there is always the option of going for a title III criminal warrant if ultimately you are unable to show a connection with any other person. The hardest thing about frustrating a lone wolf terrorist attack is not accessing their communications but finding the lone wolf.

Mr. BAKER. FISA is a good tool to use in these situations because the information we have about this target, this lone wolf may be from a sensitive source. And we don't want to necessarily put that source at issue in a criminal proceeding. We want to use the protections that FISA has which are constitutional.

Mr. DELAHUNT. Under a title III proceeding, you could still, I presume, request the necessary protections to protect that source. I mean that is not unheard of.

Mr. BAKER. There are mechanisms, but they're not as good. And Congress, in 1978, assessed that there was a better way to try to protect the national security sources as well as the methods we are going to use against this type of individual. If we have somebody——

Mr. DELAHUNT. There's always—the burden always has to be placed on the Government if we are going to protect the liberty and our freedoms. And I guess the question is, is the measure, is the quantum of the burden sufficient to make it so difficult that we can't achieve the goal of protecting our national security.

Mr. BAKER. We live with that issue in terms of balancing security versus liberty every single day in my office. And the folks who work for me diligently try to achieve both of those goals at the same time, and it is a difficult job. But what I would urge you is to give us the tools where there is clarity, where there is sufficient protection on both sides of that.

And again, as I went through, the difference between a group of—international terrorist group of two people versus one person is not that great, and I don't think it is of constitutional significance. And so I think you should feel comfortable in allowing this provision to continue.

Mr. COBLE. We will start a second round now. Mr. Baker and Ms. Spaulding have been examined more thoroughly, Ms. Buchanan. I don't want to ignore you, so I'm going to start with you. How does providing immunity to those who assist law enforcement with a FISA order help intelligence investigations and the war on terrorism?

Ms. BUCHANAN. Under the criminal law, we have had a provision in the law which provides immunity to those who assist law enforcement with obtaining pen registers and trap and trace orders. What I mean by assist, those individuals who are working with the communications company who installed the equipment and those individuals are immune from civil suit as a result of their participation. We ought to have that same immunity in the FISA statute to protect individuals who assist in the installation and application for pen register or trap and trace. That is what the PATRIOT Act gives us.

Mr. COBLE. Some are now arguing that a higher standard should be used for pen registers. Are you familiar with any of these proposals and do you agree with them, A? And if you would, Ms. Buchanan, explain what the relevant standard requires and why it is applied to a pen register or trap and trace order rather than probable cause standard.

Ms. BUCHANAN. The standard is and should be relevance with respect to this type of information. This information that is collected is not a search under the fourth amendment. Individuals have no expectation of privacy in this information. And that is why the standard is set at a lower standard, which is relevance. I think there has been a little confusion in the questioning this morning about what is collected with the pen register versus a wiretap.

With the pen register, the device is simply collecting the telephone numbers, the routing information, it is not collecting the substance of any of the communications. In fact, the equipment doesn't have that capability. So that is not what is the subject of collection. And that is why the standard is set at relevance. With the relevance standard, the Government simply alleges that the information would be related or connected to an ongoing investigation, that it is likely to produce other information. That is the standard. And it is much lower than probable cause.

When you look at a probable cause standard under the criminal law, you are dealing with information that has a higher expectation of privacy and that is why the law requires a probable cause standard to collect information where there is a greater expectation of privacy. And because they are very different, that is why there are different standards recognized under our law today.

Mr. COBLE. Reverting to content, Mr. Baker, if the court determines that content was collected and used by the Government under 214, what would the court likely do?

Mr. BAKER. In that case, you would have a situation where we would have disobeyed a court order, and I would gather they would want to know was this an intentional violation? Was it inadvertent? How did it happen, what procedures were in place to make sure it doesn't happen again, who's responsible, what part of the Government is going to conduct an investigation. We have, in the Department of Justice, an inspector general. We have an Office of Professional Responsibility, both at main Justice and at the FBI. You've got an inspections division at the FBI and multiple entities within the Government that the court could look to to find out the facts and take steps to address it.

I mean, there is this one case from several years ago where the court had concerns about representations by an agent in some pleadings and the court barred that person from appearing before the court again. The court is quite vigilant about ensuring that what's happening is consistent with the law.

Mr. COBLE. Ms. Spaulding, do you want to visit the sections you have not had a chance to emphasize?

Ms. SPAULDING. Thank you, Mr. Chairman. I would like to talk about section 214 and this relevancy standard. The question is relevant to what. In the criminal context, it is relevant to a criminal investigation. In section 214, it's relevant to an investigation to protect against international terrorism. It drops all references to

any criminal predicate. Under our Constitution, crimes must be very clearly defined so that Americans are clearly on notice whether their activities might violate the law and thereby invite Government scrutiny.

Investigations to protect against terrorism can be based merely on suspicious activity, which is undefined, and any one of us might be engaging in it without even knowing it. The implications of this, I think, are very profound and have not been thoroughly examined.

Mr. COBLE. Ms. Buchanan, I will end with you.

Ms. BUCHANAN. The American people have every right to be protected against international terrorism as they do against criminal violations. The standard is the same and should be the same because the dangers are equal if not greater in the terrorism arena.

Mr. COBLE. Mr. Baker, very quickly.

Mr. BAKER. The definition of international terrorism includes a nexus to criminal law. So that is in there when you are dealing with an international terrorism investigation.

Mr. COBLE. I thank you. The gentleman from Virginia.

Mr. SCOTT. Thank you, Mr. Chairman. One of the problems we have had with some of these provisions is that people when they talk about them say loudly and clearly terrorism and then mumble something about foreign intelligence. Foreign intelligence doesn't have anything to do with crimes. It is just spying on people. You could be talking about anything involving conduct of foreign affairs, which may not have any criminal connection. Now am I right on the lone wolf provision, you have to have a terrorism connection not just vague foreign policy?

Mr. BAKER. You have to have a terrorism connection. You could not be an agent of a foreign power unless you were engaging in international terrorism or activities in preparation therefor.

Mr. SCOTT. For the purpose of a lone wolf?

Mr. BAKER. Correct.

Mr. SCOTT. For the other purposes, you could be the agent of a foreign government having nothing to do with terrorism or crimes, you could just be negotiating trade deals and stuff like that?

Mr. BAKER. Without commenting on the specifics what we would be acquiring, you could be an agent of a foreign power if you are a non-U.S. person who acts as such in the United States and you're an officer or employee of a foreign government.

Mr. SCOTT. And have foreign affairs type information nothing to do with criminal activity?

Mr. BAKER. That's correct.

Mr. SCOTT. That's what I said. People will loudly and clearly say terrorism and then mumble something about foreign intelligence, suggesting that we are talking about terrorism. We are talking about many of these circumstances, things that have nothing to do with crimes, terrorism or anything else, just foreign intelligence.

Mr. BAKER. That's correct.

Mr. SCOTT. But for the lone wolf, it has to be terrorism connected. What about the pen and trap and trace?

Mr. BAKER. You have to have a showing—make a showing in the application that the information that's likely to be obtained is either foreign intelligence information not concerning a U.S. person

or is relevant to an investigation to protect against international terrorism or clandestine intelligence activities.

Mr. SCOTT. You can get this pen and trap and trace with things that are not criminally related or crime or terrorism-related? It can be foreign intelligence related?

Mr. BAKER. Foreign intelligence is a defined term in the statute.

Mr. SCOTT. Which includes terrorism and weapons of mass destruction and conduct of foreign affairs, which could be about anything. So I'm talking about it can involve just about anything part of it. We know the terrorism is in there. What else is in there?

Mr. BAKER. As you suggested, definitely includes foreign affairs. That's one of the prongs of foreign intelligence.

Mr. SCOTT. We're talking about getting this trap and trace on foreign intelligence?

Mr. BAKER. Not concerning a U.S. person.

Mr. SCOTT. And not concerning any crimes and not concerning any terrorism?

Mr. BAKER. Potentially. That's correct. Because Congress wanted to regulate all of the Government's——

Mr. SCOTT. The reason I say this is we scare people to death, and think we are talking only weapons of mass destruction when, in fact, we are talking about information that could have nothing to do with any criminal law at all.

Mr. BAKER. In a situation not involving a U.S. person.

Mr. SCOTT. In the United States?

Mr. BAKER. That's correct.

Mr. SCOTT. The predicate for this FISA wiretap and this FISA trap and trace could be the desire to get information about negotiating with another country on conduct of foreign affairs that have nothing to do with the terrorism or crimes or anything else that would endanger people in the United States?

Mr. BAKER. Well, it's always focused on the foreign relations of the United States vis-à-vis——

Mr. SCOTT. Which could include things that are not terrorism or crime related? You can start these wire taps off with "foreign intelligence," which is conduct of foreign affairs, but with the lone wolf, you have to be in terrorism. For the other, trap and trace, it could be any other thing. What about wire tapping outside of the United States proper? Can CIA agents and all that wiretap outside of the United States? Are we even talking about that?

Mr. BAKER. FISA governs surveillance and physical searches inside the United States.

Mr. SCOTT. Is it quicker to get a FISA wiretap than a criminal wiretap?

Mr. BAKER. I don't know the statistics on the criminal wiretaps. But there are provisions in FISA that allow us for start to collection in an emergency situation based upon the authorization of the Attorney General. In an emergency circumstances, there are mechanisms to address that. There is a mechanism similar to that in the title III area.

Mr. SCOTT. And if you are in Colorado, it's quicker to come to Washington, D.C. To go before a FISA court than it is a magistrate in Colorado?

Mr. BAKER. I don't know about that. Faced with a situation like that, we obviously have secure telephones. The FBI field office in Colorado would call headquarters and they would call us at the main justice.

Mr. SCOTT. Rather than just running over to the magistrate and get a quick warrant? If you have probable cause that a crime is being committed and can get information from a wiretap, why wouldn't you get a criminal warrant?

Mr. BAKER. It depends on what you are investigating and what you're focused on and what tools you want to use that are at issue and what sources of information you have and what protections you think that the various statutes are going to give you with respect to these various areas. And so the FBI agents look at the investigation they've got and make an assessment about the various tools they have available to them and try to decide what to use.

Mr. SCOTT. We've heard about people for whom you have evidence that they are gathering up explosives about to blow something up. What's the barrier to getting a title III wiretap?

Mr. BAKER. Again, these are very fact specific situations. But FISA was built by Congress to address these kinds of threats to the national security. And it includes definitions, time periods, protections against disclosure of information, and other provisions, including minimization procedures that fit better in these situations than title III does necessarily. That's why it would be used in a particular situation versus a title III.

Mr. COBLE. Gentleman's time has expired. The gentleman from Massachusetts.

Mr. DELAHUNT. Just an observation to the Chair, Mr. Coble. We have been having some excellent hearings. And all of the panels, I think, have been very helpful. I guess my question to you my friend. We are going at a fairly accelerated pace. And much of the information that we're getting, I would suggest, needs some reflection. I understand we're having another hearing this week—two more. Does the Chair have a time table for when we might consider a resolution or a bill? Could you give us some guidance?

Mr. COBLE. If the gentleman would yield. I say to the gentleman, this accelerated schedule is not determined by me.

Mr. DELAHUNT. I suspected that. If the Chair knows, do we have—is there a calendar for when the Subcommittee itself might consider a proposal?

Mr. COBLE. If the gentleman would yield further to me. Not known to me.

Mr. DELAHUNT. Not known to you.

Mr. COBLE. No fixed calendar.

Mr. DELAHUNT. Because we are really rolling along here and I would make a request to the Chair and I know you're a diligent worker, but many of us do not, you know, have your experience. And maybe if we could slow the pace down in terms of the calendar itself, it might provide us an opportunity to consult with many of the witnesses that have already appeared before us just to provide us with an opportunity to become even more informed. The Chair might consider passing that request on up wherever it may go, but I would hope that that the Chair would consider that.

Mr. COBLE. If the gentleman would yield again. I would convey that and thank the gentleman from Massachusetts.

Mr. DELAHUNT. I don't think I have—I do have another question. I'm reading one of these Hill papers here about the nominee for the United Nations, and there appears to be a question regarding his inquiry about the names of American citizens on 10 different intercepts. And I'm not going to ask you specifically about that, but I guess this goes along with the question that was posed by Mr. Scott.

In terms of protection of non-U.S. persons who are referenced in the course of a surveillance, who has access to that information? Would somebody from the Department of State have access to that information under a FISA order or would that simply—only designated officials have access to that information?

Mr. Baker?

Mr. BAKER. Again, you have to keep in mind that every court order is different—they are all different, but they all include minimization procedures. So there are restrictions on the acquisition, retention, and dissemination of U.S. person communications. And that's the focus, to protect the privacy of Americans. With respect to who has access, if you have an FBI surveillance, the FBI in the field office conducts a review of the material and decides what information is foreign intelligence information, what information is not. And then it can write summaries or do other transcripts.

Mr. DELAHUNT. I understand that. But let me—if an official, let's say hypothetically, Mr. Bowl was the deputy Under Secretary for whatever in the Department of State or the Department of Defense, whatever, and he communicated—presumably the Attorney General of the United States has access to this information under a FISA court order, because presumably it's written in a way that would allow that, the Attorney General of the United States and/or his designee, would a high ranking official in another department have access to that information, i.e., the name of the American citizen?

Mr. BAKER. Not directly. If they had some reason to believe there was some information out there and had a basis to ask for it, they would submit a request to the agency they think has the information and the agency would have to make an assessment whether disclosure of that information to that person would be consistent with the minimization procedures. And there are statutory restrictions on the use of FISA information as well.

Mr. DELAHUNT. I understand statutory restrictions. This is simply accessing information, however. Would there be, for example, the need to return before the FISA court to seek a—if such a request was made, would the—there has been any history of this, would one of—if there was doubt as to whether the request fell within the ambit of the minimization that was issued pursuant to the court order, would it be reasonable to infer that there would be an additional appearance before the FISA court to clarify?

Mr. BAKER. It could be. The FISA court carefully monitors the minimization of U.S. Person communications.

Mr. DELAHUNT. In the report back to FISA, would that information be disclosed, the individuals who did have—who had access to that information?

Mr. BAKER. Not on a regular basis. Not necessarily, no. But there are other mechanisms for that. And what would happen, the agency that requested, if they didn't think it fell squarely within the minimization procedures, would seek advice from our office, and we would make a decision as to whether we felt comfortable or not doing it.

Mr. DELAHUNT. Have you ever had those kind of requests?

Mr. BAKER. I can't think of one off the top of my head. It's an expectation that sometimes people will read a report that might reference a U.S. person and might want to know the name of that person and there are established procedures to deal with that situation and approval levels and so on that you go through.

Mr. COBLE. I thank the gentleman. Thank you all for being here and thank you for those in the audience. We live in a chaotic time, as you all know, folks. I don't think we ever want to see a repeat of 9/11 when those bastards came over here, pardon my vernacular—referring to the murderers, of course. On the other hand, I don't think any one of us wants to compromise our liberties. It's a delicate line we're negotiating. And Mr. Baker, since you are in my direct line of fire, let me go to you. Again, thinking aloud, the President has the authority grounded in the Constitution to protect our Nation's security. Based on that responsibility, what did the Government do prior to 1978, prior to FISA, A? And why was FISA enacted?

Mr. BAKER. Prior to the enactment of FISA, as I understand it, sort of the beginning of electronic communications, collection of those kinds of communications for national security purposes was done pursuant to the President's inherent authority under the Constitution to collect foreign intelligence without a warrant. It was done from the beginning up until 1978 for those purposes without a warrant.

And it was, as a result of, frankly, abuses of that authority by the executive branch that came to light in the 1970's that resulted in, among other things, the enactment of FISA in 1978. It takes us from a regime where there was no congressional legislation to a regime that Congress, as I said earlier, puts into place, clear standards for who can be a legitimate target of this kind of collection, requirements to protect the privacy of Americans and the minimization procedures and accountability for the individuals who decide to engage in one of these surveillances and to make sure it is done for a legitimate national security purpose.

Mr. COBLE. We are going to visit this PATRIOT Act time and again, and as Mr. Delahunt said probably in an accelerated mode. Thank you, Mr. Scott, Mr. Delahunt, Mr. Conyers and Mr. Chabot, for attending as well. The Subcommittee very much appreciates your contribution. 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 this same 7-day period. This concludes the oversight hearing on the Implementation of the USA PATRIOT Act: Foreign Intelligence Surveillance Act (FISA), part one. Thank you for your cooperation and the Subcommittee stands adjourned.

[Whereupon, at 11:30 a.m., the Subcommittee was adjourned.]

IMPLEMENTATION OF THE USA PATRIOT ACT: SECTIONS OF THE ACT THAT ADDRESS THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA)

Part II

THURSDAY, APRIL 28, 2005

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

The Subcommittee met pursuant to call, at 9:30 a.m., in Room 2141, Rayburn House Office Building, the Honorable Howard Coble (Chair of the Subcommittee) presiding.

Mr. COBLE. Good morning, ladies and gentlemen. Good to have all of you with us today.

The Subcommittee on Crime, Terrorism, and Homeland Security will conduct two hearings on the USA PATRIOT Act. At this morning's hearings, the Subcommittee will examine section 206, the roving wiretap provision, and section 215, the business records provision. Both section 206 and 215 amend the Foreign Intelligence Surveillance Act of 1978, known as FISA, and both expire on December 31, 2005. These two sections are among the most controversial. I believe much of the controversy is due to misinformation about the provisions, and I hope this hearing will clarify exactly what the law does.

While I expect an in-depth and lively discussion on these issues, I would like to point out a few things we've recently learned through our hearings and oversight.

We know, though I am not sure the public is aware of this, that section 215, the so-called library provision, does not even mention the word "library." It covers business records.

And yes, section 215 could be used to obtain business records from a library, but we also know from the Attorney General's oral testimony to this committee on April 6, that section 215 has never been used to obtain business records from a library. Nor has section 215 been used to obtain bookstore records, medical records, or gun sale records. In fact, no evidence has been presented to this Subcommittee or to the Department of Justice's Inspector General of any abuse of 215 for any use.

We also know from the Department of Justice response to questions from this Subcommittee and full committee that terrorists are

indeed using our libraries so that at some point section 215 may be needed there.

Section 206 amends the wiretap provision under the Foreign Intelligence Surveillance Act to allow the wiretap order to follow the person instead of covering a communication facility. Thus, when a terrorist uses a cell phone, then throws it away, uses another phone, throws it away, law enforcement does not have to get a new order each time.

We also know that this section has been used 49 times, and, according to the Attorney General, has been effective in monitoring international terrorists and spies.

Now, folks when I said there's a lot of misinformation surrounding these provisions, a lot people—well, strike that. Maybe I shouldn't say a lot people—some people. In fact, some have even talked to me.

They portray it in this manner: A couple FBI agents riding around town. Well, let's go get a couple burgers and a milkshake, and then maybe stop by the FISA Court. Pick up a couple roving wiretaps and maybe a couple 215 orders and—now, folks, I don't mean this to be cute, because folks back home have said this to me, and then maybe go to the library. See what we can come up with. Maybe share with our friends and neighbors some of the information we've found. Folks, that's far a field from what happens. It's difficult to obtain this, and I want the public to know that.

Having said that, I will now—I now look forward to hearing from my good friend, the Ranking Member, the gentleman from—the distinguished gentleman from Virginia, Mr. Bobby Scott.

Mr. SCOTT. Thank you, Mr. Chairman. Don't give them any ideas.

Thank you for holding this hearing on section 216 and 215 of the USA PATRIOT Act. These are some of the most controversial sections of the bill that will come up for renewal.

They're controversial because of the extraordinary powers of virtually—virtually unchecked powers that allow Government to use the—to allow the Government to use to invade the privacy of individuals. Section 215 is particularly disturbing, given its breadth of authority, especially because it allows law enforcement officers to obtain private records with no more than a representation that it is relevant to foreign intelligence.

And even though section 505 of the PATRIOT Act is not under sunset, you really can't talk about 215 without discussing the same problems with 505. 505 allows a host of private records and information to be obtained through the issuance by line level officers of National Security Letters on mere representation that they are relevant to an investigation of foreign intelligence.

There need to be no crime, no probable cause of a crime, no reason to believe that there's a crime, no credible or particular facts, just representation in the case of a 215 and the FISA Court has no choice but to issue the order for the production of records.

In the case of the National Security Letters, there's no court issuance or oversight, just a line officer's issuance of the letter in terms of the requirements of law.

Now, all of this is done in secret, and no explicit right to challenge the orders with a permanent gag order on the keepers' of the

records, even to the extent apparently of consulting with an attorney. With our liberalized information sharing rules, this information can be distributed all over town to various agencies and this means your neighbors who may be law enforcement agents or Defense Department officials, may know a lot more about you private medical, organizational affiliation, reading or video viewing habits than you ever imagined.

Now, with respect to section 206, the FISA roving wiretaps, I've often noted the difficulties that I see. Again, under the law no crime need even be alleged, and under the John Doe wiretap no person or particular device need to be shown, and in either case, no effort has been made to ascertain whether or not the target is actually using the device before communications are actually intercepted.

And again, all of this is in secret; secret court with limited oversight and reporting requirements when compared to the criminal wiretap process. And the Department of Justice witnesses often use the powers extended on the criminal side to justify the same powers on the FISA side.

However, they don't call for the same oversight and reporting requirements as a criminal warrant, and I think we need to pay a lot more attention to as we consider renewing these powers.

So, Mr. Chairman, I look forward to the testimony of our witnesses for enlightenment on why we should consider renewing these extraordinary powers and, if so, under what circumstances and conditions, and I look forward to working with you as we try to implement those recommendations.

Mr. COBLE. I thank the gentleman. We've been joined by the Ranking Member of the Full Committee, the distinguished gentleman from Michigan, Mr. Conyers.

Mr. CONYERS. Good morning, Chairman Coble.

Mr. COBLE. Good morning, sir.

Mr. CONYERS. And Members of the Committee welcome the panel. And this is one of the important Subcommittee hearings in which this review of the PATRIOT Act is so important, and I'm glad we have the witnesses here.

I just want to say one word about the executive director of the American Civil Liberties Union Chief Legislative Council because that organization has done so much important work, not alone. There are plenty of other organizations with them, but I single them out this morning.

But there are three considerations here. One is whether we need John Doe taps and roving taps. To me, that's a critical consideration. And what are the safeguards we need to put around it. The thing of while National Security Letters have been left off the oversight list of the committee. I hope that some of our witnesses today will tell us about their use. It appears from a redacted Freedom of Information Request that this provision has been used lots of times, hundreds of times.

The less famous part of section 215, National Security Letters, are dangerous because in addition to adding a complete gag order on the recipient, they're issued without any oversight, even from the FISA Court.

And because DOJ admits getting information from libraries, I suspect that these letters may be the source and we must have more information about them.

And finally, section 215, allowing the Government to secretly get anything from any business only upon showing a—the showing of relevance to a terror or intelligence information—only on showing of relevance to terror information or intelligence information. And as super secret as usual, DOJ refuses to explain how this section has been used. We're the lawmakers. It seems like the courtesy should be given to us, and if for any reason, it can't be done public, we're all cleared for the most secret information that's in our Government. It does confirm it has been used 35 times. The information comes on the eve of the sunset. After 3 years of pressing national security that required a secret classification.

So these are the areas that I'm concerned with and I reiterate my concern that the committee has left, in my judgment many important terror-related policies off its oversight schedule—the practice of rendition to the abuse of the material witness statute, to unsuccessful racial profiling. This committee is, in my view—and I want to work on trying to get this corrected before this series of hearings ends—is ignoring the most pressing matters within its jurisdiction. We can't limit our oversight to a few sections of the code that are due to expire. There's plenty of things to examine that don't have any expiration date, and so the Department has shifted the weight of its terror pursuit to other authorities, and or even in the absence of lawful authority at all. So, if we're truly to do our constitutional duty of overseeing the Executive's use of criminal and intelligence laws, I beg this committee to look at all of these issues, and I thank you for this opportunity, Chairman Coble.

Mr. COBLE. I thank the gentleman. We've been joined by the distinguished gentleman from Arizona, Mr. Flake, and the distinguished gentleman from Massachusetts, Mr. Delahunt.

It's the practice, I say to the panel of the Subcommittee to swear in all witnesses appearing before it. So, if you all would please stand and raise your right hands.

[Witnesses sworn.]

Mr. COBLE. Let the record show that each of the witnesses has answered in the affirmative, and you all may be seated.

Our first witness today is Mr. Kenneth Wainstein—is that correct, Mr.?—United States Attorney for the District of Columbia. Prior to joining the U.S. Attorney's Office, Mr. Wainstein served as general counsel of the FBI and as director of the Justice Department's Executive Office for the U.S. Attorney. He is a graduate of the University of Virginia, and the Boalt Hall School of Law at the University of California at Berkeley.

Our second witness is Mr. James A. Baker, who's been with us before. Mr. Baker, good to have you back. I thank Mr. Baker for graciously agreeing to return as a witness for a second time during this series of oversight hearings on the USA PATRIOT Act. Mr. Baker has been in the Council for Intelligence Policy in the Office of Intelligence Policy and Review at the Department of Justice since 2002. He served as acting counsel from May 2001 until January 2002.

Prior to that, he was OIPR's Deputy Counsel for Intelligence Operations. Prior to joining OIPR, he served as a Federal prosecutor, handling numerous international white collar crimes for the Criminal Division of the Department of Justice. Mr. Baker was awarded his undergraduate degree from the University of Notre Dame, and his J.D. and M.A. from the University of Michigan.

Our next witness is Mr. Robert Khuzami, former Assistant United States Attorney in the U.S. Attorney's Office for the Southern District of New York. While in that office, he served in the office's terrorism unit. Mr. Khuzami clerked for the Honorable John R. Gibson of the U.S. Court of Appeals for the 8th Circuit in Kansas City, Missouri. Mr. Khuzami attended the University of Rochester and the Boston University School of Law.

Our final witness today is Mr. Gregory T. Nojeim, the Associate Director and Chief Legislative Counsel of the American Civil Liberties Union's Washington National Office. And at this time, on behalf of the Subcommittee, I would like to congratulate Mr. Nojeim in advance because I am told that next you will become the acting director of that office, so we congratulate you, Mr. Nojeim.

Prior to joining the ACLU, Mr. Nojeim served as Director of Legal Services of the American-Arab Anti-Discrimination Committee. He was graduated from the University of Rochester and the University of Virginia's School of Law.

Now, as we have told you all previously, we like to practice the 5-minute rule here. We have examined your written testimony that will be reexamined. So the panels that appear before you all on your desks there, when the amber light appears, you will have 1 minute to wrap up, and no one is going to be keel hauled if you violate the 5-minute rule, but if you could stay within—when the red light appears that indicates the 5 minutes have expired.

Mr. Wainstein, we will start with you, sir.

TESTIMONY OF KENNETH L. WAINSTEIN, INTERIM U.S. ATTORNEY, DISTRICT OF COLUMBIA

Mr. WAINSTEIN. Thank you, and good morning. My name is Ken Wainstein. I'm the U.S. Attorney here in the District of Columbia.

Mr. Chairman, Ranking Member Scott, and Members of the Subcommittee, thank you very much for inviting me here today to discuss two provisions of the USA PATRIOT Act, sections 206 and 215 that are critical to our counter terrorism and counter intelligence efforts.

These two sections are scheduled to sunset at the end of this year. If this is allowed to happen, we will find ourselves in the position where tools available to law enforcement in the fight against drugs, organized crime, and child pornography would be denied our national security investigators who are striving to protect our country against terrorism and espionage. Such an outcome would be a serious mistake, and, therefore, I am here today to ask you to make permanent sections 206 and 215 of the USA PATRIOT Act.

Section 206 allows the FISA Court to authorize roving quote unquote "roving surveillance" of a foreign power or an agent of a foreign power, such as a terrorist or spy.

Since 1986, we've had the authority to use roving wiretaps to investigate regular crimes, and this tool has proved critical to our ef-

forts against sophisticated criminals who regularly switch phones to avoid electronic surveillance.

In a case out of Florida, for example, our prosecutors and agents investigating a dangerous cell of Colombian drug dealers had gotten 23 separate wiretaps against cell members and leaders, but were failing to make a strong case because of the cell's practice of constantly cycling through cell phones.

Our people ultimately cracked the case when they got a roving wiretap that allowed them to continue surveillance as the cell members changed phones, and the suspects were ultimately arrested and convicted of distributing over a thousand kilograms of cocaine in our country.

In another drug investigation, in Chicago, investigators obtained roving surveillance authority after establishing that the drug lord target was purchasing blocks of prepaid cell phones and throwing each phone after a short period of use. In the course of about 7 months, this target went through at least 25 cell phones, thereby justifying the use of a roving wiretap under the criminal electronic surveillance statute.

Before the USA PATRIOT Act, however, national security investigators couldn't utilize such wiretaps in international terrorism or espionage investigations. Experience shows that terrorists and spies are every bit as crafty at avoiding surveillance as common criminals.

To see that, we need look no further than the Al-Qaeda training manual that warns members that quote, "communication can be a knife dug into our back if we do not take the necessary security measures." Close quote. And that manual directs Al-Qaeda members to undertake a variety of measures to counter our electronic surveillance efforts.

With no roving authority for national security investigators, the terrorists and spies used to have the advantage, and they could stay one or two steps ahead of our investigators by switching phones.

Thankfully, section 206 balanced the playing field by authorizing the use of roving wiretap authority in national security investigations. Some have expressed concerns that wiretaps, roving wiretaps, somehow open the door to unconstitutional intrusion into our privacy.

This concern is best addressed by looking at the various safeguards in the statute that protect against abuse and overreaching.

First, we can only get a roving wiretap if we show probable cause to believe that the target of a roving surveillance order is either a foreign power or an agent of a foreign power, such as a terrorist or spy. To make that showing, we must know the target's name or else describe the target with sufficient specificity to convince the FISA Court that there's probable cause to believe that that target is a foreign power and agent of a foreign power.

We have to show that that target is taking action, such as switching phones, that may have the effect of thwarting surveillance. And finally, roving surveillance under 206 carries all the court approved minimization procedures that limit all FISA surveillance.

Because of these procedures and safeguards, all appellate courts that have heard challenges to roving wiretaps have upheld their constitutionality.

Section 215. This section provides national security investigators with the authority to ask the FISA Court to order the production of the same kind of tangible things, such as business records, that prosecutors have long been able to acquire through grand jury subpoenas and criminal investigations.

As a prosecutor, I can tell you from first hand experience that the ability to obtain records with grand jury subpoenas is an essential tool for law enforcement. Investigating crime without subpoena power would be like Tiger Woods playing the Masters without a putter.

Before the USA PATRIOT Act, however, it was difficult for national security investigators to obtain business records, as the FISA Court could only authorize orders for certain categories of records.

For example, an agent prior to the PATRIOT Act who was investigating a terrorism suspect would not have been able to get a FISA Court order to obtain records showing that that suspect purchased bulk quantities of fertilizer to produce a bomb because a feed store is not a quote "common carrier, public accommodation facility, physical storage, or rental facility," the entities for which the old law authorized the use of FISA Court orders.

Section 215 remedied that glaring problem by authorizing investigators to request the production of any tangible things that are relevant to the investigation. In my experience as a prosecutor, I view section 215 as a commonsense investigative tool. I recognize, however, that the provision has been subject—the subject of concern by many across the country.

Once again, I believe part of the problem here is that people don't understand the safeguards that are in the statute. 215 has a number of these safeguards, which we'll discuss today.

Unlike grand jury subpoenas, it requires prior court approval. It protects against the use of 215 orders to investigate activities based solely on the exercise of first amendment rights. They have a narrow scope, and they are subject to congressional oversight.

Like 206, section 215 fully safeguards privacy while providing us the tools we need to protect our country against international terrorists and spies.

Given the threat these individuals pose to our nation, I urge Congress to allow us the continued use of these vital tools.

[The prepared statement of Mr. Wainstein follows:]

PREPARED STATEMENT OF KENNETH L. WAINSTEIN

KEN WAINSTEIN
UNITED STATES ATTORNEY
DISTRICT OF COLUMBIA
PREPARED REMARKS FOR THE
SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY
COMMITTEE ON THE JUDICIARY
UNITED STATES HOUSE OF REPRESENTATIVES
APRIL 28, 2005

I. Introduction

Mr. Chairman, Ranking Member Scott, and Members of the Subcommittee, thank you for the invitation to appear before you today to discuss two important provisions of the USA PATRIOT Act. Section 206 of the Act provides national security investigators with the ability to obtain roving surveillance orders from the Foreign Intelligence Surveillance Court ("FISA Court"), and section 215 authorizes the FISA Court to issue orders requiring the production of business records relevant to national security investigations. Criminal investigators have long enjoyed similar authorities for years, and I have seen firsthand how the ability to obtain roving wiretap orders and relevant business records have assisted law enforcement in combating serious crime.

Sections 206 and 215, however, are currently scheduled to sunset at the end of 2005. If this is allowed to happen, then we will once again be in a position where tools available to law enforcement in the fight against drugs, organized crime, and child pornography would not be at the disposal of national security investigators for use in the war against terrorism. Such an outcome would be a tragic mistake, and I am therefore here today to ask you to make permanent sections 206 and 215 of the USA PATRIOT Act.

II. Section 206

Section 206 of the USA PATRIOT Act allows the FISA Court to authorize "roving" surveillance of a foreign power or an agent of a foreign power, such as a terrorist or spy. A "roving" wiretap order attaches to a particular target rather than a particular phone or other communication facility. Since 1986, law enforcement has been able to utilize court-approved roving wiretaps in appropriate cases to investigate ordinary crimes, including drug offenses and racketeering. Investigators and prosecutors know from hard experience that a traditional wiretap order that applies to a single phone is often not effective because sophisticated criminals can change phones to thwart surveillance more quickly than investigators can go to court to obtain a new wiretap order.

Before the USA PATRIOT Act, however, while law enforcement investigators could utilize roving wiretaps in criminal investigations, national security investigators could not utilize such wiretaps in international terrorism or espionage investigations. To put it simply, this inconsistency in the law not only defied common sense, because well-trained terrorists and spies as a general matter are even more skilled at evading surveillance than the average criminal, it also significantly hampered our ability to effectively monitor terrorists and spies. We know that Al Qaeda members go to great lengths to foil our electronic surveillance efforts. A seized Al Qaeda training manual warns members that "communication . . . can be a knife dug into our back if we do not . . . take the necessary security measures." It then describes the means by which we conduct electronic surveillance and directs the Al Qaeda "brothers" to undertake a variety of measures to counter those efforts. Thankfully, however, section 206 remedied this

problem by authorizing the use of roving wiretap authority in national security investigations, thus putting investigators in a better position to keep up with international terrorists or spies, rather than falling one or two steps behind every time they change phones.

Because some, including Members of this Subcommittee, have expressed concerns about the use of roving wiretaps in national security investigations, I would like to discuss briefly the important privacy safeguards contained in section 206. To begin with, it is important to note that section 206 did not change the requirement that the target of roving surveillance must be identified or described in a surveillance order issued by the FISA Court. Therefore, a roving surveillance order is always connected to a particular target. To be clear, roving surveillance orders do not jump from target to target; rather, they follow a particular target as that target jumps from phone to phone. The FISA Court also must find that there is probable cause to believe the target of a roving surveillance order, just like any electronic surveillance order, is either a foreign power or an agent of a foreign power, such as a terrorist or a spy. To be sure, some have complained that FISA allows for the use of roving surveillance in cases where the government describes, rather than identifies, the target of surveillance. It is critical, however, to keep in mind that the government's description of the target must be sufficiently specific to convince the FISA Court that there is probable cause to believe that the target is a foreign power or agent of a foreign power.

Additionally, roving surveillance under section 206 can be authorized by the FISA Court only after it makes a finding that the actions of the target may have the effect of thwarting the identification of those, such as the telephone company, whose assistance

will be needed to carry out the surveillance. And finally, while there has been concern expressed that roving surveillance may intrude on the privacy of innocent Americans, section 206 in no way altered the requirement that FISA surveillance orders include court-approved minimization procedures to limit the acquisition, retention, and dissemination by the government of information or communications involving United States persons.

Whether in the criminal or national security realm, roving wiretaps recognize the technological realities of our modern age, in which a criminal or terrorist can change communications devices in the blink of an eye. Roving surveillance, however, also fits well within our longstanding and revered constitutional tradition of respecting civil liberties. For example, the United States Courts of Appeals for the Second, Fifth, and Ninth Circuits all have squarely ruled that "roving" wiretaps are perfectly consistent with the Fourth Amendment, and no court of appeals has reached a contrary conclusion.

III. Section 215

Section 215 provides national security investigators with the authority to ask the FISA Court to order the production of the same kinds of tangible things, such as business records, that prosecutors have long been able to acquire through grand-jury subpoenas in criminal investigations. As a prosecutor, I can tell you from firsthand experience that the ability to obtain records with grand-jury subpoenas is an essential tool for law enforcement. In criminal investigations, such subpoenas are routinely used to obtain all types of records. Asking law enforcement to effectively investigate and prosecute crime without using grand-jury subpoenas to obtain records would be like asking Tiger Woods to win the Masters without using a putter. The records obtained through grand jury

subpoenas often represent the critical building blocks of a successful criminal investigation and are used to determine whether the use of more intrusive investigative techniques, such as physical searches, are justified.

Before the USA PATRIOT Act, however, it was very difficult for national security investigators to request the production of business records in international terrorism and espionage investigations. For example, such investigators could only ask the FISA Court to order the production of records from "a common carrier, public accommodation facility, physical storage facility or vehicle rental facility." This patchwork of court order authority was confusing to investigators, who had to determine if the records they needed fit within one of these categories before deciding whether to seek a FISA Court order. Moreover, it left investigators without the ability to obtain a court order for records that could be vitally important to terrorism investigators. Under the prior law, for example, an investigator would not have been able to get a FISA court order to obtain records showing that a suspect purchased bulk quantities of fertilizer to produce a bomb because a feed store is not "a common carrier, public accommodation facility, physical storage facility or vehicle rental facility." Section 215 of the USA PATRIOT Act eliminated this restriction on the types of entities from whom records could be obtained. Now, investigators may ask the FISA Court to request the production of "any tangible things (including books, records, papers, documents, and other items)" from any type of entity. Section 215 therefore allows national security investigators to obtain the same types of records that grand juries have always been able to subpoena in the criminal context.

Because investigations into international spies and terrorists often can only be effective if the targets are unaware they are being investigated, court orders under this provision prohibit the recipient from telling others -- including the target -- about the order. This non-disclosure provision is akin to that which Congress has authorized for other types of process – such as subpoenas to financial institutions in criminal cases under the Right to Financial Privacy Act and under 18 U.S.C. 2703 relating to toll and subscriber records and stored wire and electronic communications. It only makes sense to apply a similar requirement in national security investigations, where the need for secrecy is greater and the stakes for the safety of our country is higher.

Given my experience as a prosecutor, I view section 215 as a common-sense investigative tool. I recognize, however, that the provision has been the subject of concern by many across the country. Part of the reason for this, I believe, is that many of the safeguards contained in section 215 to protect civil liberties are not widely known or understood.

Upon close examination, for instance, it is clear that orders requesting the production of records under section 215 are actually more protective of civil liberties than are grand jury subpoenas. Grand jury subpoenas and section 215 orders are governed by a similar standard of relevance; investigators may only seek to obtain records that are relevant to an ongoing investigation. To obtain any records under section 215, however, investigators must first obtain a court order. Grand jury subpoenas, by comparison, do not require prior judicial approval.

Section 215, unlike grand jury subpoenas, also explicitly protects First Amendment activities as investigations utilizing the provision may not be solely based on

such activities. For example, Americans may not be investigated under the provision solely because of their political speech. Section 215 also has a very narrow scope; it can only be used (1) "to obtain foreign intelligence information not concerning a United States person"; or (2) "to protect against international terrorism or clandestine intelligence activities." It cannot be used, as can grand jury subpoenas, to investigate domestic terrorism or ordinary crimes. And finally, section 215, unlike grand jury subpoenas, is subject to regular congressional oversight. The Attorney General is required to file reports with appropriate congressional committees on a semi-annual basis fully informing them of the Department's use of the provision.

To some, section 215 has become known as "the library provision". This moniker, however, is a gross distortion of the provision and makes about as much sense as calling all grand jury subpoenas "library subpoenas." Section 215 does not single out or mention libraries, and the Attorney General has recently declassified that as of March 30, 2005, the provision had never be used to obtain library records.

As explained above, section 215 can be used to request the production of a wide variety of records, and library records are simply one of the types of records to which the provision could theoretically be applied. While some have called for library and bookstore records to be exempted from section 215, I think that this course of action would be a serious mistake.

Libraries should not be carved out as safe havens for terrorists and spies. We know for a fact that terrorists and spies use public libraries. In the spring of 2004, to give one example, federal investigators in New York conducted surveillance on an individual who was associated with al Qaeda. In the course of tracking the individual, investigators

noted that, although he had a computer at his home, he repeatedly visited a library to use the computer. Investigators discovered that the individual was using the library computer to e-mail other terrorist associates around the world. The library's hard drives were scrubbed after each user finished, and he used the computer at the library because he believed that the library permitted him to communicate free of any monitoring. Thankfully, this individual is now in federal custody. But this example should teach us that we should not make it more difficult to investigate a terrorist's use of a library computer than his or her use of a home computer.

In criminal investigations, prosecutors have subpoenaed library records for years. For example, in the 1997 Gianni Versace murder case, a Florida grand jury subpoenaed records from public libraries in Miami Beach. Similarly, in the Zodiac gunman investigation, after investigators came to believe that a Scottish occult poet inspired the gunman, they prompted a grand jury in New York to subpoena library records to learn who had checked out the poet's books. And the Iowa Supreme Court has even upheld the use of subpoenas to obtain library records in an investigation of cattle mutilation. Surely, if grand jury subpoenas could be used to obtain such records in these criminal investigations, national security investigators, with court approval, should have the option of obtaining these records in appropriate international terrorism or espionage investigations.

Just as prosecutors use grand jury subpoenas in a responsible manner, information recently declassified by the Justice Department reveals that the Department has used section 215 in a judicious manner. As of March 30, 2005, federal judges have reviewed and granted the Department's request for a section 215 order 35 times. To date, the

provision has only been used to obtain driver's license records, public accommodations records, apartment leasing records, credit card records, and subscriber information, such as names and addresses, for telephone numbers captured through court-authorized pen registers and trap-and-trace orders (a pen register records the numbers a telephone dials and a trap-and-trace device records the numbers from which it receives calls). The Department has not requested a section 215 order to obtain library or bookstore records, medical records, or gun sale records.

Like section 206, section 215 is scheduled to sunset at the end of 2005, and it is important that the provision is made permanent. If section 215 were allowed to expire, it would be easier for prosecutors to obtain relevant records in investigations of non-violent crimes than for national security investigators to obtain relevant records in international terrorism investigations. Given the threat to the safety and security of the American people posed by terrorist groups such as al Qaeda, Congress must not let this happen.

IV. Conclusion

Thank you once again for the opportunity to discuss sections 206 and 215 of the USA PATRIOT Act. These two provisions are critical to the Department's efforts to protect Americans from terrorism, and from my experience as a prosecutor, I know firsthand the importance of roving wiretap orders and the ability to obtain relevant records in criminal investigations. I look forward to answering any questions you might have.

Mr. COBLE. Thank you, Mr. Wainstein. Mr. Baker.

TESTIMONY OF JAMES BAKER, COUNSEL FOR INTELLIGENCE POLICY, U.S. DEPARTMENT OF JUSTICE

Mr. BAKER. Thank you, Chairman Coble, Ranking Member Scot, and Members of this Subcommittee.

I am pleased to be again before you to discuss the Government's use of the authorities granted to it by Congress under FISA, including amendments to FISA and the USA PATRIOT Act.

As I mentioned on Tuesday, these provisions have made a critical contribution to our ability to protect the national security of the United States.

For the benefit of Members who were unable to attend on Tuesday, my office conducts oversight of the intelligence and counter intelligence activities of executive branch agencies, including the FBI.

We prepare all FISA applications and represent the United States before the FISA Court.

I report directly to the Deputy Attorney General. I'm a career member of the senior executive service, and not a political appointee.

Again, rather than simply read my written statement into the record, I'd like to make a few general points about FISA, and amplify on some of my prior comments from the other day.

As I mentioned the other day, the purpose of FISA was to—as enacted in 1978—was to provide legislative authorization for and regulation of electronic surveillance conducted within the United States for foreign intelligence purposes. FISA was not intended to prohibit collection of important intelligence information, but to subject such collection to statutory procedures.

Over the years, Congress has expanded the scope of FISA to create mechanisms for the Government to obtain separate authorizations for pen registers, searches, and to obtain access to business records and other tangible things.

Prior to the enactment of FISA, the Executive Branch conducted electronic surveillance to collect foreign intelligence information without a warrant, based upon the President's inherent constitutional authority to do so.

In the 1970's, however, abuses of domestic national security surveillance were disclosed. As a result, Congress looked for an appropriate mechanism to safeguard civil liberties, consistent with the needs of national security.

Since the enactment of FISA, 27 years ago, I submit that there has been no repeat of the abuses of the past. I believe this is so for several reasons.

First, there are now clear standards for determining who may be a legitimate target of a FISA surveillance or search. The only authorized targets of FISA full content collection are foreign powers and agents of foreign powers, both of which are defined terms in the act.

Similarly, FISA only permits the use of other collection activities, such as orders for tangible things, when there is a sufficient nexus between the information that will be collected and a legitimate intelligence investigation.

When such an investigation involves a U.S. person, it cannot be based solely upon protected first amendment activities.

Second, there is accountability for authorizations for national security collection. FISA includes several mechanisms to ensure written accountability within the Executive Branch for the decision to engage in foreign intelligence collection, including a requirement that the Attorney General or his deputy personally sign each full content application. This serves as a check on Executive Branch arbitrariness.

In addition, the Attorney General must fully inform the intelligence committees of both Houses of Congress on our use of FISA on a regular basis.

Third, there is judicial oversight of our actions. Whenever a surveillance or search for foreign intelligence purposes may involve the fourth amendment rights of any U.S. person, approvals for such collection must come from a neutral and detached Federal judge. Moreover, even when fourth amendment rights are not implicated, such as for third party business records, FISA still requires approval by a Federal judge or a magistrate before the Government may engage in such collection.

Finally, FISA contains other provisions to protect the privacy of Americans, most notably including court-ordered minimization procedures. The Government may only conduct a full content surveillance or search when there are adequate procedures in place to minimize the intrusion into the privacy of Americans. This includes minimization of the acquisition, retention, and dissemination of information about U.S. persons obtained pursuant to full content collection under FISA.

In conclusion, as we proceed with our discussion today, we must remember that it's our collective fundamental task to determine how best to protect the national security of the United States in a manner consistent with the Constitution. We must be mindful, as the Supreme Court stated in the Keith case in 1972, that unless Government safeguards its own capacity to function and to preserve the security of its people, society itself could become so disordered that all rights and liberties would be endangered.

I am proud to be here today to represent the dedicated men and women OIPR who work diligently everyday to do their part to protect both the national security and the Constitution of the United States, and to enforce the laws as enacted by Congress, especially FISA. With these principles in mind, I'm happy to answer any questions that the committee may have.

[The prepared statement of Mr. Baker follows:]

PREPARED STATEMENT OF JAMES A. BAKER

Testimony of
James A. Baker
Counsel for Intelligence Policy
Office of Intelligence Policy and Review
United States Department of Justice
before the
Subcommittee on Crime, Terrorism, and Homeland Security
Committee on the Judiciary
United States House of Representatives

April 28, 2005

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

I am pleased to be here today to discuss the government's use of authorities granted to it by Congress under the Foreign Intelligence Surveillance Act of 1978 (FISA). In particular, I appreciate the opportunity to have a candid discussion about the impact of the amendments to FISA under the USA PATRIOT Act and how critical they are to the government's ability to successfully prosecute the war on terrorism and prevent another attack like that of September 11 from happening again.

As Counsel for Intelligence Policy in the Department of Justice, I am head of the Office of Intelligence Policy and Review (OIPR). OIPR conducts oversight of the intelligence and counterintelligence activities of the Executive Branch agencies including the FBI. We prepare all applications for electronic surveillance and physical search under FISA and represent the government before the Foreign Intelligence Surveillance Court (FISA Court). OIPR reports directly to the Deputy Attorney General. I am a career member of the Senior Executive Service, not a political appointee.

I. FISA Statistics

As I noted in my testimony before this Subcommittee on Tuesday, since September 11, the volume of applications to the FISA Court has dramatically increased from 1,012 applications for surveillance or search filed under FISA in 2000 to 1,758 applications in 2004.

II. Key Uses of FISA Authorities in the War on Terrorism

In enacting the USA PATRIOT Act, the Intelligence Authorization Act for Fiscal Year 2002, and the Intelligence Reform and Terrorism Prevention Act of 2004, Congress provided the government with vital tools that it has used regularly and effectively in its war on terrorism. The reforms in those measures affect every single application made by the Department for electronic surveillance or physical search of suspected terrorists and have enabled the government to become quicker and more flexible in gathering critical intelligence information on suspected terrorists. It is because of the key importance of these tools to winning the war on terror that the Department asks you to reauthorize the USA PATRIOT Act provisions scheduled to expire at

the end of this year. Today, it is my understanding the Committee wishes to discuss sections 206 and 215 of the USA Patriot Act. Both provisions are scheduled to sunset at the end of the year.

A. Roving Wiretaps

Section 206 of the USA PATRIOT Act extends to FISA the ability to "follow the target" for purposes of surveillance rather than tie the surveillance to a particular facility and provider when the target's actions may have the effect of thwarting that surveillance. As you know, in his testimony earlier this month before the Senate Judiciary Committee, the Attorney General declassified the fact that the FISA Court issued 49 orders authorizing the use of roving surveillance authority under section 206 as of March 30, 2005. Use of roving surveillance has been available to law enforcement for many years and has been upheld by several federal courts, including the Second, Fifth, and Ninth Circuits. Some object that this provision gives the FBI discretion to conduct surveillance of persons who are not approved targets of court-authorized surveillance. This is wrong. Section 206 did not alter the requirement that before approving electronic surveillance, the FISA Court must find that there is probable cause to believe that the target of the surveillance is either a foreign power or an agent of a foreign power, such as a terrorist or spy. Without this authority, investigators will once again have to struggle to catch up to sophisticated terrorists trained to constantly change phones in order to avoid surveillance.

Critics of section 206 also contend that it allows intelligence investigators to conduct "John Doe" roving surveillance that permits the FBI to wiretap every single phone line, mobile communications device, or Internet connection the suspect may use without having to identify the suspect by name. As a result, they fear that the FBI may violate the communications privacy of innocent Americans. Let me respond to this criticism in the following way. First, even when the government is unsure of the name of a target of such a wiretap, FISA requires the government to provide "the identity, if known, or a description of the target of the electronic surveillance" to the FISA Court prior to obtaining the surveillance order. 50 U.S.C. §§ 1804(a)(3) and 1805(c)(1)(A). As a result, each roving wiretap order is tied to a particular target whom the FISA Court must find probable cause to believe is a foreign power or an agent of a foreign power. In addition, the FISA Court must find "that the actions of *the target* of the application may have the effect of thwarting" the surveillance, thereby requiring an analysis of the activities of a foreign power or an agent of a foreign power that can be identified or described. 50 U.S.C. § 1805(c)(2)(B). Finally, it is important to remember that FISA has always required that the government conduct every surveillance pursuant to appropriate minimization procedures that limit the government's acquisition, retention, and dissemination of irrelevant communications of innocent Americans. Both the Attorney General and the FISA Court must approve those minimization procedures. Taken together, we believe that these provisions adequately protect against unwarranted governmental intrusions into the privacy of Americans. Section 206 sunsets at the end of this year.

B. Access to Tangible Things

Section 215 of the USA PATRIOT Act allows the FBI to obtain business records or other tangible things under FISA pursuant to a FISA Court order if the items relate to an ongoing authorized national security investigation, which, in the case of a United States person, cannot be based solely upon activities protected by the first amendment to the Constitution. The Attorney General also recently declassified the fact that the FISA Court has issued 35 orders under section 215 from the effective date of the Act through March 30th of this year. The Attorney General also declassified the types of business records sought by these orders. They include driver's license records, public accommodation records, apartment leasing records, credit card records, and subscriber information, such as names and addresses, for telephone numbers captured through court-authorized pen register devices. None of those orders were issued to libraries and/or booksellers, or were for medical or gun records.

Section 215 provides a tool under FISA that is similar to a grand jury subpoena in the criminal context. A prosecutor in a criminal case can issue a grand jury subpoena to obtain items relevant to his investigation. Section 215 provides a mechanism for obtaining records or items relevant to an investigation to protect against international terrorism or clandestine intelligence activities. Section 215 orders, however, are subject to greater judicial oversight than are grand jury subpoenas before they are issued. The FISA Court must explicitly authorize the use of section 215 to obtain business records before the government may serve the request on a recipient. In contrast, grand jury subpoenas are not subject to judicial review before they are issued. Section 215 orders are also subject to the same burden of proof standard as are grand jury subpoenas — a relevance standard.

Section 215, which makes no reference to libraries and booksellers, has been criticized because it does not exempt libraries and booksellers. The absence of such an exemption is consistent with criminal investigative practice. Prosecutors have always been able to obtain records from libraries and bookstores through grand jury subpoenas. Libraries and booksellers should not become safe havens for terrorists and spies. While section 215 has never been used to obtain such records, last year, a member of a terrorist group closely affiliated with al Qaeda used Internet service provided by a public library to communicate with his confederates. Furthermore, we know that spies have used public library computers to do research to further their espionage and to communicate with their co-conspirators. For example, Brian Regan, a former TRW employee working at the National Reconnaissance Office, who recently was convicted of espionage, extensively used computers at five public libraries in Northern Virginia and Maryland to access addresses for the embassies of certain foreign governments. A terrorist using a computer in a library should not be afforded greater privacy protection than a terrorist using a computer in his home.

Concerns that section 215 allows the government to target Americans because of the books they read or websites they visit are misplaced. The provision explicitly prohibits the government from obtaining a section 215 order if an investigation were to be based solely upon protected First Amendment activity. 50 U.S.C. §§ 1861(a)(2)(B). However, some criticisms of section 215 have apparently been based on possible ambiguity in the law. The Department has already stated in litigation that the recipient of a section 215 order may consult with his attorney and may challenge that order in court. The Department has also stated that the government may

seek, and a court may require, only the production of records that are relevant to a national security investigation, a standard similar to the relevance standard that applies to grand jury subpoenas in criminal cases. The text of section 215, however, is not as clear as it could be in these respects. The Department, therefore, is willing to support amendments to Section 215 to clarify these points. Section 215 is scheduled to sunset at the end of 2005.

Conclusion

It is critical that the elements of the USA PATRIOT Act subject to sunset in a matter of months be renewed. The USA PATRIOT has greatly enhance the government's ability to effectively wage the war on terrorism.

I thank the Committee for the opportunity to discuss the importance of the USA PATRIOT Act to this nation's ongoing war against terrorism. I appreciate the Committee's close attention to this important issue. I would be pleased to answer any questions you may have. Thank you.

Mr. COBLE. Mr. Baker, you've been on the Hill several times. You know how to beat that red light. You did it again.

Mr. BAKER. Thank you, sir.

Mr. COBLE. Mr. Khuzami, good to have you with us, sir.

TESTIMONY OF ROBERT KHUZAMI, FORMER ASSISTANT U.S. ATTORNEY, SOUTHERN DISTRICT OF NEW YORK

Mr. KHUZAMI. Thank you. Chairman Coble, Ranking Member Scott, Members of the Subcommittee, it's an honor to testify before you today in a matter of such importance to our national security.

For nearly 12 years, I was an Assistant United States Attorney in the U.S. Attorney's Office in the Southern District of New York, and spent a significant amount of time working on terrorism cases. I was a member of the team that in 1995 prosecuted Sheik Omar Abdel-Rahman, the blind cleric and head of the Egyptian Islamic Group, and 11 others for conducting a war of urban terrorism against the United States. The acts of that group included among other things the 1993 bombing of the World Trade Center; the murder in 1990 of Rabbi Meir Kahane, the head of the Jewish Defense League; and a conspiracy to carry out a day of terror in New York, the planned simultaneous bombing of various New York City landmarks, including the United Nations complex, the Lincoln and Holland Tunnels, and the FBI's New York headquarters.

I was also involved in assisting in the supervision of the U.S. Attorney's Command Post in lower Manhattan following the events of 9/11.

I am here today to support reauthorization of sections 215 and 206 of PATRIOT Act.

I'll confine my remarks this morning to section 215.

Some view it as a radical extension of Government authority that permits unprecedented snooping into the private reading habits of Americans and threatens to sweep innocent Americans into secret terrorism investigations.

My experience teaches me otherwise.

Section 215 simply and modestly is designed to permit the Government to collect standard business records from third parties relevant to foreign intelligence or terrorism investigations. These are the same records that prosecutors across the country every day routinely obtain in drug, and larceny, and fraud, and corruption investigations.

They're credit card receipts. They're bank statements. They're hotel bills. They're leases, and so on. There is nothing unusual or nothing accusatory of asking innocent third parties to produce such records in terrorism investigations.

Second, terrorists use libraries. The 9/11 Commission found that to be case that some had used Internet access in a Hamburg, Germany library. A recent espionage prosecution revealed that a spy had used computer terminals at various public libraries to send classified information. An Al-Qaeda terrorist used library computer terminals to send electronic messages.

The Unabomber, Ted Kaczynski, in a criminal investigation, was captured in part when the police obtained his library records and learned that he had borrowed from his local library obscure books that were cited in his widely distributed Manifesto.

Third, section 215 neither targets nor exempts library records. Nor has it been used for that purpose, as the Chairman has pointed out.

This doesn't mean that section 215, however, should be amended to exempt libraries and bookstores, for their records could be critical in a terrorism investigation. Lack of use is not the same thing as lack of importance. In a terrorism case, even a single missed opportunity or misstep can have catastrophic consequences. That is simply not the case in criminal investigations.

Fourth, section 215 provisions do protect the privacy and civil liberties of Americans. It can't be used to investigate a U.S. person based solely on first amendment activities and not at all to investigate domestic terrorism. The Foreign Intelligence Surveillance Court must approve section 215 applications.

Fifth, section 215 properly expanded the type of records obtainable in terrorism investigations beyond what had been the law—simple lodging or vehicle rental or storage facilities.

This corrected the anomaly that allowed the Government to obtain a would-be terrorist's motel records, but not receipts evidencing purchases of explosives or precursor chemicals or books on how to manufacture explosives.

Sixth, section 215 also eliminated the previous requirement that the Government provide specific articulable facts that are the subject—that the subject of the investigation was an agent of a foreign power. As a legal matter, this standard only applies where there exists some legally recognized privacy interest, and there is no such interest in section 215 records.

There may be some circumstances where such a strict standard should apply even though there's no privacy interest at stake, but national security is not one of those instances. It is where the public interest in Government access, in my view, is most urgent.

Next, the Department of Justice interprets and has endorsed amendments that would allow those getting section 215 orders to consult with attorneys and challenge the order and its scope before the FISA Court. That change protects citizens against improper use of section 215.

Lastly, there has been some concern expressed about rogue agents, agents who may be inclined to violate the civil liberties of Americans by looking for ways to circumvent the law in order to learn what we read and what organizations we belong to. The agents and translators and surveillance specialists and analysts that I worked with were dedicated, talented, and law abiding. And there are many procedures designed to prevent that from happening.

But even if you can't eliminate the occasional rogue, the empirical evidence from the Department of Justice Inspector General establishes that not a single case of abuse of civil rights or liberties from the PATRIOT Act has been documented.

I strongly urge the committee to reauthorize section 215. I'd be happy to answer any questions.

[The prepared statement of Mr. Khuzami follows:]

PREPARED STATEMENT OF ROBERT S. KHUZAMI

Chairman Coble, Representative Scott, and members of the Subcommittee on Crime, Terrorism and Homeland Security, thank you for inviting me here this morning. It is an honor to testify before you, particularly on a matter of such importance to our national security.

I am currently a lawyer in private practice in the New York area. For nearly 12 years, I was an Assistant United States Attorney in the United States Attorney's Office for the Southern District of New York, and spent a significant amount of time working on counterterrorism cases. From shortly after the February 26, 1993 bombing of the World Trade Center through early 1996, I was a member of the team that prosecuted Sheik Omar Abdel Rahman—the blind cleric who led the Egyptian-based Islamic Group and played a key role in the 1981 assassination of President Sadat—and eleven others for conducting a war of urban terrorism against the United States. Their acts included, among other things, the WTC bombing, the 1990 murder of Rabbi Meir Kahane (the founder of the Jewish Defense League), plots to murder various political and judicial leaders, and a conspiracy to carry out a "Day of Terror"—the simultaneous bombing of various New York City landmarks, including the United Nations complex, the Lincoln and Holland Tunnels (through which thousands of commuters travel daily between lower Manhattan and New Jersey), and the Jacob K. Javits Federal Building that houses the FBI's New York Headquarters.

Following the events of 9/11, I assisted in supervising the U.S. Attorney's Command Post in lower Manhattan, where hundreds of law enforcement and intelligence personnel worked tirelessly to investigate that attack and to prevent another.

The changes set forth in the PATRIOT Act, as well as the events of 9/11 in general, have brought about significant public debate about the appropriate balance of civil liberties, privacy and security. That debate is undeniably healthy, a fact which Congress recognized when it sunsetted certain PATRIOT Act provisions in order to provide an opportunity for an informed evaluation of their impact.

Two PATRIOT Act provisions are being considered this morning—Section 206, the so-called "roving wiretap" provision and Section 215, the access to records provision.

I approach my analysis from two perspectives. The first is that of an ex-prosecutor of terrorism crimes, who believes firmly that we must fully identify and utilize every lawful tool to prevent terrorist attacks and capture those involved. The second is as an American citizen who recognizes the fundamental importance of the privacy rights and civil liberties of all Americans. Balancing these two perspectives, I conclude that, with two amendments recently embraced by the Department of Justice ("DOJ"), Sections 215 and 206 should be reauthorized.

SECTION 215

Section 215 authorizes the Foreign Intelligence Surveillance Court to order the production of "tangible things (including books, records, papers, documents and other items)" as long as they are "sought for" an "authorized investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." In its most common application, Section 215 permits the government in terrorism investigations to obtain business records held by third parties, including those held by banks, hotels, landlords, credit card companies and, yes, libraries and bookstores. Somewhat surprisingly, Section 215 is viewed by many Americans as a radical extension of government authority that permits unprecedented snooping into the library records and private reading habits of Americans, and threatens to sweep up innocent Americans into secret investigations of terrorist activity. It has caused such angst amongst librarians that it has been labeled the "Angry Librarians Provision."

Four points need to be made. First, Section 215 permits a court to order the production of standard business records from third parties. These are the same records that prosecutors across the country routinely obtain every day in drug, larceny, fraud, corruption and all manner of standard criminal investigations. They include credit card receipts, bank statements, hotel bills, leases, subscriber information for phones, and the list goes on and on. There is nothing unusual or accusatory about requiring third parties possessing these records—innocent third parties all of them—to produce them in a terrorism investigation of another person. That is all Section 215 does.

Second, Section 215 is agnostic about libraries and bookstores—it neither targets nor exempts them, and the word "library" is nowhere mentioned in its text. In fact, rather than aggressively use Section 215 to collect information about library patrons, as some have feared, the government recently reported that it has obtained Section 215 orders on 35 occasions, but never once for library records. Presumably,

this reflects the fact that library records are rarely relevant to terrorism investigations, a fact that should assuage its critics.

Third, terrorists use libraries. The 9/11 Commission found that some of the 9/11 conspirators used Internet access through a Hamburg, Germany library. A recent espionage prosecution revealed that a spy used computer terminals at various public libraries to send classified information. An Al Qaeda terrorist used library computer terminals to send electronic messages. Terrorists and their sympathizers also create, collect and disseminate writings and speeches that train, recruit and incite others to participate in terrorist acts. In the Blind Sheik prosecution, for example, evidence consisting of bomb-making manuals, including pages containing the fingerprints of co-conspirators, was introduced at trial. In his written sermons, the Blind Sheik extolled the virtues of violent jihad against the United States with "the sword, with the cannon, with the grenades and with the missile," and urged his followers to embrace the terrorist label:

> Why do we fear the word "terrorist?" If the terrorist is the person who defends his right, so we are terrorists. And if the terrorist is the one who struggles for the sake of God, then we are terrorists. . . . They may say "he is a terrorist, he uses violence, he uses force." Let them say that.

It is for this reason that library records, writings and other literature have long been available to criminal investigators through the use of a grand jury subpoena. The "Unabomber," Ted Kaczynski, was captured based on a tip from his brother, who thought he recognized the writing in the Unabomber's "manifesto" as that of his brother. Law enforcement corroborated the brother's suspicion in part by examining library records, from which they learned that Kaczynski had checked out little-known books referenced in the manifesto. Section 215 simply extends to terrorism investigations the same authority available to criminal investigators.

Fourth, it does not follow that because the government's has not to date used Section 215 authority to obtain library records, that Section 215 should sunset, or be amended to exempt libraries and bookstores. This would turn libraries into sanctuaries, where would-be terrorists could communicate with their cohorts without fear of detection. This is not mere speculation—an Al Qaeda terrorist reportedly used library computer terminals to send messages to his associates around the world specifically because he knew the digital records were deleted nightly, thus concealing his activity. Unfortunately, some library representatives are creating *de facto* sanctuaries by ordering daily shredding of library log-in and other records, in response to misplaced fears about Section 215.

This "use it or lose it" argument is also specious because it equates lack of usage with lack of importance. The mere fact that Section 215 has not been "used" historically to obtain information from libraries or bookstores does not mean that such authority could not be critically important in the next case. More so than criminal prosecutions, terrorism plots, however speculative or nascent, must be zealously pursued by investigators armed with the option of using the fullest arsenal of lawful investigative tools. That is because even a single missed investigative opportunity or misstep can have catastrophic consequences. In contrast, in criminal investigations, for example, it is unfortunate but not fatal if before a stockbroker is arrested, he executes one more stock purchase using inside information. That is not being falsely alarmist; the horrific consequences of the detonation of a dirty bomb over a major urban center, or the Blind Sheik's plan to bomb multiple New York City landmarks simultaneously, are undeniable.

In sum, the four points establish a compelling case for Section 215 reauthorization. They show that Section 215 is not about libraries, but provides for routine document collection in terrorism cases; that as far as libraries are concerned, terrorists use them and library records can provide evidence of that; and that the catastrophic consequences of a successful terrorist attack demand that we have available all lawful investigative tools.

In addition to these points, the provisions of Section 215 should mollify critics, since they set forth a sensible framework to permit intelligence agents to obtain business records. Section 215 requires the government to certify that the records are "sought for an authorized investigation to obtain foreign intelligence information [not against a United States person] . . . to protect against international terrorism or clandestine intelligence activities." The DOJ interprets this provision as requiring that the records be "relevant" to such investigations, and has endorsed an amendment to that effect. In recognition of First Amendment concerns, Section 215 cannot be used to conduct an investigation based solely on the activities protected by the First Amendment.

The Foreign Intelligence Surveillance Court must approve Section 215 applications. While the level of that judicial review is not high, it is appropriate given the

type of records under consideration in Section 215 proceedings. Business and library records are preexisting documents that belong, will be given, or are available, to third parties—banks, landlords, rental car agencies and even librarians—and thus persons lack a reasonable expectation of privacy in them. For that reason, they are obtainable in a criminal investigation with a grand jury subpoena alone, which is issued without judicial review or supervision. From the perspective of judicial review, Section 215 provides more protection, not less, for library patrons than they enjoy in parallel criminal proceedings involving the same records.

To be sure, Section 215 expanded the government's pre-PATRIOT Act authority to obtain records in terrorism cases. This change was overdue, since the prior law was unnecessarily restrictive. Whereas Section 215 now permits the government to obtain with court approval all "tangible things (including books, records, papers, documents and other items)," the prior provision limited the government to obtaining records from lodging and vehicle rental and storage facilities. Again, criminal investigators have long been permitted to obtain the broader range of records now provided for in Section 215. Comparisons with criminal investigations aside, the expansion of authority under Section 215 makes sense in its own right, since it would be irrational, for example, to permit the government in a terrorism investigation to obtain under Section 215 a would-be terrorist's motel records, but deny it the ability to obtain receipts evidencing purchases of fertilizer or precursor chemicals, or to learn that he obtained books on how to manufacture explosive devices or detect surveillance.

Another expansion of authority in Section 215 was the elimination of the requirement that the government provide "specific articulable facts" that the subject of the investigation was an "agent of a foreign power." Critics assert that elimination of this particularized showing allows the government to use Section 215 to obtain records from persons without showing that they relate to a real terrorist or spy. Of course, as noted above, the third-party records at issue here do not implicate a recognized expectation of privacy. The government should generally be required to make a particularized showing only in circumstances where this is necessary to overcome some legally recognized privacy interest. There may be some instances where a departure from that general rule is warranted, but national security is not one of them—it is where the public interest in government access is most urgent. Leaving that aside, this change recognizes the reality that targets of terrorism investigations are trained to operate through multiple aliases and identities. It would serve no purpose to delay obtaining what might be records critical to uncovering a terrorist plot simply because the target's real name, or associational connections, has not yet been ascertained. Evidence of the purchase of detonators is equally relevant to preventing a terrorist plot, regardless of whether the government yet knows that the purchaser has ties to Al Qaeda. Once again, elimination of the requirement that a particularized showing be made places terrorism investigations on the same footing as criminal investigations, where no such showing is required to obtain the exact same records.

Critics cite excessive confidentiality—a "gag order"—as another flaw in Section 215. It prohibits persons receiving Section 215 orders from disclosing to third parties those orders or that the FBI has sought or obtained them. Section 215 detractors suggest that the threat of government overreaching in Section 215 would be less troubling if the statute allowed for more transparency, such that the public could understood what records the government sought and why. Critics also contrast Section 215's confidentiality provision with the grand jury process, where they claim the recipient receives notice of the subpoena and can move to quash it in court.

It is unassailable that real and potentially catastrophic harm can result from the premature disclosure of a terrorism investigation. I agree, however, that this risk does not justify barring recipients of Section 215 orders from consulting with attorneys, and from challenging the order before the Foreign Intelligence Surveillance Court. The DOJ has publicly agreed with this position. If such consultation and challenge were permitted, it would place Section 215 proceedings on a par with grand jury proceedings, where the subpoena recipient obviously knows of its existence and can challenge it in court, but at the same time may be prohibited from disclosing its existence to others.

Beyond this amendment, however, the confidentiality provisions of Section 215 should not be disturbed. You do not want potential terrorists to know you are investigating them or are aware of their plans. A leak could cause conspirators to accelerate the plot to a point where authorities are less prepared to prevent it or protect American lives. Or terrorists might abandon the plot, destroying evidence and taking flight, which would hinder prevention, capture and prosecution. The plot might later resurface, at a point when we are less prepared and more vulnerable. Each and all of these scenarios present a missed opportunity to protect innocent Ameri-

cans from harm. Premature disclosure also risks harm to agents, witnesses and undercover operatives. Against this risk of harm must be weighed the interests that are served from permitting the recipient of a Section 215 order to disclose it to persons other than an attorney. Whatever that interest is, it does not in my view outweigh the risk that flows from wrongful disclosure.

Some Section 215 criticisms assume the existence of large numbers of "rogue agents," who are characterized as inclined, given the opportunity, to violate the civil liberties and privacy rights of Americans by searching for and exploiting legal and administrative loopholes to browse through their reading materials and subscription and membership lists. This hypothetical rogue agent then becomes, so the argument goes, the justification for additional Section 215 restrictions. It is not apparent to what extent, if at all, such rogue agents exist. As Andy McCarthy wrote, agents "generally lack voyeuristic interest in the public's reading and viewing habits . . . and voluminous information streams and finite resources leave no time for this sort of malfeasance." [1] The agents, analysts, translators and surveillance specialists with whom I worked were dedicated, talented and law-abiding. And the gauntlet of administrative guidelines, directives, policies, laws and committees applicable to the FBI and DOJ, as well as congressional and judicial oversight, all deter rogues by providing training, oversight, and a mechanism for redress and discipline.

Even assuming rogues present the threat identified by Section 215 critics, it hardly follows that the restrictions they suggest would have the desired effect. Those determined to break rules are not easily deterred, and the real impact of such restrictions may be to unnecessarily burden the conscientious, law-abiding agent trying to do his job effectively. In the end, the best response to the "rogue agent" concern is the empirical evidence—according to the DOJ's Inspector General, who was required under Section 1001 of the PATRIOT Act to investigate complaints of abuse of civil rights and liberties under the Act, there have been no documented cases of abuse of civil rights or liberties from the PATRIOT Act in the more than three and one-half years since its passage.

In sum, Section 215 orders are useful investigative tools in combating terrorism. Most of what the statute permits is already available in criminal investigations, and any differences either make good investigative sense and, given the DOJ's willingness to consider two amendments, do not threaten the legitimate privacy and civil liberty interests of Americans.

SECTION 206

Section 206 of the PATRIOT Act provides for so-called "roving" wiretaps and other electronic surveillance in foreign intelligence and counterterrorism investigations. Prior to PATRIOT, once having obtained the approval of the Foreign Intelligence Surveillance Court for a wiretap, agents had to return to that Court each time the subject of that surveillance switched phones, in order to amend the order to direct the new electronic communications provider to give the technical assistance necessary to install and maintain the new wiretap. Due to concerns that targets were rapidly changing phones to avoid detection, including prior to important conversations and meetings, Section 206 eliminated the need for agents to return to the Court each time a target switched devices. It accomplished this by permitting the government, upon a showing that the subject is taking steps to thwart surveillance, to include in the original order a general directive that any electronic communications provider extending services to the target in the future must provide the necessary technical assistance.

In part because authority for "roving" wiretaps has long been available in criminal cases, the only serious criticism of section 206 is that it allows intelligence investigators to conduct "John Doe" roving surveillance that permits the FBI to wiretap every single phone line, mobile communications device, or Internet connection the suspect may use without having to identify the suspect by name. This criticism ignores hurdles that guard against overly-broad wiretapping. First, "roving" wiretaps are available only upon a showing that the subject is taking steps to avoid surveillance. Second, where agents cannot identify by name the target of a proposed wiretap, they must describe the subject with sufficient particularity to convince the FISA Court that there is probable cause to believe the subject is a "foreign power" or an "agent of a foreign power." That is, the wiretap order applies only to a specific person, even if the government has not yet ascertained his or her identity. The alternative—to make wiretaps unavailable until the target is identified—is a highly risky restriction, since valuable intelligence may be lost while a person's identity is investigated,

[1] *Patriot Debates: A Sourceblog for the USA PATRIOT Debate* (available at http://www.patriotdebates.com/214-and-215)

especially given that terrorists operate in a clandestine world and are trained to use multiple aliases and identities. Third, if the government wants to conduct a wiretap of a new target, it must return to the Court with a new application. Finally, agents conducting wiretap investigations must abide by "minimization" requirements, which strictly control the monitoring and retention of conversations by innocent persons not involved in the wrongful conduct.

These provisions provide adequate safeguards to protect the civil liberties and privacy interests of Americans.

CONCLUSION

I strongly urge the Committee to reauthorize Sections 206 and 215 of the PATRIOT Act. These provisions strike the correct balance between homeland security and civil liberties.

I thank the Committee for its time and attention, and would be happy to answer any questions.

Mr. COBLE. Thank you, Mr. Khuzami. Mr. Nojeim.

TESTIMONY OF GREGORY T. NOJEIM, ASSOCIATE DIRECTOR/ CHIEF LEGISLATIVE COUNSEL, AMERICAN CIVIL LIBERTIES UNION

Mr. NOJEIM. Thank you, Chairman Coble, Ranking Member Scott, Members of the Subcommittee.

It's a pleasure to testify before you today on behalf of the ACLU about certain sunsetting provisions of the USA PATRIOT Act. I will focus your attention on one of them—section 215, which deals with FISA records requests.

I'll also focus your attention on a related provision, section 505 of the PATRIOT Act that does not sunset, but that raises many of the same concerns as does section 215.

The PATRIOT Act expanded two existing sections of law that allow the FBI to compel people in businesses to produce documents and things.

Section 215 of the PATRIOT Act expanded a provision of law to authorize the FBI to more easily obtain a court order from the secret FISA Intelligence Court requiring a person or business to turn over documents or things "sought for" an investigation to protect against international terrorism or clandestine intelligence activities.

This "sought for" standard minimizes the role of the FISA Judge in controlling abuse, because it does not require any assessment of whether the records sought pertain to an agent of a foreign power or whether specific facts support a particular conclusion.

Section 505 of the PATRIOT Act expanded National Security Letter authority to allow the FBI to issue a letter compelling Internet Service Providers, financial institutions, and consumer credit reporting agencies to produce records about people who use or benefit from their services.

This power was later expanded to include records of car dealers, boat dealers, jewelers, real estate professionals, pawn brokers, and others.

In both section 215 and 505, the PATRIOT Act removed from the law the requirements that the records being produced pertain to an agent of a foreign power; that is, a foreign country, a foreign business, or a foreign terrorist organization. This significantly expanded law enforcement access to records pertaining to Americans. In these days of data mining, one cannot ignore this stark fact:

under these provisions, the Government can easily obtain records pertaining to thousands of Americans who have nothing to do with terrorism, so long as the records are "sought for" or are allegedly relevant to one of these investigations.

Neither of these statutes signals the recipient of a letter or order that the recipient can challenge it in court. Both statutes indicate that the recipient can tell no one that the recipient has received the order or letter, including an attorney with whom the person might like to consult.

In common parlance, the recipient is gagged, and under the statutory language the gag stays in place forever.

We do not ask that you repeal either of these sections of law. Rather, we ask that you restore the "agent of a foreign power" requirement and that you amend the statute to time limit the gag, exempt attorney-client communications from it, and allow for court challenges.

If these changes are made to the NSL statutes, they would satisfy the court that struck down as unconstitutional the NSL statute that applies National Security Letters to Internet Service Providers.

We also recommend that you require the Government to report publicly about the number of times it uses these powers.

Mr. Chairman, this could be one of the most productive hearings that you've conducted to date on the PATRIOT Act, and I say that because the Government has conceded that many of these changes need to be made. The Attorney General conceded that the gag to which I refer shouldn't cover attorney-client communications. Let's put it in the statute.

The Government has conceded that—the Attorney General has conceded that the statute has a relevance requirement. Let's put a standard into the statute instead of this very loose "sought for" standard.

The Attorney General has conceded that a court challenge ought to be allowed. Let's put that in the statute. The Department of Justice in its sunsets report has indicated that evidence must be presented to the judge who is evaluating an application for a section 215 order. Let's put that in the statute.

And finally, the Department of Justice has implicitly conceded that the number of times section 215 has been used can be disclosed without any damage to national security, and it did that because it has twice disclosed the number of times section 215 has been used.

Mr. Chairman, I'd be happy to discuss roving wiretaps during the question and answer period, but let me sum up by saying this: We're not asking that law enforcement tools be taken away. Rather, we're asking that they be made subject to reasonable checks and balances, such as meaningful judicial oversight and appropriate disclosure to the public of the use of the power. Congress could adopt many of the reforms that I have mentioned by enacting the Security and Freedom Ensured Act, H.R. 1526. This bipartisan legislation, co-sponsored by Representative Otter, Representative Flake, Mr. Conyers, and others, contains a series of carefully calibrated adjustments to the PATRIOT Act that would go a long way

toward bringing it more into line with the Constitution and advancing the goal of keeping America both safe and free. Thank you.

[The prepared statement of Mr. Nojeim follows:]

PREPARED STATEMENT OF GREGORY T. NOJEIM

American Civil Liberties Union
Testimony at an Oversight Hearing on sections 206 and 215
of the USA PATRIOT Act of 2001
before the Subcommittee on Crime, Terrorism and Homeland Security
of the House Judiciary Committee
Submitted by Gregory T. Nojeim,
Associate Director and Chief Legislative Counsel,
and Timothy H. Edgar, National Security Policy Counsel

April 28, 2005

Chairman Coble and Ranking Member Scott:

It is a pleasure to testify before you on behalf of the American Civil Liberties Union at this oversight hearing on two sections of the USA Patriot Act – section 215, a provision allowing the government to obtain library, bookstore and other personal records in foreign intelligence cases without individual suspicion, and section 206, the provision authorizing roving wiretaps in foreign intelligence cases.

The Patriot Act became law only 45 days after the September 11 attacks. While it acted swiftly, Congress subjected approximately a dozen provisions of the Patriot Act to a sunset date of December 31, 2005, so that it could take a second look at them.

Congress was wise to do so. Terrorism has been with us for a long time. It will likely be with us for generations to come. The decisions that you make over the coming months about the Patriot Act must be made with an eye toward that reality.

Congress should use the debate over the renewal of parts of the Patriot Act as an opportunity to reassert its rightful role in determining law enforcement and national security policy in the post-9/11 context, which has waned as the power of the Executive Branch has waxed. Before re-authorizing any power, this committee should require the Executive Branch to meet the standard articulated by the bipartisan 9-11 Commission.

- First, Congress should take care not to renew any provision unless 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."[1]

- Second, "[i]f the power is granted, there must be adequate guidelines and oversight to properly confine its use."[2]

- Finally, Congress should resist efforts by the Executive Branch to evade searching review of its existing powers, both under the Patriot Act and under other legal authorities, by

[1] Final Report of the National Commission on Terrorist Attacks Upon the United States ("The 9/11 Commission Report") 294-95 (2004) (boldfaced recommendation)
[2] *Id.*

shifting the debate to new anti-terrorism legislation, such as proposals for administrative subpoenas.

Congress may not be able to fully review or assess the effectiveness, and impact on civil liberties, of some anti-terrorism powers that the Executive Branch was granted in the Patriot Act. The lack of meaningful information about the use of many powers is sometimes a direct result of excessive secrecy in the Executive Branch, and sometimes the result of necessary secrecy. In any case where sufficient information is not available to undertake a thorough review, Congress should set a new sunset date and impose additional reporting requirements to facilitate a proper review, rather than cede those powers permanently to the Executive Branch.

Section 215: Power to Obtain Library and Bookstore Records, Medical Records, Other Personal Information and "Tangible Things" Outside a Criminal Investigation

Section 215 of the Patriot Act expanded the Foreign Intelligence Surveillance Act to authorize the FBI to more easily obtain a court order requiring a person or business to turn over documents or things "sought for" an investigation to protect against international terrorism or clandestine intelligence activities.

Section 215 is not the only newly expanded records-gathering power within the Patriot Act, although it is the only such power subject to the sunset clause. Section 505 of the Patriot Act expanded national security letter authority to allow the FBI to issue a letter compelling Internet Service Providers, financial institutions and consumer credit reporting agencies to produce records about people who use or benefit from their services. This power was later expanded to include records of car dealers, boat dealers, jewelers, real estate professionals, pawnbrokers and others. Because section 505 raises many of the same concerns as section 215 without even the requirement of a FISA court order, Congress should examine section 505 at the same time as it examines section 215.

For both section 215 records searches and national security letters, the Patriot Act removed from the law the requirement that the records being produced pertain to an "agent of a foreign power," – that is, foreign countries, businesses, and terrorist organizations. This significantly expanded law enforcement access to records pertaining to Americans. In these days of data mining, one cannot ignore this stark fact: under these provisions, the government can easily obtain records pertaining to thousands of Americans who have nothing to do with terrorism, so long as the records are sought for, or are allegedly relevant to, one of these investigations.

Both powers differ markedly from traditional criminal subpoenas. Neither of these statutes signals the recipient of a letter or order that the recipient can challenge it in court. Both statutes indicate that the recipient can tell no one that the recipient has received the order or letter, including any attorney with whom they may like to consult. In common parlance, recipient is "gagged," and under the statutory language, the gag stays in place forever.

These records search provisions are the subject of two court challenges by the ACLU. In *Muslim Community Association of Ann Arbor* v. *Ashcroft*, No. 03-72913 (E.D. Mich.), the ACLU has challenged section 215 of the Patriot Act First and Fourth Amendment grounds. As explained in

the case example (attachment A), the ACLU's challenge has uncovered serious and unconstitutional chilling effects of section 215 on the exercise of basic freedoms. The district court has not yet ruled in this case.

In *Doe* v. *Ashcroft*, 334 F. Supp. 2d 471 (S.D.N.Y. 2004), a federal district court struck down a "national security letter" records power expanded by the Patriot Act, agreeing with the ACLU that the failure to provide any explicit right for a recipient to challenge a national security letter search order violated the Fourth Amendment and that the automatic secrecy rule violated the First Amendment. The case, described in further detail in attachment B, is now on appeal before the United States Court of Appeals for the Second Circuit.

There has been some confusion about whether *Doe v. Ashcroft* struck down a provision of the Patriot Act. In fact, *Doe v. Ashcroft* struck down, in its entirety, 18 U.S.C. § 2709(b), the national security letter authority for customer records of communications service providers, as amended by section 505(a) of the Patriot Act. The court referred repeatedly to the Patriot Act in its opinion. To be clear, the court invalidated *all of section 505(a) of the Patriot Act.* It is simply inaccurate to imply that the court's decision was unrelated to the Patriot Act, or that it did not strike down a provision of the Patriot Act. If the court's decision is sustained on appeal, section 505(a) of the Patriot Act will no longer have any force or effect.[3]

Both FISA records demands and national security letters can be used to obtain sensitive records relating to the exercise of First Amendment rights. A FISA record demand could be used to obtain a list of the books or magazines someone purchases or borrows from the library. A FISA record demand could be used to obtain the membership list of a controversial political or religious organization. A national security letter could be used to monitor use of a computer at a library or Internet café under the government's theory that providing Internet access (even for free) makes an institution a "communications service provider" under the law.

While both national security letters and FISA records demands cannot be issued in an investigation of a United States citizen or lawful permanent resident if the investigation is based "solely" on First Amendment activities, this provides little protection. An investigation is rarely, if ever, based "solely" on any one factor; investigations based in large part, but not solely, on constitutionally protected speech or association are implicitly allowed. An investigation of a temporary resident can be based "solely" on First Amendment activities, and such an investigation of a foreign visitor may involve obtaining records pertaining to a United States citizen. For example, a investigation based solely on the First Amendment activities of an international student could involve a demand for the confidential records of a student political group that includes United States citizens or permanent residents.

---

[3] While the use of national security letters are secret, the press has reported a dramatic increase in the number of letters issued, and in the scope of such requests. For example, over the 2003-04 holiday period, the FBI reportedly obtained the names of over 300,000 travelers to Las Vegas, despite casinos' deep reluctance to share such confidential customer information with the government. It is not clear whether the records were obtained in part with a national security letter, with the threat of such a letter, or whether the information was instead turned over voluntarily or to comply with a subpoena.

The government defends section 215 as analogous to a grand jury subpoena in a criminal investigation, which they point out does not require probable cause and can be issued, unlike a section 215 order, without prior review by a judge. As explained above, section 215 is dramatically different from a subpoena because it provides no explicit right to challenge and contains an automatic, permanent gag order that even the Attorney General concedes should be amended to ensure it permits conversations with attorneys.

Moreover, this argument fundamentally misunderstands the difference between foreign intelligence and criminal investigations, and the impact of that difference on First Amendment freedoms. Foreign intelligence investigations are domestic investigations of the activities of foreign governments or organizations, including foreign terrorist organizations. Foreign intelligence investigations may involve investigation of criminal activities, such as espionage or terrorism, but may also involve intelligence gathering for foreign policy or other purposes involving lawful activities. The guidelines for conducting foreign intelligence investigations (including what level of suspicion is required for certain intrusive techniques) are classified.

As Justice Powell, writing for the Supreme Court in a landmark case involving intelligence gathering, observed:

> National security cases, moreover, often reflect a convergence of First and Fourth Amendment values not present in cases of 'ordinary' crime. . . History abundantly documents the tendency of Government--however benevolent and benign its motives--to view with suspicion those who most fervently dispute its policies. . . .
>
> The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power.[4]

Congress should not accept the superficial argument that every power that is available in a criminal investigation should be available to the same extent in a foreign intelligence investigation. Grand juries have extraordinary powers to compel documents and testimony for investigative purposes that would be entirely inappropriate in the hands of intelligence agents.

Moreover, as a result of section 203 of the Patriot Act, information properly obtained in a criminal investigation of terrorism (including information obtained with a grand jury subpoena) can be freely shared with intelligence agents. Section 215 is an entirely different, and more intrusive, power – a power for intelligence agents to obtain highly personal records unbounded by any need to show relevance to any criminal investigation.

The administration has also tried to allay fears about the broad scope of section 215 by selectively disclosing fragmentary information about its use. At a hearing before the Senate Judiciary Committee, Attorney General Gonzales revealed that section 215 had been used 35 times, and had not been used to obtain library or medical records. Of course, once is too often where the underlying statute is unconstitutional, as is the case with section 215. The administration defends the potential use of section 215 to obtain library or other highly personal records without any individual suspicion.

[4] *United States v. United States District Court*, 407 U.S. 297, 313-14 (1972).

The selective disclosure of information about how often section 215 has been used, and what records it has been used to obtain, calls into serious question the government's longstanding position that such information is properly kept secret. If such aggregate information can be disclosed as part of an aggressive call for Congress to renew the Patriot Act, it can be disclosed in a more balanced and systematic way.[5]

We do not ask that you repeal either section 215 or section 505 of the Patriot Act. Rather, we ask that restore the "agent of a foreign power" requirement and that you amend the statute to time limit the gag, exempt attorney-client communications from it, and allow for court challenges. If these changes are made to the NSL statute, they would satisfy the court that struck down that statute under the First and the Fourth Amendment.

The SAFE Act ("Security and Freedom Ensured Act," H.R. 1526) restores the requirement of "specific and articulable facts giving reason to believe" the records involve an "agent of a foreign power" for FISA records demands and provides a sunset date for the expanded national security letter power.[6] Restoring this requirement is needed to ensure sections 215 and 505 of the Patriot Act are not used to obtain the personal records of ordinary Americans.

The Senate version of the SAFE Act (S. 737) makes additional improvements which should be added to the House version should the SAFE Act be marked up in this subcommittee or in the full Judiciary Committee.[7] S. 737 makes explicit the right to file a motion to quash the records demands because they are unreasonable, contrary to law, or seek privileged information. The Senate bill also sets standards for a judicially-imposed, temporary secrecy order that can be challenged by the recipient of a records demand. Finally, the Senate bill provides a right to notice, and an opportunity to challenge, before information from a FISA records search or national security letter search can be used in a court proceeding.

"Roving Wiretaps" Without Sensible Privacy Safeguards

"General warrants" – blank warrants that do not describe what may be searched – were among those oppressive powers used by the British crown that led directly to the American Revolution. As a result, the framers required all warrants to "particularly describ[e] the place to be searched, and the persons or things to be seized."

The same "particularity" requirements apply to wiretap orders. In the landmark case *United States* v. *Donovan*, 429 U.S. 413 (1977), a majority upheld the federal criminal wiretap law, noting that Congress had redrafted the law to include safeguards regarding, among other things, the need to identify targets of surveillance in response to the "constitutional command of particularization."[8]

---

[5] Section 8 of S. 737, the "Security and Freedom Enhancement Act," requires that the annual number of section 215 searches be made available in a public report along with information about other FISA powers, including the annual number of physical searches, electronic surveillance orders, "lone wolf" surveillance orders, and pen/trap searches.
[6] A section-by-section chart of H.R. 1526 is appended as attachment C.
[7] A section-by-section chart of S. 737 is appended as attachment D.
[8] *Id.* at 426-27 (quoting S. Rep. No. 1097, 90th Cong., 2nd Sess., at 66 (1968), *reprinted in* U.S. Code Cong. and Admin. News 1968, at 2190).

Section 206 of the Patriot Act erodes the basic constitutional rule of particularization by creating "roving wiretaps" in foreign intelligence cases without sensible privacy safeguards. As amended by later legislation, these wiretaps do more than allow the government to get a single order that follows the target of surveillance from telephone to telephone. The government can now issue "John Doe" roving wiretaps that fail to specify a target or a telephone, and can use wiretaps without checking that the conversations they are intercepting actually involve a target of the investigation. Section 206 is subject to the Patriot Act's sunset clause.

Prior to the passage of the Patriot Act, roving wiretaps were available in criminal investigations (including criminal investigations of terrorists), but were not available in foreign intelligence investigations.

Because roving wiretaps contain more potential for abuse than traditional wiretaps, which apply to a single telephone or other device, when Congress enacted roving wiretaps for criminal investigations, it insisted on important privacy safeguards.

First, a criminal wiretap must specify either the identity of the target or the communications device being used. In other words, a surveillance order may specify only the target, or only the phone, but it must specify one or the other. Second, a criminal wiretap that jumps from phone to phone or other device may not be used unless the government "ascertains" that the target identified by the order is actually using that device.

When Congress enacted the Patriot Act, it extended "roving wiretap" authority to FISA investigations, but did not include the common sense "ascertainment" safeguard. Shortly thereafter, the newly enacted roving wiretap authority was broadened by the Intelligence Act for FY 2002, which authorized wiretaps where neither the target nor the device was specified. As a result, FISA now allows "John Doe" roving wiretaps. These are new wiretaps that can follow an unknown suspect from telephone to telephone based only on a potentially vague physical description.

The Justice Department points to the need to provide a physical description, and the need to show "probable cause" that the wiretap will intercept conversations of an agent of a foreign power, as sufficient protection for roving surveillance. Congress provided more exacting scrutiny for criminal roving wiretaps, and it should provide additional safeguards here. A roving tap, unbounded by any need to identify the target, opens the door to surveillance of anyone who fits that description, or (because of the lack of an ascertainment requirement) anyone else who might be using that telephone.

Of course, particularization is a separate constitutional demand; probable cause does not satisfy the Fourth Amendment without particularization. For that reason, the criminal roving wiretap statute includes the requirement to identify a target even though criminal wiretap orders also require criminal probable cause. FISA wiretaps, of course, require no probable cause of crime, so the need for safeguards is, if anything, greater.

In its defense of section 206 of the Patriot Act, the Justice Department takes issue with both the ascertainment requirement and the requirement to identify the target of a roving wiretap. The Justice Department's "sunsets report" implies, wrongly, that the ascertainment requirement only applies to oral interceptions (i.e., bugs) and not to wiretaps. [9] While the wording of the ascertainment requirement for wiretaps is different than the same requirement for oral interception,[10] there is no doubt that the criminal wiretap statute bans "John Doe" roving wiretaps and requires ascertainment.

18 U.S.C. § 2518(11)(b), which applies to wire and electronic communication, plainly provides that no judge may issue a roving wiretap unless, among other things:

> the application identifies the person believed to be committing the offense and whose communications are to be intercepted and . . . the order authorizing or approving the interception is limited to interception only for such time as it is reasonable to presume that the person identified in the application is or was reasonably proximate to the instrument through which such communication will be or was transmitted.

Congress should tighten the FISA roving wiretap so that it has the sensible safeguards for privacy, just as criminal roving wiretaps. Indeed, FISA roving wiretaps appear to be far more common than criminal roving wiretaps. Attorney General Gonzales reported in testimony before the House Judiciary Committee on April 6, 2005 that FISA roving wiretaps had been issued 49 times since passage of the Patriot Act. By contrast, the federal government reported only six federal criminal roving wiretaps in 2003 (the latest report available), with nine federal criminal roving wiretaps in 2002.[11]

Supporters of the Patriot Act often argue that changes to the law were needed to give the government the same powers in foreign intelligence investigations that it already had in criminal investigations. To the extent that is appropriate, it is fair to insist that the same safeguards apply as well.

Section 2 of H.R. 1526, the SAFE Act, would provide just such safeguards. While it preserves FISA roving surveillance authority, it also makes sure that these privacy safeguards, which apply to criminal roving wiretaps, would also apply to FISA roving wiretaps.

Conclusion

In short, we are not asking that law enforcement tools be taken away. Rather, that they be made subject to reasonable checks and balances – such as meaningful judicial oversight and appropriate disclosure to the public of use of the power.

Congress could easily make some of the needed reforms to sections 206 and 215, as well as other important reforms, by adopting the Security and Freedom Ensured Act, or SAFE Act, H.R. 1526.

---

[9] Department of Justice, *USA PATRIOT Act: Sunsets Report* (April 2005), at 20.
[10] *See* 18 U.S.C. § 2518(12) (ascertainment requirement for oral interception).
[11] Wiretap reports are available at the website of the Administrative Office of the U.S. Courts, at http://www.uscourts.gov/library/wiretap.html

This bipartisan legislation is co-sponsored by, among others, Representatives Otter (R-ID), Flake (R-AZ), Sanders (I-VT) and Conyers (D-MI). Its Senate counterpart, the Security and Freedom Enhancement Act, S. 737, is sponsored by Senators Craig (R-ID) and Durbin (D-IL).[12]

Adopting the SAFE Act would go a long way toward bringing it more into line with the Constitution, and advancing the goal of keeping America both safe and free.

---

[12] See attached charts explaining H.R. 1526 and S. 737.

Attachment A: Examples of the Chilling Effects of Patriot Act Section 215

In July 2003, the ACLU filed suit on behalf of six community and non-profit organizations because it had learned of a serious chilling effect that resulted from Section 215 of the Patriot Act.[13] Excerpts from some plaintiffs' declarations highlight how Section 215 chills political speech and hinder privacy rights:

The president of a community association: "The enactment of Section 215 has significantly changed the way members of [the Muslim Community Association of Ann Arbor, or MCA] participate in the organization. Many previously active members have become passive ones. Attendance at daily prayer services, educational forums, and social events has dropped. Some members have totally withdrawn their membership from MCA. Charitable donations to MCA have decreased."[14]

A prominent member of the association: "Although I had been very outspoken politically before passage of the Patriot Act, I became afraid after the Patriot Act was passed that if I continued to remain a vocal and visible Muslim, the government would target me for investigation and seek private records about me even thought I had not done anything wrong.

"While I was upset by several policies of the U.S. and would have ordinarily taken a leadership role in protesting these policies, I decided to step out of the limelight to lessen the chances that the government would target me for an investigation under the Patriot Act."[15]

The administrator of a Christian refugee aid organization: "Section 215 has harmed our ability to serve our clients in a number of different ways.

"Section 215 has caused Bridge to redirect resources from client assistance. Resources that we otherwise would have used to help clients are instead being used to re-evaluate our record-keeping and record retention policies.

"Because we would not have an opportunity to challenge a Section 215 order before complying with it, we have had no choice but to act now to ensure that our records do not contain personal or other sensitive information that we could be forced to disclose to the government. Accordingly, my staff and I have been deciding on a case-by-case basis to exclude some sensitive information from our files.

"While we believe that we have no practical choice but to adopt this policy, there is no question that the practice compromises the level of services we can provide to our clients."[16]

---

[13] *Muslim Community Association of Ann Arbor v. Ashcroft*, Civil Action No. 03-72913 (E.D. Mich., filed July 30, 2003).
[14] Nazih Hassan Decl. ¶ 22.
[15] John Doe (Member of MCA) Decl. ¶¶ 8-9.
[16] Mary Lieberman Decl. ¶¶ 23-27.

Attachment B: Example of Patriot Act Abuse

Unconstitutional National Security Letters

Section 505 of the Patriot Act expanded the government's authority to use National Security Letters (NSL's) to seize information from businesses and others, with no judicial approval. Prior to the Patriot Act, the government could use NSL's to obtain records about alleged terrorists or spies – people who were thought to be "foreign powers" or their agents. Financial, travel and certain Internet Service Provider (ISP) records are accessible under the NSL authority. Section 505 changed the law to allow the use of NSL's to obtain such records about anyone without the limitation that they be agents of foreign powers. In the Intelligence Authorization Act of 2004[17] Congress further expanded the NSL letter authority to permit seizure of casino and other records.

On a date that the government maintains must be kept secret for reasons of national security, the FBI served an NSL on an ISP the identity of which the government also claims must be kept secret for reasons of national security. Through its NSL authority at 18 U.S.C. Section 2709, the government can seek certain sensitive customer records from ISPs – including information that may be protected by the First Amendment – but the ISP can never reveal that it has been served with an NSL, and nothing in the statute suggests that the NSL can be challenged in court. On behalf of the ISP and itself, the ACLU challenged the statute as amended by the Patriot Act, as a violation of the First and Fourth Amendments because it does not impose adequate safeguards on the FBI's authority to force disclosure of sensitive and constitutionally protected information and because its gag provision prohibits anyone who receives an NSL from disclosing in perpetuity and to any person even the mere fact that the FBI has sought information.

On September 28, 2004, Judge Victor Marrero of the Southern District of New York issued a landmark decision striking down as unconstitutional the NSL statute and its gag provision. The court struck down the entire statute as violative of Fourth and First Amendment rights, thus rendering any use of the statute an abuse of those rights. The court found that there have been hundreds of such uses.[18] It found that the statute was abusive in practice because it sanctioned NSL's that coerced immediate compliance without effective access to court review or an opportunity to consult with counsel:

> The form language of the NSL served upon [plaintiff ISP] Doe, preceded by an FBI phone call, directed him to personally provide the information to the FBI, prohibited him, his officers, agents and employees from disclosing the existence of the NSL to anyone, and made no mention of the availability of judicial review to quash or otherwise modify the NSL or the secrecy mandated by the letter. Nor did the FBI inform Doe personally that such judicial review of the issuance of the NSL or the secrecy attaching to it was

[17] Pub. L. No. 108-177, Section 374 (Dec. 13, 2003).

[18] *Doe v. Ashcroft*, (04 Civ. 2614, S.D.N.Y. Sept. 28, 2004), at 63-64. The court concluded that hundreds of NSL's had been requested by the FBI from October, 2001 through January, 2003, and hundreds must have been issued during the life of the statute. The government takes the position that even the number of NSL's it issues cannot be disclosed for reasons of national security, though it has disclosed publicly to Congress a number of such uses. *See, e.g.* "H.R. 3179, The 'Anti-Terrorism Intelligence Tools Improvement Act of 2003," Hearings Before the Subcomm. on Crime, Terrorism, and Homeland Security of the House Comm. on the Judiciary, 108th Cong. (2004) (statement of Thomas J. Harrington, Deputy Assistant Director of the FBI Counterterrorism Division).

> available. The court concludes that, when combined, these provisions and practices essentially force the reasonable NSL recipient to immediately comply with the request.[19]

In finding the statute unconstitutional under the *Fourth* Amendment, Judge Marrero referred repeatedly to the amendments made by Section 505. He noted as an example of the kind of abuse now authorized by the statute that it could be used to issue a NSL to obtain the name of a person who has posted a blog critical of the government, or to obtain a list of the people who have e-mail accounts with a given political organization.[20] The government could not have obtained this information with an NSL prior to the Patriot Act amendment in Section 505, unless the blogger or the people with such accounts were thought to be foreign powers or agents of foreign powers. The court also cited Patriot Act Section 505 as a reason it struck down the statute on *First* Amendment grounds. The court determined that the tie to foreign powers – eliminated by Section 505 – "limits the potential abuse" of the statute[21] and distinguishes it from other intelligence search provisions that retain the requirement of such a tie and include a statutory gag provision.

Because of the gag in 18 U.S.C. Section 2709(c), the government obtained a sealing order it has consistently used to suppress wholly innocuous information in the litigation. Until the court struck down the statute, the government prevented the ACLU from disclosing that it represented someone that had been served with an NSL, and from even acknowledging that the government had used a statutory power. The government has demanded that the ACLU redact a sentence that described its anonymous client's business as "provid[ing] clients with the ability to access the Internet." Ironically, the government even insisted that the ACLU black out a direct quote from a Supreme Court case in an ACLU brief: "The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect 'domestic security.' Given the difficulty of defining the domestic security interest, the danger of abuse in acting to protect that interest becomes apparent."

The gag in Section 2709 would effectively prevent an ISP (or its lawyers) from disclosing other abuses of Section 2709. For example, if the government was targeting someone because of their First Amendment activity, or if the ISP was being forced to turn over First Amendment protected information about associational activities, the gag would bar disclosure of this abuse.

---

[19] *Id.* at pp. 44-45.
[20] *Id.* at p. 75.
[21] *Id.* at p. 93.

Attachment C: Section-by-Section of H.R. 1526: Security and Freedom Ensured (SAFE) Act
Providing Checks and Balances for Patriot Act Surveillance Powers

surveillance power	*before Patriot Act*	*now*	*SAFE Act safeguard*
Roving wiretaps under the Foreign Intelligence Surveillance Act (FISA).		✓	✓
	No roving wiretaps under FISA, but were available for criminal investigations (including for terrorism). Criminal roving taps require that target of search is specified and agents "ascertain" that target is using the facility.	Now there are FISA roving wiretaps, but unlike criminal roving wiretaps, FISA roving wiretaps do not need to specify target and agents need not ascertain target is using that telephone. **PATRIOT § 206; Intelligence Act for FY2002 § 314.**	Would keep FISA roving wiretaps, but they would have to observe same requirements as criminal roving wiretaps, i.e., they must (1) specify a target, and (2) would have to ascertain target is using that facility. **SAFE § 2**
"Sneak and peek" – criminal search warrants with delayed notice.	✓	✓	✓
	Some courts had approved in specific circumstances, despite lack of statutory authority. Two circuit courts of appeals imposed presumptive seven-day limit on delaying notice.	Now there is statutory authority for sneak and peek searches under wide-ranging circumstances, including whenever notice could "seriously jeopardize" a prosecution or delay a trial. No time limit for delaying notice **PATRIOT § 213**	Would limit statutory reasons for delaying notice to four specific harms – danger to persons, flight from prosecution, intimidation of a witness, or destruction of evidence – and imposes a seven-day limit, which court can renew for periods of (21 days?) **SAFE § 3**
Library and other personal records searches under FISA.		✓	✓
	FISA search orders were available only for certain travel-related "business" records (not library or personal records) where FBI has "specific and articulable facts" connecting records to foreign agent.	Now these orders are available for any and all records, including library records, without individual suspicion. **PATRIOT § 215**	Would still be available for any and all records – including library records – but only where FBI has "specific and articulable facts" connecting records to foreign agent. **SAFE § 4**

surveillance power	*before 9/11*	*now*	*after SAFE*
National security letters (no court order required) for financial records, telephone and ISP records, consumer credit reports.	✓	✓	✓
	Were available only where FBI could show "specific and articulable facts" connecting records to foreign agent.	Now available without individual suspicion; definition of "financial records" greatly expanded. **PATRIOT § 505; Intelligence Act for FY2004 § 334.**	Would still be available without individual suspicion, but libraries with Internet terminals would not be subject to national security letters. **SAFE § 5**
Definition of "Domestic Terrorism"		✓	✓
	none	any state or federal criminal act involving "acts dangerous to human life" and intending to influence government or civilian population **PATRIOT § 802**	any act involving a listed federal crime of terrorism intending to influence government or civilian population **SAFE § 6**
Sunset clause.	not applicable	Now applies to 14 provisions (out of 158 total). **PATRIOT § 224**	Would be expanded to include four additional provisions, for a total of 18 (out of 158 total). **SAFE § 7**

Attachment D: Section-by-Section of S. 737: Security and Freedom Enhancement (SAFE) Act
Providing Checks and Balances for Patriot Act Surveillance Powers

	Surveillance power	*Before Patriot Act*	*Now*	*Sun-sets?*	*SAFE Act safeguard*
1	Short title.				
2	Foreign intelligence (FISA) roving wiretaps. **-Patriot Act § 206 -Intelligence Act for FY2002 § 314.**	No roving wiretaps under FISA, but were available for criminal investigations, including criminal terrorism investigations.	FISA roving wiretaps allowed in all intelligence investigations, but unlike criminal roving wiretaps, FISA roving wiretaps do not need to specify target and agents need not ascertain target is using that telephone.	Yes	The SAFE Act would retain roving wiretaps in FISA investigations, but would require FISA roving wiretaps to observe same requirements as criminal roving wiretaps, i.e., they must (1) specify a target, and (2) would have to ascertain target is using that facility.
3	"Sneak and peek" searches -- criminal search warrants with delayed notification. **-Patriot Act § 213**	Some courts had approved in specific circumstances, despite lack of statutory authority. Two circuit courts of appeals imposed presumptive seven-day limit on delaying notice.	Patriot Act provides statutory authority for sneak and peek searches under wide-ranging circumstances, including whenever notice could "seriously jeopardize" a prosecution. No time limit for delaying notice.	No	The SAFE Act would limit statutory reasons for delaying notice to specific harms – danger to persons, flight from prosecution, destruction of evidence, or intimidation of witnesses – and imposes a seven-day limit, which court can renew for additional periods of 21 days.
4	FISA records search orders **-Patriot Act § 215**	FISA search orders were available only for certain travel-related "business" records on basis of individualized suspicion connecting records to foreign agent.	Now these orders are available for any and all "tangible things," including library records, medical records, and other highly personal records, without individual suspicion.	Yes	The SAFE Act allows orders for all "tangible things," including library records. It limits all orders to where the FBI has "specific and articulable facts" connecting records to foreign agent. In addition, it provides a right to challenge the order, limits on the secrecy order and a right to challenge that order, and notice and an opportunity to challenge the use of such information in court.

5	National security letters (no court order required) for financial records, telephone and ISP bills, consumer credit reports. **-Patriot Act § 505 -Intelligence Act for FY2004 § 334**	Were available only where FBI could show "specific and articulable facts" connecting records to foreign agent.	Now available without individual suspicion; definition of "financial records" greatly expanded.	No	The SAFE Act retains the broader definition of "financing records." It restores the requirement of individual suspicion, provides a right to challenge records demands, limits the secrecy order and provides for a right to challenge the secrecy order, and providing notice to persons when the government seeks to use information from such demands against them in court.
6	Surveillance of the Internet, other communications without probable cause using pen/trap authority. **-Patriot Act §§ 214 (criminal) and 216 (FISA)**	Unclear whether pen/trap authority applied to the Internet; FISA pen/traps available only for facilities used by agents of foreign power or those involved in international terrorism activities.	Pen/trap authority extended to Internet communications; FISA pen/traps can be used at more facilities, including for U.S. persons, and regardless of what facility is being monitored.	Yes-(214) No-(216)	The SAFE Act would require that the determination of relevance for pen/trap orders (both FISA and criminal) be based on a statement of "specific and articulable facts," not on mere certification. It requires more detailed reporting for criminal pen/trap devices (including reporting on what information is obtained) and notice when surveillance is terminated. **-SAFE Act § 6**
7	Definition of domestic terrorism, triggers other surveillance powers. **--Patriot Act § 802**	Definition of international terrorism only.	Domestic terrorism is <u>any</u> state or federal criminal act primarily within US involving "acts dangerous to human life" and that "appears to be intended" to influence government or civilian population.	No	The SAFE Act limits the definition to criminal acts involving a specific list of serious federal crimes of terrorism that are actually intended to influence government or civilian population.
8	Public reporting on FISA surveillance.	Only reporting is the yearly number of applications and number of orders granted.	Public reporting is unchanged. FISA was expanded by Patriot Act and is now used far more often. Section 6001 of the Intelligence Reform Act added new reporting requirements for Congress.	N/a	The SAFE Act expands sunshine by making public reporting under the 2004 intelligence reform act, which (1) breaks total number of FISA orders down into types of surveillance (wiretaps, physical searches, pen/trap, records searches, lone wolf) and (2) makes available unclassified versions of significant legal pleadings and opinions of the FISA court.

Mr. COBLE. Thank you, Mr. Nojeim. We have been joined by the distinguished gentleman from Florida, Mr. Feeney, and the distinguished gentleman from Texas, Mr. Gohmert. But don't start me yet.

Gentlemen, we apply the 5-minute rule to ourselves, as well. So if you all could keep your responses as terse as possible and yet address the point, that would enable us to move along.

Now, what I'm about to say has nothing to do with 206 or 216. Mr.—I want to advise the Members of the Subcommittee and those in the hearing room that effective today, Mr. Bobby Vassar, who is the counsel to Mr. Scott, has become a granddaddy, a grandfather. And I told him earlier, I said, Bobby you look too young to be a grandfather, but congratulations to you, Bobby.

Mr. VASSAR. Thank you, Mr. Chairman.

Mr. COBLE. And incidentally, I had received Mr. Scott's permission before I did that, Bobby.

He said you would not approve.

Mr. Baker, what type of library records are covered under 215 and how do these records assist or help in terrorism investigation, A; and B—and I think you touched on this—if we exempt library and book records from a 215 order, does that create a sanctuary for terrorists?

Mr. BAKER. Well, as I think you mentioned in your opening remarks, Mr. Chairman, the section 215 of the PATRIOT Act, does not discuss any particular holder of records at all. It doesn't mention libraries at all. It doesn't mention anyone else. And that's why it's an important provision. It allows the Government to go after what it needs with respect to each investigation. But it does not single out libraries or bookstores or anything else. That's point number one.

Point number two is the effect would be it would create—it would put everybody on notice, if you exempted libraries or booksellers somehow, it would put people on notice that there was a, you know, a Government free zone where investigations could not go, and conduct could be conducted there, including, for example, use of computers or, you know, checking out other types of materials that might in some instances, as it has in the past and actual investigations provided important information for investigators. So we don't support that singling out or creating a sanctuary for any type of documents at all.

Mr. COBLE. I thank you, sir. Mr. Wainstein, some have suggested that since 215 has not been used to obtain library records, it's not needed, although I think maybe Mr. Baker probably will answer this as well. A recent commentary indicated that the 9/11 hijackers used libraries in the United States in the period leading up to September 11. Do you know whether or not, in fact, this is true?

Mr. WAINSTEIN. Yes. Some 9/11 hijackers did use libraries in the United States. Investigators have received information that individuals believed that 9/11 hijackers Wail Alshehri, Waleed Alshehri, and Marwan Al-Shehhi visited the Del Ray Beach Public Library in Del Ray Beach, Florida.

Wail Alshehri and Waleed Alshehri entered the library one afternoon in July of 2001, and asked to use the library's computers to access the Internet. After about an hour a third man, Marwan Al-

Shehhi, joined the two. Waleed and Wail Alshehri were hijackers aboard American Airlines Flight 11, while Al-Shehhi was the pilot who took control of United Airlines Flight 175, both of those flights crashed into the World Trade Center on September 11th.

A witness, who recognized photos of the three individuals that ran the newspaper articles after September 11th, provided the information about the Del Ray Beach library visit. While no records exist to confirm the hijackers' visit to the Del Ray Beach Library, the timing, location, and behavior described by the witness are consistent with other information gathered in the course of the investigation.

In addition, investigators tracing the activities of the hijackers determined that on four occasions in August of 2001, individuals using Internet accounts registered to Nawaf Alhazmi and Khalid Almihdhar, 9/11 hijackers, used public access computers in the library of a State college in New Jersey. The computers in the library were used to review and order airline tickets on an Internet travel reservations site. Alhazmi and Almihdhar were hijackers aboard American Airlines Flight 77, which took off from Dulles Airport and crashed into the Pentagon. The last documented visit to the library occurred on August 30, 2001. On that occasion, records indicate that a person using Alhazmi's account used the library's computer to review September 11th reservations that had been previously booked.

Mr. NOJEIM. Mr. Chairman, may I respond to that? May I respond to that?

Mr. COBLE. Well, I'll get to you in just a minute, Mr. Nojeim. I want to ask Mr. Khuzami a question. We're going to probably have a second round here as well. Comparing the process for obtaining records through a grand jury subpoena, Mr. Khuzami, with the process for obtaining records through section 215, which process in your opinion contains more safeguards to ensure the privacy of Americans?

Mr. KHUZAMI. Mr. Chairman, I believe that section 215 does for a host of reasons.

First, it has a much narrower scope. It only applies in foreign intelligence investigations or investigations designed to protect against international terrorism or espionage activities.

Whereas, in the grand jury process, you can investigate anything in the entire Federal criminal code, as well as terrorism and espionage cases. So the scope is much narrower in section 215.

Two, you cannot use section 215 authority to investigate a U.S. person based solely on their first amendment activities. There is no such similar restriction in the grand jury process.

Third, and most importantly, there is judicial review of the section 215 order before it is issued. Agents can't just go out and grab your records. They have to present an application to the court and the court has to review it. It is an independent check on law enforcement that does not exist in the grand jury process.

Next, there's congressional oversight, as you well know, for section 215 orders and the Department of Justice has to report on its use of that provision.

And lastly, the Inspector General has to report on abuses in general under the PATRIOT Act. Neither of those two oversight functions exist in the grand jury process.

Mr. COBLE. Well, my time has expired. The gentleman from Virginia, Mr. Scott.

Mr. SCOTT. Thank you, Mr. Chairman. Let me follow through on that. On the grand jury you're actually investigating a crime; is that right?

Mr. KHUZAMI. That's correct.

Mr. SCOTT. And in 215, you can be investigating—you said terrorism. But you can also be investigating—is 215 limited to terrorism or crimes?

Mr. KHUZAMI. No, it can be used to collect foreign intelligence information or to investigate espionage.

Mr. SCOTT. Whoa. Whoa. Whoa. Wait a minute. What is foreign intelligence information mean?

Mr. KHUZAMI. That is information designed to determine if there are foreign intelligence agents collecting information or acting within the United States who may pose a threat.

Mr. SCOTT. A threat? Does it have to be a threat?

Mr. KHUZAMI. Does it have to be a threat?

Mr. SCOTT. Right.

Mr. KHUZAMI. No, it doesn't have to be a threat. But you have to be very careful to make sure that you are collecting this information so that you can prevent an attack rather than prosecuting it after it happens. And that's the critical difference in 215.

Mr. SCOTT. How about getting information on trade deal negotiations in helping you conduct foreign affairs?

Mr. KHUZAMI. I'm not aware that it's ever been used for that purpose.

Mr. SCOTT. I didn't ask you—it says the code—does the code say conduct of foreign affairs, Mr. Baker. Is that what it says?

Mr. BAKER. Yes, sir. It does.

Mr. SCOTT. Okay. Well, conduct of foreign affairs—a trade deal. Where is the threat if we don't get their low price on steel?

Mr. KHUZAMI. I'm not aware that there is a threat for those purposes?

Mr. SCOTT. Okay. But you can get 215 information if it's helping you conduct your foreign affairs; is that right?

Mr. KHUZAMI. I'm not aware that it has ever been used for that purpose.

Mr. SCOTT. Well, do you want to—can we strike it—well, how would you like us to limit this to just crimes and terrorism so we don't have to ask these questions every time we have a hearing about you getting a roving wiretap for things that have nothing to do with criminal activity or any national security of the American public?

Mr. BAKER. May I respond to that, Congressman?

Mr. SCOTT. Sure.

Mr. BAKER. We discussed this briefly the other day, and I mean one of the purposes of FISA is to provide the President of the United States with timely and accurate information about the capabilities, plans, and intentions of foreign powers and their agents across the board. And the President of the United States has broad

responsibilities to protect the national security, but also to conduct the foreign affairs of the United States.

So as in my prior dealings with the Congressman, he always challenges me, and I always have to go do my homework to make sure I know exactly what we're talking about here. So after we discussed this the other day, I went off and looked up the legislative history on this particular point, and I believe it provides some comfort in this area, because it says that the provision we're talking about here requires that the information sought involves information with respect to foreign powers or territories and would, therefore, not include information solely about the views or planned statements or activities of Members of Congress, Executive Branch officials, or private citizens concerning the foreign affairs or national defense of the United States.

Mr. SCOTT. If you have the agent of a foreign government that you're discussing a trade deal with, can you get a 215 information and can you get the roving wiretap?

Mr. BAKER. In?

Mr. SCOTT. And that's all the probable cause you got. The probable cause he's a foreign agent, and the probable cause he's going to talk about with his people back home what the low price on steel is. Can you get a roving wiretap?

Mr. BAKER. Under the statute, the answer is yes.

Mr. SCOTT. Okay.

Mr. BAKER. But there's a limitation in that the information sought must be with respect to foreign powers or their territories, so it's different. It's not information about that U.S. person. It's information about what the foreign power.

Mr. SCOTT. Okay. Well, let's talk about this U.S. person where you say you can't get it solely for protected first amendment activities.

Mr. BAKER. Yes. That's correct.

Mr. SCOTT. And that solely invites a question. Suppose it's mostly for first amendment activities? A war protester?

Mr. BAKER. I am quite confident that my office, the Attorney General, and the FISA Court would be very concerned about any requests to conduct a FISA that was not done for a proper purpose; that was done apparently for a purpose to collect information about somebody who was merely protesting against the Government. There's——

Mr. SCOTT. What does "solely" mean?

Mr. BAKER. Solely means, in my mind, solely—the only reason.

Mr. SCOTT. And if it's mostly because of war protesting, but you got a little smidgeon of something else, it would be okay to get the information?

Mr. BAKER. In theory, that's what the language says. But——

Mr. SCOTT. Well, I mean in theory. I'm talking about the English language. Is that what the words say?

Mr. BAKER. Yes, it does.

Mr. SCOTT. Okay.

Mr. BAKER. But, as I said, there are mechanisms in place and individuals in place to enforce the law, and it seems to me that the rule of law does not depend merely on writing down laws on paper. You have to have people——

Mr. SCOTT. What information do you present to the court to get a 215, to get 215 information?

Mr. BAKER. We would present to the court information—because of the restriction that it can't be based solely on first amendment activities. We would provide to the court in that situation and the pen register situation, where you have similar restriction, information to assure the court, as well as our office, that it is not based solely on protected first amendment activities, and we would also explain to the court why it's relevant to the investigation.

Mr. SCOTT. Are we coming back? Okay.

Mr. COBLE. The gentleman's time has expired. In order of appearance, the gentleman from Arizona, Mr. Flake. You're recognized for 5 minutes.

Mr. FLAKE. Thank you, Mr. Chairman. I thank the witnesses. Let me just follow up. Have any—with Mr. Wainstein, if you could. Have any 215 applications been denied by a judge? By a FISA Court?

Mr. WAINSTEIN. I think actually the best person to speak to that would be Jim Baker because he actually appears before the FISA Court.

Mr. BAKER. The answer is no.

Mr. FLAKE. No?

Mr. BAKER. The answer is no.

Mr. FLAKE. Under what scenario could you see one actually being denied, given that the language actually says the judge shall issue the order.

Mr. BAKER. In my experience, I mean if the court was not obviously what we were just discussing with Mr. Scott. If the court was not satisfied that there was a legitimate basis for this investigation, a legitimate foreign intelligence or protective basis, then it would deny it, and should deny it, if we filed such an application.

Mr. FLAKE. But it says—the words used there are "shall." Do you see a problem with that, and do you think that we in Congress ought to be concerned that we would have to rely, as you put it on individuals and their discretion at the Department of Justice or prosecutors?

Mr. BAKER. Well, it's not just the Department of Justice, it's the court. It's Federal district court judges sitting especially designated as FISA Court judges, but who are appointed for life——

Mr. FLAKE. But who are told by statute shall issue an order. Shall instead of should, might, use your discretion. Rather, it says shall.

Mr. BAKER. In my dealings as a lawyer, I have never met a judge who's just going to look at a blank request from the Government and not assure himself or herself that it's consistent with the law and ask commonsensical questions about what it is the Government is trying to do, especially in FISA and especially with the history that we have with respect to how national security authorities have been misused in the past. We're all very cognizant of that, and we all work very hard to make sure that doesn't happen again.

Mr. FLAKE. But shouldn't we—I mean you're then saying that you're confident that a judge would ignore the statute that says he shall issue it, and actually defy it?

Mr. BAKER. Well, shall—I mean let me just be clear. The word shall is not just found in 215 and in no other creature of Federal law. It is found in other provisions as well, and when the Government meets the statutory requirements of that statute or other statues, it directs the court to issue the order.

Now, having said that, my experience again with Federal judges is that they look hard at any requests from the Government to do anything, especially intrusive activities. And the court is going to look at that. That's why Congress put Federal judges into this process when they enacted FISA.

Mr. FLAKE. Mr. Nojeim, would you comment on that?

Mr. NOJEIM. What the statute says is that when the Government applies for 215 order, it must specify that the records that it seeks are sought for an authorized investigation. Once it makes that specification, the statute requires that the judge issue the order giving them access to those records. The debate ought to be about what the Government should have to prove to the FISA Court, not—and that you shouldn't allow the statute to stay in its current condition that allows the Government to get these records merely when it makes the specification. Remember what's happening here. There's one party in front of the judge. And that one party need only specify. That's it.

Mr. FLAKE. Moving on just a bit. In testimony the other day at a hearing, it seemed as if—and I want to get your opinion on this—that an individual who is not the target of probe, who is on the periphery somehow could have information on a Internet server, for example, that he could be surveilled for a long period of time without knowledge that he was under surveillance; that the notice simply has to go to the Internet provider or the server and not the individual. Is that accurate, Mr. Nojeim, first?

Mr. NOJEIM. Say it again? That the notice?

Mr. FLAKE. That notice that surveillance is being conducted need not ever go to the individual?

Mr. NOJEIM. Oh, no. No. The individual who is being surveilled?

Mr. FLAKE. Yes.

Mr. NOJEIM. Never knows.

Mr. FLAKE. Never knows?

Mr. NOJEIM. Right.

Mr. FLAKE. And that could happen for a long period of time, over a couple of years, and under the current law, they need not be ever notified that they are under surveillance?

Mr. NOJEIM. That's right. They would never be notified.

Mr. FLAKE. Okay.

Mr. NOJEIM. And if I could just follow up on part of the discussion earlier? This notion about exempting libraries from the coverage of section 215.

Mr. FLAKE. I was going to get to that.

Mr. NOJEIM. We have to remember that 215 and National Security Letters also apply to Internet Service Providers. The Government says that the library is an Internet Service Provider. But it can use its Internet Service Provider authority to get those records without having to go through section 215. In other words, if you exempted libraries from section 215, the FBI could still serve a National Security Letter on the Internet Service Pprovider that is

serving the library and get those records using that authority, and it wouldn't even matter that the library had been exempted from section 215.

Mr. FLAKE. But you have not—just to clarify—you or your organization has not asked for an exemption for libraries? You simply asked for a more rigorous standard that's applied before appearing before a judge?

Mr. NOJEIM. That's right.

Mr. COBLE. The gentleman's time has expired. And, as I said, we'll have a second round. The distinguished gentleman from Michigan, Mr. Conyers.

Mr. CONYERS. Thank you, Mr. Chairman. I appreciate the witnesses' testimony.

How many convictions based on terrorist activity have we had in the United States since 9/11? I'll start with Mr. Wainstein?

Mr. WAINSTEIN. Yes, sir. Thank you. I don't have——

Mr. CONYERS. I understand.

Mr. WAINSTEIN.—off the tip of my tongue an exact number, but I have actually—I know this question has come up, so I had a listing of various——

Mr. CONYERS. Sure. What number?

Mr. WAINSTEIN. I came up with about a dozen or so.

Mr. CONYERS. Okay. I'd like to see you afterward to find out how your list compares to mine.

Mr. WAINSTEIN. And keep in mind, that's not a total list.

Mr. CONYERS. No. It's not.

Mr. WAINSTEIN. It's just the cases that occurred to me as being terrorism cases that I——

Mr. CONYERS. Well, I'm in the process of trying to find this out. This is probably the most elemental question that we could be talking about.

I asked you this already once, Mr. Baker, didn't I?

Mr. BAKER. Yes, sir, last time.

Mr. CONYERS. What number do you have?

Mr. BAKER. I don't—I didn't count.

Mr. CONYERS. You didn't count.

Mr. BAKER. I was just able to come up with—you asked—I think if we—if there had been any convictions, and I think——

Mr. CONYERS. All right.

Mr. BAKER.—the answer was yes. But I believe that the Department, the Criminal Division, of the Department, would be the most likely place to have that kind of information.

Mr. CONYERS. Thank you. Mr. Khuzami, what number do you have?

Mr. KHUZAMI. I'll defer to my Department of Justice colleagues.

Mr. CONYERS. Okay.

Mr. KHUZAMI. I do not have a number.

Mr. CONYERS. All right. Director Nojeim, how many do you have?

Mr. NOJEIM. I'd be happy to get back to you, Congressman.

Mr. CONYERS. Okay. All right.

Mr. NOJEIM. But let me just point out that it's important that when we're reporting numbers of convictions that we actually look at what the person was convicted of.

Mr. CONYERS. Well, exactly.

Mr. NOJEIM. Often the Department says that somebody was convicted of terrorism in connection with a terrorism investigation, when really the conviction is about a very minor crime.

Mr. CONYERS. Precisely. Well, I want to tell everybody and put it on the record that I've got four that I would be willing to—that's a number I would stand behind. But somewhere in our Government, and I'll take your suggestion, Mr. Baker, to check with who you referred us to.

Now, let me ask if there's any witness here that has any objection—well, I don't—I guess I know the answer to this question already. All of the witnesses except one wants to make section 206 permanent; is that right? Right?

Mr. BAKER. Yes.

Mr. WAINSTEIN. Yes, sir.

Mr. CONYERS. Okay. Then I have to ask Mr. Nojeim what's the case for more safeguards and what would they be and why shouldn't we have, and why should we discontinue the use of simultaneously both John Doe wiretaps and roving wiretaps?

Mr. NOJEIM. We're not asking that you repeal section 206, the roving wiretap provision of the PATRIOT Act. What we ask is that you conform it to the corresponding provision in the criminal code. Doing this would entail requiring that the Government specify in its application for a wiretap either the identity of the person who's phone or computer would be tapped or to specify the facility that would be tapped.

It would also entail borrowing from the criminal code the ascertainment requirement that helps focus law enforcement eavesdropping on conversations to which the target is really a party. Doing these two things would conform the intelligence roving wiretaps to the criminal roving wiretaps and would go a long way toward protecting the privacy of Americans engaging in innocent telephone conversations.

Mr. CONYERS. Finally, we've been trying to get information about these numbers. The only time we get cooperation from the Government, namely DOJ and the FISA people, is when there's an expiration of a provision, and then we get some numbers. Other than that we get stiffed for—what is it—three years we've been trying to engage in a discussion, and it was off the charts, and I just want to put on the record that this amounts to me to misclassification, because there's been no accounting for the wiretaps, the National Security Letters, and then all of a sudden when seeking reauthorization, we can get the numbers.

And I think, Mr. Chairman, that's an abuse of power on the part of the Executive Branch that handles this kind of activity. Does anybody want to defend the Government on that score? Mr. Baker?

Mr. BAKER. Yes, sir. I'd be happy to. On a regular, on semi-annual basis, we provide to the intelligence committees of both Houses of Congress a very lengthy report full of all the numbers you could want quite frankly. It's a very, very long report, with a lot of data in it that is available at the committees', the intelligence committees, and, as I understand it, Members of Congress and cleared staff can have access to that. So we provide those numbers. We also provide less highly classified reports, with admittedly less

information in them to, I think, both the Judiciary and Intelligence Committees of both Houses of Congress.

Mr. CONYERS. Well, all somebody had to do was put it in a letter to us saying go see the right agency. We're loaded with. You got more information than you could ever use, but we get stiffed.

Now, I'll take it up with the staff and the Subcommittee as well but I'm glad you're telling us that it's really available if we can get cleared.

Mr. BAKER. And I come up regularly. I was up I think last week in front of the House Intelligence Committee to come up and do staff briefings and explain the numbers and provide additional details. So I'm happy to do that at any point in time.

Mr. NOJEIM. Mr. Conyers? Mr. Conyers, the Department reports every year the number of full FISA wiretaps and physical searches that it does. And it does that without any risk to national security. It could—and those are much more intrusive searches than our—than the searches under section 215 and than our National Security Letter requests as well.

This is what we got when we filed a Federal Freedom of Information Act request for information about the use of National Security Letters. It is page after page after page of blanked out information that seems to suggest that National Security Letters are being used, but that you can't really tell that they are or how often they are being used.

We would suggest that more reporting could be done on National Security Letters.

And I'd like to submit this for the record, and the letters that the Attorney General—I'm sorry that the Department of Justice—has provided over the last 2 years about even more intrusive surveillance.

Mr. COBLE. Without objection.

The gentleman's time has expired.

Mr. CONYERS. Thank you.

Mr. COBLE. The gentleman—the distinguished gentleman from Texas, Mr. Gohmert.

Mr. GOHMERT. Thank you, Mr. Chairman, and once again I appreciate the opportunity for these hearings. It's very helpful.

I was a little surprised, and I want to be sure about this, but did I understand that you know the U.S. Attorney' office knows or intelligence knows that the hijackers actually did use the library of the State college in New Jersey to make airline reservations for flight 77? Did I understand that correctly?

Mr. WAINSTEIN. Sir, the—what I stated earlier is that two of the hijackers used computers at that New Jersey library. They did review and order airline tickets. The airline tickets they ordered were not the airline tickets for the flight on September 11th. Those were ordered on some other computer somewhere else. They did review their reservations——

Mr. GOHMERT. I see.

Mr. WAINSTEIN. The September 11 reservations on that computer in that library on August 30 of 2001, 11 days before the attacks.

Mr. GOHMERT. There had been discussion about the gag order. Would it be appropriate to have at least a one-sided gag order where the Government does not reveal, but if the individual target

wishes to reveal that he or she could do so? I'm interested in each of your responses?

Mr. BAKER. Well, I believe what the Department has supported in general is an amendment to the section 215 that would allow the recipient of the order, which remember is most likely a third party. We're unlikely to serve a 215 order on the target of the investigation, but that—we would serve it on a third party and that third party then could consult with their attorney to discuss whatever legal action they want to take or compliance of whatever other matters they want to discuss.

So we would support some kind of an amendment to address what's been referred to as a gag order in that regard.

Mr. GOHMERT. So that would basically be a one-sided gag order, where the Government would not reveal, but the recipient could; is that correct?

Mr. BAKER. The recipient could reveal to his or her attorney or to the company's attorney, whatever it is. They could have a meaningful discussion with their attorney to get legal advice on this issue.

Mr. GOHMERT. So it is currently the law you're telling me that somebody gets this order. They can not even talk with an attorney about it?

Mr. BAKER. On its face, that's what it says. The Department has already taken the position that they could talk to their lawyers with respect to this—with respect to receiving one of these items, but that is what the law says. And that's why we would support clarifying that specifically.

Mr. GOHMERT. But your position is only that it be extended to consultation with an attorney or someone of that nature, not that they could go public with it?

Mr. BAKER. No. Certainly, I mean we don't want the target of the investigation, who is a spy or terrorist, to find out we're looking for documents about them.

Mr. NOJEIM. Mr. Gohmert, we agree with that. We would add one more thing and that is that to satisfy the court that struck down the National Security Letter statute that applies to Internet Service Providers, to satisfy that court, you would also need to time limit the gag. It would have to expire after a time certain. And I think that that could be done; that the time could be a lengthy one. In the Senate version of the SAFE Act, to which I referred earlier, has I believe a 6-month time limit on the gag.

I'd also like to submit for the record a copy of the form of a National Security Letter so that people can see exactly what these look like. They have very compelling language. You get the letter. You must turn over the documents, and you can't tell anyone that you got the letter, and we would support the amendment that was discussed earlier.

Mr. BAKER. Congressman, if I could just on this——

Mr. GOHMERT. Certainly.

Mr. BAKER. On the time limit, I mean, to me I think that's a very dangerous and bad idea quite frankly, because I mean some of the targets of our investigations, let's be quite clear, are agents of a foreign power. What does that mean? That means in some instances, they are foreign government officials who we are investigating, and

we want to obtain information about them, and I don't think that anybody here thinks that they should deserve notice about what the United States Government is doing to investigate their activities. I just think that doesn't make any sense.

Mr. NOJEIM. Should the Government concede——

Mr. GOHMERT. Excuse me. Just a moment.

Mr. NOJEIM. By the agency?

Mr. GOHMERT. Just a moment. Let me follow up on that. What if there were a time limit, some might call it a sunset provision, where you'd have to come back in and re-justify the need to extent it further?

Mr. BAKER. Well, I mean off the top of my head, that kind of—come back to the FISA Court and try to justify it—that kind of idea makes more sense because there are some times when even if you're investigating a United States person where the Government assesses that it makes more sense; we're getting more intelligence information by leaving this person in place than by trying to take them out or arrest them or something like that. And so sometimes intelligence investigations can go on for a considerable period of time, and that's appropriate and done under the scrutiny of the FISA Court.

So I think that is an idea that I'm sure the Department would be willing to work with the committee on.

Mr. GOHMERT. Mr. Nojeim, does that address your concern?

Mr. NOJEIM. It does, and it is the approach that the Senate took in its version of the Safe Act, and we would support it.

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

Mr. GOHMERT. Okay. I'm sorry.

Mr. COBLE. We'll have a second round, Mr. Gohmert.

Mr. COBLE. The distinguished gentlelady from California, Ms. Waters.

The distinguished gentleman from California, Mr. Lungren.

Mr. LUNGREN. Thank you very much, Mr. Chairman. I appreciate these hearings continuing on the oversight responsibility of the Judiciary Committee and if anybody doesn't believe that we're reviewing the PATRIOT Act, they ought to just look at the schedule of the committee and the Subcommittee.

I'd like to get one thing, though, at least my response on the record. There was a use of a phrase a little while ago about abuse of power. And the suggestion was made that you in the Justice Department have failed in your responsibility to report to us. But, Mr. Baker, you've made it clear that you on a regular basis have to do those detailed reports to the House and the Senate Intelligence Committees; is that correct?

Mr. BAKER. That's correct.

Mr. LUNGREN. Have you discharged that responsibility in the last 4 years?

Mr. BAKER. Absolutely. I have. When I first came to OIPR as an attorney assigned to do those reports—it's very painstaking—and since then I've supervised the preparation.

Mr. LUNGREN. Has there been a time in which those reports were not done to the relevant committees as required by law, both the House and the Senate.

Mr. BAKER. No. We comply with the law in that regard.

Now, I'm going to be frank. There are times—on the big semi-annual report that I talked about that has all the details in it, we provide those on a timely basis. There's times when on some of the other reports we're slower than we should be. And we know that. We're trying to address that, and it's a question of resources within our office quite frankly.

Mr. LUNGREN. I appreciate that. It's just been experience when I served on the House Intelligence Committee that generally speaking—I'm not talking about any single member, but generally speaking the other Members of Congress don't take advantage of the opportunity they have to look at that information. So I just want to make it clear that you have reported as required in the detail as required?

Mr. BAKER. Yes, sir.

Mr. LUNGREN. Secondly, have you ever heard of sleeper cells that they sometimes sleep longer than 6 months?

Mr. BAKER. Sleeper. Well, without going into specifics about what we know about sleeper cells, I mean that's the whole idea. They sit there until such time as, you know, the authority that has control of them activates them.

Mr. LUNGREN. I understand. See here's what I don't understand. We passed these laws in response to a specific attack on the United States by those who wish to do us harm. A fatwa that issued in 1999 that said it is the obligation of everybody who is the subject of the fatwa, the recipient of the fatwa, it is their obligation to kill every American anywhere in the world—man, woman, or child; belligerent or non-belligerent. That's what we're up against. We passed the law in that context, and sometimes I think we forget in what context we passed that law.

Now, the claim was made that a judge has no discretion whatsoever, at least the impression was made that the judge has no discretion whatsoever under section 215 in the application, because it says shall. It says upon application made pursuant to this section, the judge shall enter a next party order as requested or as modified, approving the release of records. Followed by this language if the judge finds that the application meets the requirements of this section. And what are the requirements of this section? That there be an investigation quote "to obtain foreign intelligence information not concerning a United States person." Correct?

Mr. BAKER. Yes.

Mr. LUNGREN. The judge has to make that finding. Correct? He has to check and make sure that what you say is in there?

Mr. BAKER. That's correct.

Mr. LUNGREN. Or to protect against international terrorism or clandestine intelligence activities?

Mr. BAKER. That's right.

Mr. LUNGREN. Provided that such investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment of the Constitution. The judge is required to look at that, is he not?

Mr. BAKER. Yes.

Mr. LUNGREN. And you have to prove to his satisfaction that, in fact, that is the basis for the request; correct?

Mr. BAKER. Under the law, the judge has to see and assure himself or herself that the certification is there.

Mr. GOHMERT. Right.

Mr. BAKER. But in my experience, this court, going back many years is very active in looking at and looking behind what the Government is presenting to it, and so I can assure you that that's what happens, and as we've reported publicly in the report that was mentioned earlier, last year on the full content FISAs, the FISA Court made modifications, substantive modifications in 94 applications. It's a very active court. They look at what we're doing. They're very conscientious.

Mr. LUNGREN. Now, as I understand the testimony, library records have not been accessed by resort to section 215?

Mr. BAKER. That's correct.

Mr. LUNGREN. Even though we know now in retrospect that the—some of the hijackers in 9/11 utilized public libraries, their computers, for the various reasons you've talked about?

Mr. WAINSTEIN. That's true. We have not issued any 215 orders directed at libraries. Keep in mind, however, and there has been testimony over the last week or two about this, that we have had contact with libraries, and many libraries have actually voluntarily provided information to us over the years since 9/11 in relation to terrorism and criminal investigations.

So we haven't had to resort to 215 order.

Mr. LUNGREN. See if some of the discussion I've seen in the public has suggested that somehow the Federal Government is so interested in going after libraries as if there's no context in this. And I think a lot of American citizens would be surprised to know that 9/11 hijackers utilize the libraries, and in retrospect, we wish we knew about that. In retrospect, we wish we'd been able to connect dots. Thank you.

Mr. COBLE. I thank the gentleman from California. The gentleman from Massachusetts, Mr. Delahunt.

Ms. Waters, did you want to reclaim your time?

Ms. WATERS. Yes, I would like very much, Mr. Chairman.

Mr. COBLE. The gentlelady from California.

Ms. WATERS. I appreciate and thank you. I think we should continue on the discussion about the libraries. I just heard our witness say that you have not had to access information about people using the library. You have not had to resort to that, and you have not had to resort to informing a librarian that they cannot share that information or tell the party that maybe is being investigated. Is that true?

Mr. BAKER. That is correct. We have not used this provision, section 215 for the purpose of obtaining information from libraries.

Ms. WATERS. I see. I'm sorry. That's not my understanding, and I have to go back and do a little research about the information that was—that alarmed us when we first learned about your ability to identify individuals who use a library and the materials that they seek in that library. My friend from California, my colleague on the opposite side of the aisle, indicated that he could not understand Americans who would be concerned about that. And he thought perhaps Americans may not have heard that some of the

hijackers may have used the libraries in order to access information that may have been used in the attack.

I think that many Americans heard that that was a possibility. I am one who's adamantly opposed to librarians having to give information to law enforcement of any kind about who uses the library, when they use the library, and what subject matter they researched or read or had access to in the library. And it's not because we're not concerned about safety, and we're not concerned about terrorism. America is a very special country, with a constitution that guarantees us privacy, and to think that you would be—your privacy would be invaded in the way that this section allows is alarming to some of us.

And so I wish not to have the moment pass by having my colleague from California describe his understanding of this section and his lack of appreciation for why Americans would be concerned about this, and I wish to just share with you that I'm glad you have not had to use it. I'm going to research the information that I thought I had seen about your having used that, and I would oppose this continuously and forever because I think it is one of the most egregious violations of privacy to be targeted in the library.

Mr. CONYERS. Would the gentlelady yield?

Ms. WATERS. Yes, I will certainly yield to the gentleman.

Mr. CONYERS. One of our problems, and I'm glad you've re-raised this subject is that you don't need to use what is it—215?—to get to the libraries. You can get to the libraries through a National Security Letter, which is an administrative subpoena. And guess what? They won't tell us how many of those letters they've used. And what we think has been happening is that they've been getting to libraries, not through 215, but through this other route.

I have not raised that. I didn't raise that question yet, and that's why I praise you reclaiming your time.

Mr. NOJEIM. If I could just put a little fine point on that? The Government could use a National Security Letter to get the records of a person's use of the library computer, but they couldn't use the National Security Letter to get records about what books the person checked out. So they could find out where the person went on the Internet, but not use it to get records about what they checked out of the library.

Here's where the real debate ought to be on this section. If the Government believes that Mohammad Atta has gone into a library, checked out a book, and that he's an agent of a foreign power or foreign terrorist organization, they ought to be able to get records about that if they can show that they're relevant to an investigation. They ought to be able to do that.

The real debate is about whether they can go to the library and say, "Give us the records about what everybody checked out, because in that—inside of those many records will be information that's relevant to our investigation." And what we're saying is focus on the agent of the foreign power, but leave the records that pertain to innocent people alone.

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

Ms. WATERS. All right. All right.

Mr. COBLE. The gentleman from——

Ms. WATERS. Thank you. Thank you very much.

Mr. COBLE. Mr. Wainstein may respond if you wanted to very—do you want to respond?

Mr. WAINSTEIN. I just wanted to point out that the Department has taken the position that the recipient of a 215 order can, in fact, challenge it if they think that it's overly broad and oppressive, and, in that case, a library, if they really thought that we were overly broadly asking for all the records—the records of all of the readers in the library could, in fact, consult with their attorney and then challenge it in court.

Mr. COBLE. Very well. The gentleman from Ohio is recognized for 5 minutes.

Mr. CHABOT. I thank the gentleman for his recognition. I'd just like to start out by reiterating something that my colleague from California, Mr. Lungren, mentioned before, and that's that I sometimes read articles and hear my colleagues sort of loosely state that after we passed the PATRIOT Act, there has been essentially no oversight; that we've kind of turned the Federal law enforcement forces loose on the American public and all kinds of kind of wild allegations, but clearly Congress has been getting the reports. Now, who's been reading these reports and whether we've been following up with our responsibilities in doing that is another matter.

But we were pretty careful in crafting this legislation. We also put in that legislation the requirement that we come back and revisit this to see how this has actually been carried out over the past 3, 4, 5 years, and that's what we're doing now. And I want to commend the Chairman for holding these hearings, and we've had a significant number of these hearings; and I think the attendance has been pretty good on both sides of the aisle. Both Republicans and Democrats who have been here I want to commend them for doing that.

But this is part of that oversight process, and I think when we passed the PATRIOT Act, we were very serious about exercising this oversight, and this is all part of that procedure and process.

Mr. Nojeim, let me start with you. In your testimony, you point out that prior to the passage of the USA PATRIOT Act, roving wiretaps were available in criminal investigations, but not, of course, in FISA investigations.

Leaving aside for a moment the two particular criticisms of section 206 contained in your testimony, do you agree with the other witnesses on the panel that roving wiretap authority should be available in FISA investigations?

Mr. NOJEIM. We believe that roving wiretaps are potentially particularly intrusive and that for that reason, if Congress decides to make them available in intelligence investigations, it ought to include the same kinds of protections that it put for roving wiretaps in criminal investigations.

Mr. CHABOT. Okay. Thank you.

Mr. Baker, let me go to you next. In Mr. Nojeim's testimony, he alleges that the Government can now issue John Doe roving wiretaps that fails to specify a target or a telephone. It's my understanding, however, that a roving wiretap order issued be the FISA Court must specify a particular target, and that this target must either be identified or described.

And furthermore, I've been told that the FISA Court must find that there is probable cause to believe that the identified or described target is a foreign power, agent of a foreign power, and may take action to thwart surveillance. Am I accurately describing the requirements set forth in FISA or is Mr. Nojeim's allegation correct?

Mr. BAKER. No. You're actually—you're accurately describing the requirements of FISA. We must provide the identity, if known, of the target or a description of the target, and then—and we have to establish probable cause to believe that that target is a foreign power or an agent of a foreign power.

As I said earlier, those two terms are defined. It's not—we don't just make it up. They're specifically defined in the statute, and when you come to a U.S. person, all of those definitions have a link to the criminal law of the United States.

And in addition to that, then the court has to make the specific finding, as you suggest, that that target, that target, is engaging in activities that may have the effect of thwarting surveillance.

Mr. CHABOT. And in Mr. Nojeim's testimony, he also suggests that the section 206 of the USA PATRIOT Act lacks sufficient privacy safeguards, but he doesn't mention the statutory requirement that each roving wiretap order issued by the FISA Court contains specific minimization procedures in order to limit the Government's acquisition and retention and dissemination of information about Americans.

Could you please discuss what minimization procedures are, and why they're important, and whether you feel that these procedures adequately protect the privacy of our citizens?

Mr. BAKER. In order to obtain a FISA Order in the first place, each application must include within it minimization procedures that are specifically approved by the Attorney General and that are reasonably designed in light of the purpose and technique that's going to be used to protect against the acquisition, retention, and dissemination of non-pertinent communications by Americans. And these procedures have to be specific. They have to be reasonably designed in light of the need for the Government to obtain, collect, and disseminate foreign intelligence information, and then the court makes a finding, when it's reviewing our application, that those minimization procedures meet the definition set forth in the statute by Congress.

Once the court has made that assessment and the other assessments under the statute and determines that the order can be lawfully issued, the court grants us the authority and then it orders us to follow the minimization procedures.

The minimization procedures are—there are standard procedures that exist that we use in just about every case. And then for particular circumstances, the court or the Government or both will craft specialized minimization procedures to address situations that come up where the intrusion in privacy might be higher, and you have to adjust accordingly. And so the court is very active in assuring itself before it issues an order that the minimization procedures are appropriate.

Mr. COBLE. And the gentleman's time has expired. And consistent with what the gentleman—Mr. Delahunt, I'll give you just

a minute. I just want to follow up on what the gentleman from Ohio said regarding our oversight.

And the other day, at our hearing, Mr. Delahunt, you commented about the accelerated path that we are now pursuing. I hope that if any of these provisions are subsequently sunsetted, I would like to see the sunset occur at the conclusion of the calendar year of the second year of the Congress rather than the first year. That might, Mr. Delahunt, preclude our having to do this exercise again.

The distinguished gentleman from Massachusetts, Mr. Delahunt.

Mr. DELAHUNT. Thank you, Mr. Chairman. Just to follow up on that point. I think it was you, Mr. Wainstein, that said you encouraged this committee to make these provisions permanent. This really does go to the issue of oversight. I don't want to get into the details of the various provisions at this point.

But, Mr. Chairman, you know, as I participate in these various hearings, I'm becoming—I'm reaching the conclusion that if they're not to be sunsetted, if they're to be modified, if there are to be changes, or if there are—if they are just reauthorized as is, I think it's very important that they not be made permanent; that these kind of hearings are positive and are absolutely integral in terms of our role as far as oversight is concerned. It gives us—I can—I dare say the gentleman from Justice would not be here but for the fact that there is a sunset provision. And maybe, just maybe, we ought to expand the sunset aspect of the PATRIOT Act to other provisions to give us a more—how shall I say—leverage in terms of our oversight function, and that is if nothing with that act changes.

But the reality is, with all due respect, you know, dealing with the Department in terms of securing information without the leverage of the sunset is extremely difficult. It isn't easy. And I think that is a sentiment that is shared on both sides and in other committees. And I have no doubt, Mr. Baker, that, you know, you take your role very seriously, and I'm sure that the career people that are working under your direction are people who act in good faith. But the system itself requires more than just checks and balances within the Executive Branch.

And that's why I put this idea out about as we reauthorize or as we address the sunset provisions to expand the sunset to the entire PATRIOT Act, to allow us to have a more significant role in terms of our responsibility and our review.

Mr. BAKER. May I just respond briefly to that?

Mr. DELAHUNT. Sure.

Mr. BAKER. And I thank you for your comments. We do take our jobs very seriously.

Mr. DELAHUNT. I know that.

Mr. BAKER. And we do conduct—ourselves we conduct oversight of the activities of the FBI and the——

Mr. DELAHUNT. I understand.

Mr. BAKER.—the intelligence committees. I mean intelligence community. And oversight it seems to me—effective oversight to do it—it's a hard job—it's a really hard job. You really got to roll up your sleeves and dig in and do a lot of work——

Mr. DELAHUNT. Right.

Mr. BAKER.—and push, and get the information you need to satisfy yourself that what's being done is appropriate and consistent with the law.

I will tell you that even though I don't agree with all their conclusions, the Senate Intelligence Committee audit staff conducted a very lengthy oversight or audit of the FISA process, and they're finishing the report, and it was referenced yesterday, and that, I mean, I myself spent many, many, many hours with them discussing the process and so on.

Mr. DELAHUNT. Right.

Mr. BAKER. And they had access to everything. And that——

Mr. DELAHUNT. I'm running out of time. Here's part of my problem, too, Mr. Baker, is that you reference the, you know, the reports to the Intelligence Committee. I don't know, but does the Judiciary Committee that has, you know, jurisdiction over the Department of Justice—do we get those same reports?

Mr. BAKER. I don't pretend to understand all the rules of Congress, but——

Mr. DELAHUNT. Neither do I.

Mr. BAKER.—as I understand it, those kinds of reports are available to Members of other committees. You go up and read it in the secure space of the Intelligence Committee, and then staff members who have appropriate clearances——

Mr. DELAHUNT. Okay.

Mr. BAKER.—can go——

Mr. DELAHUNT. Well, again, another suggestion would be, Mr. Chairman, is when the time comes to have—that Justice report directly to this committee as well as the Intelligence Committee since we do have oversight.

Part of the problem, Mr. Baker, is that the FISA Court—and I'm sure again—that these judges—you know, they're really title III judges I understand that move over to the FISA Court—but there again everything is done in secret, obviously by necessity. But, as I said earlier in the week, part of the problem here is balancing the need for transparency versus the need for secrecy because of national security and the concerns that people have expressed about privacy and libraries, et cetera are part of that balance. And, you know, let me just ask one more question.

I think the suggestions and the recommendations by Mr.—is it Nojeim?

Mr. NOJEIM. Nojeim. Thank you.

Mr. DELAHUNT. Nojeim. Are really reasonable. I don't see the heavy burden that the adoption of those recommendations would put on the Government, and yet would, you know, accrue to the benefit of the American people in terms of their concerns about what's happening behind closed doors, because it is happening all behind closed doors. We've got to provide more information and become more transparent. That's difficult. I understand. But that's the—I think the role of this committee working with the—you know, with the Department, and really thinking this thing through in a responsible way. Thank you.

Mr. COBLE. The gentleman's time has expired. We'll get back on the second round, Mr. Baker. We're going to have a second round.

The gentlelady from Texas has joined us. Ms. Jackson Lee, you're recognized for 5 minutes.

Ms. JACKSON LEE. Thank you very much, Mr. Chairman, and, Mr. Nojeim, I'm going to pose a series of questions for you, so ask mine, and then you can weave in your commentary.

Let me first of all thank both the Chairman and Ranking Member of the Subcommittee. I know this is leading to the potential of the reauthorization of certain aspects of PATRIOT Act One, and, of course, also moving into PATRIOT Act Two.

I am on record—I might as well as they say share it all for opposing PATRIOT Act One, and considering where we are today, on any aspects that are now being called to be reauthorized.

As it relates to the next step, I'm on record for being enormously skeptical to the extent of moving past the 90 percent radar screen. It's fair to make that acknowledgement.

Let me share with you just a few comments and if you can point right back to libraries and access and the clear equation of invasion of privacy equals excellent security or absolute security.

My recollection is that one of the reasons of the Founding Fathers fleeing from their previous nation site was this question of freedom. We did not devise the Bill of Rights in the 20th century. It was devised by early founders of this nation. And so it must have been something keenly part of the cornerstone of America. And that is unfortunately other than the recognition of the dignity and the humanity of slaves and women, freedom was a very, very serious in-depth infrastructure or fabric of our society. And we were willing to die for it.

I recall after 9/11, one of the tools of so-called freedom or security was the registration of Pakistani males and others. My knowledge is that not one or barely one terrorist was found during that registration period, and quietly we ended it. So the question is, as we look toward our security, I happen to focus more on technology, security of the borders, preventing people who have untoward desires from coming into the United States, and also giving law enforcement the appropriate tools.

Would you answer for me the fact of whether or not the complete invasion of one's private e-mails, technology, library usage, et cetera is preventative of terrorism or is it simply a tool to make a case that you have the intent or the inclination or the background or the previous thought processes that might make you a terrorist?

Mr. NOJEIM. We believe that when the Government has strong evidence that a person is up to no good, that they're a terrorist, that they can get access to very private information about that person to help prove their case.

Ms. JACKSON LEE. Already? Now?

Mr. NOJEIM. That then can do it now and that they ought to be able to do it. When the Government has, for example, probable cause of crime that there's—that a person is involved in crime and that in their house is evidence of that crime, they should be able to get a warrant and go into their house and find that evidence. The important thing to remember is that there are safeguards, and what the PATRIOT Act did was erode the safeguards.

Our advocacy today and our advocacy throughout this debate has been about restoring some of those safeguards. One of the safeguards that we want to restore, besides judicial review and meaningful judicial review, is openness to the public about how particular powers are being used. And Mr. Delahunt was asking whether the committee gets reports about section 215. Indeed, the statute requires that the Attorney General provide to the Judiciary Committee a report setting forth the total number of section 215 orders that it has applied for and the total number of such orders either granted, modified, or denied.

It also has to provide similar information to the general public about FISA Orders—those full probable cause "that-the-person-is-an-agent-of-a-foreign-power" orders that allow them to wiretap or break into a person's home. It has to provide that same information about much more intrusive searches to the entire public, and we see no reason why the Government couldn't provide that same information about the less intrusive section 215 searches to the entire public, especially given that the Attorney General has twice disclosed exactly that same information.

Ms. JACKSON LEE. Mr. Baker, if I might just get an answer. What about those safeguards? Can you not live with the safeguards that the witness has just spoken about?

Mr. COBLE. Would the gentlelady suspend just for a moment, Ms. Jackson Lee? Mr. Baker, if you would answer that very quickly. We have a vote on the floor, and we will come back, Ms. Jackson Lee.

Ms. JACKSON LEE. Thank you, Mr. Chairman.

Mr. COBLE. We will come back for—Mr. Baker, if you will respond very quickly.

Mr. BAKER. FISA—excuse me—FISA includes a number of reporting provisions, and I think that the Department has expressed a willingness to work with the committee to discuss whatever additional requirements might be appropriate, but we need to remember that we're dealing with the national security, and so we have to always be consistent with that.

Ms. JACKSON LEE. We'll carry that on further.

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

Ms. JACKSON LEE. Thank you very much.

Mr. COBLE. And the panelists, if you all will just rest ways. Hopefully, we'll be back imminently. I'm thinking 10 minutes probably at the most. Thank you.

[Recess.]

Mr. COBLE. I apologize to the panelists. Sometimes these best laid plans of mice and men, you know, sometimes go awry. And to compound the confusion, as I told you all earlier, this—we must make this hearing room available to the Courts and Intellectual Properties Subcommittee. So we're going to have to adjourn about quarter 'til twelve to let them wrap up. So but for everyone's information, we will keep the record open for 7 days. And we can communicate with you all. You all can communicate with us.

So we'll start our second round, and maybe try to make the 5-minute rule, maybe a 2-minute rule just to get around.

Mr. Nojeim, you wanted to respond to Mr. Wainstein. Did you ever do that after the first round? If you did not, I'll let you do that now.

Mr. SCOTT. I think he did. He did.

Mr. COBLE. All right. Bob—Mr. Scott says that he thinks that you did.

Mr. NOJEIM. Okay.

Mr. COBLE. Did you want to respond to what he said, Mr. Wainstein. I don't remember.

Mr. WAINSTEIN. I don't remember what he responded to——

Mr. COBLE. Okay.

Mr. WAINSTEIN.—to whatever I said.

Mr. COBLE. Well, we're being fair and balanced here in any event. Let's see what we do here.

Mr. Baker, even if the Government is not sure of the actual identity of the target—I'm talking roving now—does FISA, nonetheless, require the Government to provide a description of the target of the electronic surveillance to the FISA Court, A. And, B, how difficult is it to identify international terrorists and foreign intelligence agents by name?

Mr. BAKER. Yes. The statute requires us to either provide the identity or a description of the target, and based on whatever we provide, on that factual basis, the court has to be able to make the other findings that the statute requires, including probable cause to believe that the target is an agent of a foreign power. So the answer is there has to be a target, and the court has to be able to make some findings with respect to that target.

Mr. COBLE. I want to thank you, sir. Mr. Khuzami, do you believe that with section 206 of the USA PATRIOT Act, foreign intelligence investigations can be more—can more effectively gather critical information with the purpose of preventing a massive disaster not unlike September 11th, and how would the antiquated requirement of 1986 impede the successful prevention of terrorist attacks today?

Mr. KHUZAMI. Well, I think it's——

Mr. COBLE. Your mike is not on, Mr. Khuzami.

Mr. KHUZAMI. Sorry. Yes. I—you know, the roving wiretap authority is critical because you don't always have the ability to identify in advance what communications facility the target might use, and you can lose very valuable intelligence and information in that interim period, either before you know what facility is going to be used or before you can ascertain their identity. And I frankly think that given the remainder of the protections in that statute that not making those requirements is an entirely proper balance of individual rights, but at the same time ensures that we protect national security.

Mr. COBLE. I thank the gentleman. Mr. Scott.

Mr. SCOTT. Thank you, Mr. Chairman. First, did somebody say that no part of the PATRIOT Act has been found unconstitutional?

Let me ask it another way. Has any part of the PATRIOT Act been found unconstitutional.

Mr. BAKER. I believe the answer to that question is no. I—specifically a provision of the PATRIOT Act. Material support. I take that back. There's a material support provision.

Mr. SCOTT. That's been found unconstitutional?

Mr. BAKER. Mr. Wainstein can speak on that. Yeah.

Mr. SCOTT. Any other part?

Mr. NOJEIM. There are two provisions.

Mr. SCOTT. Wasn't 505(a)?

Mr. NOJEIM. There are two provisions that have been found unconstitutional. The first is the material support provision as it relates to expert advice and assistance. And the second is section 505(a), National Security Letter provision, as it applies to Internet Service Providers.

And I'd like to illustrate that if I could. Section—what the PATRIOT Act did was to amend section 505(a), and the first poster that I'll show here shows what—I'm sorry. What the PATRIOT Act did in section 505(a) was amend 18 U.S.C., section 2709, which is the National Security Letter provision that applies to Internet Service Providers. This is 18 U.S.C., section 2709 before the PATRIOT Act.

This is how section 505(a) of the PATRIOT Act amended section 2709. That which is in yellow was added. That which is crossed out was deleted.

As you can see, it rewrote this statute. And the last poster shows what's left of this statute after the court in *Doe* v. *Ashcroft* struck it down. It stuck down not only what was in the statute before the PATRIOT Act, but it struck down every single word of section 505(a) of the PATRIOT Act.

So we believe that this illustrates how that particular section of the PATRIOT Act was ruled unconstitutional. And I should add the changes that we're advocating to section 505 of the PATRIOT Act would bring into line with that court decision so that it could—National Security Letters could again be used.

Mr. SCOTT. Okay. Now, we—on section 215 you've got to get a warrant, but we've ascertained that this is not limited to crimes or terrorism. It includes foreign intelligence as well as terrorism and everything else so that you don't need probable cause of a crime. When you get the records—a suggestion has been that if it's overly broad, somebody can challenge it, but the target doesn't know you're going after, and there's no real challenge from the recipient of the warrant because after there's a specification—I think we've ascertained that the judge doesn't have a whole lot of discretion—doesn't have any discretion. Once the specification has been made, the judge shall enter the warrant. The person who gets the warrant is gagged, so they can't—I mean there's not a whole lot they can do.

So is there any meaningful challenge that a recipient, the one that gets the warrant and has to turn over the records, is there any meaningful challenge that they can muster up?

Mr. WAINSTEIN. Yes, sir. As has been stated here and in other hearings with Department witnesses, the Department has acknowledged that the recipient of a 215 order can consult with an attorney despite the non-disclosure requirement, and can challenge that order——

Mr. SCOTT. Wait a minute

Mr. WAINSTEIN. Order and process.

Mr. SCOTT. You mean you're not enforcing that part of what's written in the law?

Mr. WAINSTEIN. The non-disclosure requirement?

Mr. SCOTT. Right.

Mr. WAINSTEIN. We—the Department has taken the position in litigation that as written that means that a person, though he or she cannot disclose it to anybody else, can disclose the fact of the order to an attorney.

Mr. SCOTT. It's not written that way. We're just interpreting it that way.

Mr. WAINSTEIN. Yes. And the Department has stated that it would agree with the clarification to that effect. But that person can, in fact, challenge. The recipient of that order can challenge it before an article III judge.

Mr. SCOTT. Now——

Mr. COBLE. Mr. Scott, would you suspend just a minute? Since the gentleman from Texas and the gentleman from California have gone to the trouble to come back, if you could wrap up, Bobby, then we'll recognize them. We're going to have to blow out of here at quarter 'til twelve.

Mr. SCOTT. Okay. Let me just stop right there.

Mr. COBLE. I appreciate that. Since you all came to the trouble, I want to recognize Mr. Gohmert.

Mr. GOHMERT. Okay. Thank you, Mr. Chairman. I'll be quick, as quick as I can be.

Let's see——

Mr. COBLE. Thank you, Bobby.

Mr. GOHMERT. Mr. Wainstein, I believe you were the one that indicated earlier the Department has taken a position that a recipient under 215 order could challenge, I believe, the breadth of the request or the scope of the request; is that correct?

Mr. WAINSTEIN. Yes, sir.

Mr. GOHMERT. Well, and it left me wondering. You said that's the Department's position because of the language. In your opinion could the next Department of Justice take a different position?

Mr. WAINSTEIN. Well, my understanding is the Department has taken that position consistent with all the witnesses who have appeared over the last few weeks, and I believe we've stated on the record that we would be supportive of a clarification of the law to that effect.

Mr. GOHMERT. Okay. That's what I wanted to be sure of. It was my concern that that might not be the case with another Administration if we did not clarify, and having signed orders or had hearings myself as a judge, when people came back and you saw that the scope was going too far a field, it seems to me pretty important that that be there for future Justice Departments that we may be concerned about. So you don't have a problem with that, either—clarifying the scope—that the scope could be challenged?

Mr. WAINSTEIN. The—It could be challenged. Yes, I think there's a variety of different challenges they could bring—it could be challenged in terms of the actual language. I don't know that that's been determined yet.

Mr. GOHMERT. Okay. Do you have anything further on that?

Mr. NOJEIM. Just that I think we should codify the person's right to challenge, and I should also add that the Department of Justice didn't always take the position that a person could consult with the attorney. They took that position after we sued them because peo-

ple were wanting to consult with ACLU attorneys about a National Security Letter that was received.

Mr. COBLE. The gentleman——

Mr. GOHMERT. Okay.

Mr. COBLE. Well, very quickly, Mr. Gohmert, and then I want to——

Mr. GOHMERT. All right. So——

Mr. COBLE.—and then I want to recognize Mr. Lungren.

Mr. GOHMERT. It sounds like Catch-22. They consult you about getting an order that they were not supposed to consult you about so it could be challenged.

Mr. NOJEIM. That was the issue. I mean they didn't know whether they could talk to anybody about it, and it was only after the litigation started that the Department of Justice started publicly taking this position.

Mr. GOHMERT. So obviously, they did let somebody know, even though that was a concern. But I understand your position. Thank you, Mr. Chairman.

Mr. COBLE. I thank the gentleman. Mr. Lungren, we have to vacate this room in about 3 minutes, and you're recognized as the final examiner.

Mr. LUNGREN. Well, that's a lot of pressure, Mr. Chairman. I just wanted to mention for the record that when we were talking about libraries, not only are we talking about those that use libraries that have already been mentioned, but the 9/11 Commission Report talked about Marwan Al-Shehhi and other members of the group that quote "used to frequent a library in Hamburg, Germany, to use the Internet." A *Washington Post* article, September 30, 2001, explained that another hijacker came from a poor Saudi family, but said quote "was facile enough with computers so he could use the Internet at a Del Ray Beach public library." I mean there is testimony that Deputy Attorney General James Comey before the Senate Judiciary Committee indicated the use of the New York Public Library by one of the hijackers.

So the only point I'm trying to make is that we didn't create this out of whole cloth. We have utilized investigative techniques for the purpose of trying to respond to the threat that is out there. And while we may tweak this law with respect to some of the suggestions that have been made here, the underlying law it seems to me is appropriate. So long as Congress continues with oversight, it is something that is necessary for the protection of this country. And I just hope that some of the—sort of the general gloom and doom that I see surrounding some of this is out there, and also some of the hyperbole utilized by some of the people in the library profession I don't believe is very helpful.

And when I read something such as a comment by Cindy Czesak, the director of New Jersey's Paterson Free Public Library, where she told Fox News that her institution collects every complete computer sign-up sheet. After that, it's removed and destroyed. We bought a new shredder. We're quite rebels.

Rebels from what? Thank you, Mr. Chairman.

Mr. COBLE. I thank you. And, Mr. Scott says he wants to be the final examiner, so I'll let him put a couple——

Mr. SCOTT. Well, I think since we're pressed for time, let me just articulate some concerns—back to the 215.

One of the problems we have is information obtained is not, as Mr. Nojeim indicated, not just information on the target. You go into the library. If Mohammad Atta had used the library, you can go and get everybody's library records as I understand it. You can get massive amounts of information. I understand in one situation somebody got—I don't know whether it was under 215 or some other—you got 300,000 records of people visiting Las Vegas.

Now, some of this kind of information may be relevant. If you got certain cities somebody's been in, it would be nice to know who has been in these five cities, on these specific dates, that could be a fairly small list, if you get millions of pieces of data. What happens to the information after you've used it? After you've run the tape, what happens to the information, and particularly when you have in here that it could be mostly in violation of first amendment rights? If it's not solely because of first amendment violations.

So if you got a list of the war protesters, you want to—that's a bit troublesome.

On the roving wiretap, we know that you can start this thing out without probable cause of a crime. There's no ascertainment requirement, and the Attorney General didn't want to agree to ascertain that the target was actually in the place where your listening in. And I think we're hearing that there is some judicial discretion as to whether or not the roving wiretap can be issued. I'm not sure how much of that discretion is related to the minimization, but that might be something we would look to.

But, Mr. Chairman, because we—and I keep harping on this—these—foreign intelligence is not just criminal terrorism activity. It can be anything that will help us in the conduct of our foreign affairs, which doesn't have to be anything relating to crimes at all. So we still have some concerns, and we'll pursue this in our additional hearings.

Mr. COBLE. I thank the gentleman. Folks, the bad news is that we are irregular in our scheduling today because of the next meeting. The good news is the record will be open for 7 days, and you all feel free to communicate with us as we will with you all.

We thank the witnesses for their testimony today. In order to ensure a full record and adequate consideration of this important issue, the record will, as I said, be left open for additional submissions for 7 days. Written questions that any Member wants to submit should also be submitted within that same 7-day period.

This concludes the oversight hearing on the implementation of the USA PATRIOT Act, Foreign Surveillance Intelligence Act (FISA) Part II. Thank you for your attendance, and this Subcommittee stands adjourned.

[Whereupon, at 11:45 a.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, for holding this hearing on the issues before us today. In a context where we have broken down the traditional wall that existence foreign intelligence gathering, particularly foreign intelligence, and criminal proceedings, to give the government broad authority to collect and share information, mostly secretly, I am concerned that we have also blurred the traditional line of protection for our privacy and freedoms.

While I agree that some lifting of the traditional restrictions in this area were justified, to induce the government to better use the authorities it already had in many instances, I am also mindful that those restrictions were placed there for a very good reason. We have seen with "COINTELPRO," Watergate, the FBI spying on Dr. Martin Luther King, Jr., and with other incidents, what abuse can occur when we do not keep a tight enough reign on the government's use of extraordinary powers. We shouldn't have to experience those problems again to ensure that such abuses do not occur.

Some of the provisions today reflect a trend that is troubling to me—the trend of the government to justify an ever increasing extension of extraordinary powers based on its convenience. We are considering time frames for surveillance operations that we have been extended even more since their PATRIOT Act extensions, all because the government says it is too costly for it to have to justify extensions to a court, even under the low burden of the FISA Court. If we can commit to speed billions of dollars in prison and other law enforcement costs just to codify sound bytes urged by the Department, we can certainly spend the time and expense it takes to assure that our privacy and freedoms are not unduly abridged.

Mr. Chairman, I believe that it is important that we be AND maintain our privacy and freedoms. I don't believe we should operate under the premise that we have to give up or balance one against the other. So, Mr. Chairman, look forward to the testimony of our witnesses on the provisions before us to learn more about what use is being made of the extraordinary powers authorized and whether sufficient oversight is being undertaken such that the powers are used in a way to protect our safety as well as our privacy and freedoms. Again, I thank you for putting together this hearing on these important matters.

PREPARED STATEMENT OF THE HONORABLE JOHN CONYERS, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN, AND RANKING MEMBER, COMMITTEE ON THE JUDICIARY

The provisions we're discussing today, like the PATRIOT Act itself, range from nonpolitical technical amendments to questionable infringements on court authority. I look forward to hearing from the witnesses about all of them.

I look forward to hearing from the Justice Department about why Section 207 should be reauthorized and allow secret surveillance for up to a year. Part of the justification for allowing the extraordinary intrusions under the Foreign Intelligence Surveillance Act is the extensive judicial oversight by the FISA court. This section takes that reasonable oversight away and gives the Justice Department authority to surveil suspects long after the relevant facts have expired. While the paperwork may be burdensome, a violation of a person's very privacy is more so.

I also look forward to hearing why Section 214 should be reauthorized. Pen register and trap and trace orders no longer need to be aimed at a agent of a foreign

power under this provision, and are available under the vague standard of "relevance." This is even more troublesome in light of how the PATRIOT Act has permanently expanded these orders to allow the government to record the websites a person visits and addresses and subject headings of the emails he sends and receives.

Also, I hope this hearing thoroughly discusses the lone wolf provision, also set to expire this year. FISA allows the secret surveillance, search and seizure only because it is necessary to protect us from foreign powers. To expand FISA to apply to those who by definition have no connection to foreign powers starts our law enforcement down a slippery slope. There is no telling where it might end.

LETTER FROM JAMIE E. BROWN, ACTING ASSISTANT ATTORNEY GENERAL, U.S. DEPARTMENT OF JUSTICE, DATED APRIL 30, 2003, TO THE HONORABLE ORRIN HATCH, CHAIRMAN, COMMITTEE ON THE JUDICIARY, UNITED STATES SENATE

U.S. Department of Justice

Office of Legislative Affairs

Washington, D.C. 20530

April 30, 2003

The Honorable Orrin G. Hatch
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

This is in response to your request for the Administration's views on various proposed amendments to S. 113, a bill that would amend the Foreign Intelligence Surveillance Act of 1978 to permit electronic surveillance and physical searches of so-called "lone wolf" international terrorists – *i.e.*, non-United States persons who engage in international terrorism or activities in preparation therefor without any demonstrable affiliation with an international terrorist group or other foreign power. On March 5, 2003, the Administration sent a letter indicating its support for S. 113 (copy attached). The Administration, however, is greatly concerned that this important FISA amendment would be subject to a sunset provision included in the USA PATRIOT Act of 2001. The Administration opposes the sunset language, and looks forward to working with Congress to ensure that this FISA amendment and those other portions of the USA PATRIOT Act subject to the sunset provision are addressed at the appropriate time. For reasons set forth below, we oppose the proposed amendments to S. 113. In particular, the Administration is concerned that the proposed amendments would weaken the FISA as an important instrument in the arsenal of the United States Government in combating terrorism and the espionage activities of foreign powers.

Authority of the FISC and FISCR. The first proposed amendment to S. 113, entitled "Sec. 2. Additional Improvements to Foreign Intelligence Surveillance Act of 1978," would add a provision to 50 U.S.C. § 1803 to grant the Foreign Intelligence Surveillance Court ("FISC") and the Foreign Intelligence Surveillance Court of Review ("FISCR") authority to "establish such rules and procedures, and take such actions, as are reasonably necessary to administer their responsibilities under this Act." The Administration opposes this grant of authority to a court that has an extremely limited statutory function of approving or disapproving applications made by the Government of orders with respect to electronic surveillance and search. Granting rulemaking authority by statute to the FISC and the FISCR – courts that operate in secret and that are of very limited jurisdiction that is specified in detail in the FISA – is inappropriate.

Reporting Requirements. A second group of related amendments would require additional reporting concerning the use of FISA. Each is objectionable for reasons discussed below.

a. The first reporting amendment would require public disclosure of the number of United States persons targeted under various provisions of FISA. Under current law, the Department publicly reports the annual aggregate number of FISA searches and surveillances, but does not disclose publicly how many of those searches and surveillances involve United States persons. *See* 50 U.S.C. §§ 1807, 1826. The proposal also would require public disclosure of the number of times the Attorney General authorized the use of FISA information in a criminal proceeding – a statistic that currently is reported to the Intelligence Committees as part of a longstanding, carefully constructed, and balanced accommodation between the Executive and Legislative branches and in accordance with the FISA itself. *See* 50 U.S.C. § 1808(a)(2)(A). Finally, the provision would require disclosure of portions of FISA pleadings and orders that deal with significant questions of law (not including discussion of facts) "in a manner consistent with the protection of the national security of the United States." Each of these three reporting requirements is addressed below.

We oppose a requirement to disclose publicly the number of FISA targets that are United States persons. Congress has in the past considered and rejected proposals to require disclosure of this information to the general public rather than to the Intelligence Committees. In 1984, the Senate Select Committee on Intelligence was "asked by the American Civil Liberties Union to consider making public the number of U.S. persons who have been FISA surveillance targets." S. Rep. No. 98-660, 98th Cong., 2d Sess. 25 (1984). The Committee rejected that proposal because "the benefits of such disclosure for public understanding of FISA's impact would [not] outweigh the damage to FBI foreign counterintelligence capabilities that can reasonably be expected to result." *Ibid.* As the Committee explained, "[a]ny specific or approximate figure would provide significant information about the extent of the FBI's knowledge of the existence of hostile foreign intelligence agents in this country. As in other areas of intelligence oversight, the Committee must attempt to strike a proper balance between the need for public accountability and the secrecy required for effective intelligence operations." *Ibid.* This analysis is at least as applicable to foreign terrorist organizations today as for foreign intelligence organizations and the Administration continues to support the balance that was struck in 1978 and reaffirmed in 1984.

We also oppose a requirement to disclose publicly the number of times the Attorney General has authorized the disclosure of FISA information for law enforcement purposes. This provision is problematic primarily because it is not confined to cases in which FISA information is actually used in a proceeding.[1] Revealing the number of Attorney General authorizations for

[1] Under current law, the Government must notify an aggrieved party – defined to include a FISA target as well as anyone whose communications were subjected to FISA surveillance – when it intends to use information obtained or derived from FISA against that person in any

such use – as opposed to the use itself – is troubling because that information could involve classified and non-public matters with ongoing operational significance – *e.g.*, an investigation that has not yet resulted in a public indictment or trial, or in which no indictment or trial ever will occur. Thus, these numbers potentially could reveal information about the Department's classified, operational efforts to protect against the activities of foreign spies and terrorists.

Finally, we believe that the disclosure of FISA pleadings and orders that deal with significant questions of law is inherently inconsistent with "the protection of the national security of the United States." Virtually the entirety of each application to the FISC discusses the facts, techniques, or pleading of highly classified FISA operations. As we noted in our letter of August 6, 2002, on predecessor legislation in the 107th Congress, "[a]n interpretation by the FISC of the applicability of FISA to a technique or circumstance, no matter how conceptually drawn, could provide our adversaries with clues to relative safe harbors from the reach of FISA." A copy of our earlier letter is attached for your convenience.

b. A separate but similar proposal, entitled "Sec. 2. Public Reporting Requirements Under the Foreign Intelligence Surveillance Act of 1978" and proposed by Senator Feingold, also would impose public reporting obligations. Instead of requiring the Department to report the number of FISA targets who are United States persons, it would require reporting of the number who are not United States persons, broken out by the type of FISA activity involved – *e.g.*, electronic surveillance and physical search. This proposal also would require the Department to identify individuals who "acted wholly alone." Like the proposal discussed above, this proposal would require the Department to report the number of times the Attorney General authorized the use of FISA information in a criminal proceeding, and portions of FISA pleadings and orders that deal with significant questions of law "in a manner consistent with the protection of the national security of the United States." The objections set forth above apply equally to this proposal.

c. Finally, a very recent reporting proposal, also proposed by Senator Feingold, would require an annual report on FISA to the Intelligence and Judiciary Committees. The report would include the classified statistical information described above – including numbers of non-U.S. persons targeted under each major provision of FISA – and would also require submission of portions of FISA pleadings and court orders. For reasons stated above and in our letter of August 6, 2002, we continue to oppose any requirement to submit portions of FISA pleadings and orders. More broadly, we strongly oppose the amendment because it threatens to upset the delicate balance between the Executive and Legislative Branches of government in the area of intelligence and intelligence-related oversight and reporting.

The FISA statute prescribes the types of information that must routinely be provided to the Judiciary Committees. Under current law, the Department of Justice provides to the Judiciary Committees and makes public "the total number of applications made for orders and

---

proceeding, including but not limited to a criminal trial. 50 U.S.C. §§ 1801(k), 1806(c); see 50 U.S.C. §§ 1821(2), 1825(d) (corresponding provisions for FISA physical searches).

extensions of orders" approving electronic surveillance and physical searches under FISA, and "the total number of such orders and extensions either granted, modified, or denied." 50 U.S.C. § 1807; see 50 U.S.C. § 1826; 50 U.S.C. § 1846 (similar reporting requirement for numbers of pen-trap applications and orders); 50 U.S.C. § 1862 (similar reporting requirement for numbers of applications and orders for tangible things). The Department has, of course, consistently met these statutory requirements.

The FISA reporting obligations concerning the Intelligence Committees are much broader. Under 50 U.S.C. § 1808, the Attorney General must "fully inform" the House and Senate Intelligence Committees "concerning all electronic surveillance" conducted under FISA, and under 50 U.S.C. § 1826 he must do so "concerning all physical searches" conducted under the statute. In keeping with this standard, the Department submits extremely lengthy and detailed semi-annual reports to the Intelligence Committees, including specific information on "each criminal case in which information acquired [from a FISA electronic surveillance] has been authorized for use at trial," 50 U.S.C. § 1808(a)(2)(B), and "the number of physical searches which involved searches of the residences, offices, or personal property of United States persons," 50 U.S.C. § 1826(3). The reports also review significant legal and operational developments that have occurred during the previous six months. These classified reports are painstakingly prepared in the Justice Department and are obviously, from the questions and comments they generate, closely scrutinized by the Intelligence Committees. See generally S. Res. No. 400, 94th Cong., 2d Sess. (1976); H.R. Res. No. 658, 95th Cong., 1st Sess. (1977).

The "fully inform" standard that governs Intelligence Committee oversight of FISA is the same standard that governs Congressional oversight of the Intelligence Community in general. See S. Rep. No. 95-604, 95th Cong., 1st Sess. 60-61 (1977); S. Rep. No. 95-701, 95th Cong., 2d Sess. 67-68 (1978); see also H.R. Rep. No. 95-1283, Pt. 1, 95th Cong., 2d Sess. 96 (1978). The requirement to "fully inform" the Intelligence Committees, rather than Congress as a whole, is consistent with the long-standing legal framework and historical practice for Intelligence Community reporting to, and oversight by, Congress on matters relating to intelligence and intelligence-related activities of the United States government. Consistent with the President's constitutional authority to protect national security information, Congress and the President established reporting and oversight procedures that balance Congress' oversight responsibility with the need to restrict access to sensitive information regarding intelligence sources and methods. The delicate compromise – embodied in FISA and more generally in Title V of the National Security Act of 1947, 50 U.S.C. §§ 413-415, and based on the preexisting practice of providing only the intelligence committees with sensitive information regarding intelligence operations – established procedures for keeping Congress "fully and currently informed" of intelligence and intelligence-related activities. Under these procedures, the Intelligence Community provides general, substantive, and, often, classified finished intelligence information to several committees of Congress, but generally provides classified operational information only to the Intelligence committees. Even with regard to the Intelligence Committees, the Director of Central Intelligence and the heads of other intelligence agencies are, under Title V, to provide such information only "to the extent consistent with due regard for the protection from

unauthorized disclosure of classified information relating to sensitive intelligence sources and methods or other exceptionally sensitive matters. 50 U.S.C. §§ 413a(a), 413b(b).

Senator Feingold's reporting proposals would, in sum, distort and damage the effective, longstanding accommodation between the President and Congress, and between the Intelligence and Judiciary Committees, over the handling of classified operational intelligence information within Congress. It is noteworthy that the current leadership of both the House and Senate Judiciary Committees have expressed their approval of the existing accommodation. In a press release dated October 17, 2002, the Chairman of the House Judiciary Committee stated that the existing accommodation provides for "reasonable, limited access, subject to appropriate security procedures, to FISA information through [the House Intelligence Committee]." In addition, your letter of February 27, 2003, to Senators Leahy, Grassley and Specter on FISA matters stated that the existing congressional oversight standards relating to FISA reflect a "careful balance between the need for meaningful oversight and the need for secrecy and information security in the government's efforts to protect this country from foreign enemies." Moreover, you stated that your years of service on both the Senate Judiciary Committee and the Senate Select Committee on Intelligence have led you to conclude that the existing accommodation allows Congress to exercise "appropriate, vigorous, robust and detailed oversight of the FISA process."

Reporting on National Security Letters. The next proposed amendment to S. 113, entitled "Sec. 3. Improvement of Congressional Oversight of Surveillance Activities," would require additional reporting specifically addressing the use of 18 U.S.C. § 2709(e) in the context of requests made to schools and public libraries. We are concerned that a reporting requirement at this level of formality and specificity would unduly increase the risk of public exposure of the information, thereby jeopardizing our counterintelligence and counterterrorism efforts.

Presumption. Another proposal is presumably intended as a substitute for S. 113 and would create a "presumption that certain non-United States persons engaging in international terrorism are agents of foreign powers for purposes of the Foreign Intelligence Surveillance Act of 1978." Under the proposal, the FISC would be instructed that it "may presume" that a non-United States person engaged in international terrorism or activities in preparation therefor "is an agent of a foreign power" as defined in FISA.

By providing that the FISC "may presume" the target is acting for or on behalf of an international terrorist group, the proposal would confer discretion on the FISC without any standards to guide the exercise of that discretion. Accordingly, the effect of the proposal is uncertain. It is conceivable that the FISC (or a reviewing court) would indulge the presumption only where the Government had established probable cause or something near to probable cause that the target in fact was working for or on behalf of a terrorist group. In that event, the proposal would be useless or nearly useless. The unpredictability inherent in the proposal also would significantly reduce its value even if, in the end, the FISC and later courts interpreted it more expansively in any particular case.

Nor do we believe that there is a reason to use a presumption – even a mandatory presumption – instead of the straightforward approach of S. 113 itself. In particular, we see no constitutional benefit likely to arise from the use of a presumption. Our letter of July 31, 2002 (copy attached), which explained the constitutionality of an earlier version of S. 113 (which would have made a lone-wolf terrorist a "foreign power" rather than an "agent of a foreign power") applies equally to the current version of S. 113. We do not believe that the use of a presumption significantly changes the constitutional analysis, nor adds any significant protection to civil liberties, except to the extent that the presumption is read narrowly to mirror current law, in which case the presumption is of little or no value for reasons explained in the previous paragraph.

Discovery. The next proposal would change the standards governing discovery of FISA materials in suppression litigation arising from the use of FISA information in a legal proceeding such as a criminal trial. We strongly object to this proposal. The proposal could harm the national security by inhibiting cooperation between intelligence and law enforcement efforts to stop foreign spies and terrorists. It could deter the Government from using information obtained or derived from FISA in any proceeding – civil, criminal, immigration, administrative, or even internal Executive branch proceedings. These overwhelming and potentially catastrophic costs would be incurred for very little benefit, because current law amply protects individual rights.

It may be helpful to begin by reviewing current law in this area and the ways in which it protects individual rights. Currently, FISA requires high-level approval from the Executive and Judicial branches before the Government conducts a search or surveillance. Each FISA application must contain a certification signed individually and personally by the Director of the FBI (or another high-ranking official accountable to the President) and must be individually and personally approved by the Attorney General or the Deputy Attorney General. 50 U.S.C. §§ 1804(a), 1823(a), 1801(g).[2] Under the statute, the Government must apply to a judge of the FISC for approval before conducting electronic surveillance or physical searches of foreign powers or agents of foreign powers inside the United States. 50 U.S.C. §§ 1804-1805 (electronic surveillance), 1823-1824 (physical searches).[3] Judges of the FISC are selected by the Chief

---

[2] By contrast, any FBI agent or Assistant United States Attorney may apply for a criminal search warrant and such a warrant may be issued by a Federal magistrate judge or a State court judge, neither of whom enjoy the protections of Article III (*e.g.*, life tenure). Fed. R. Crim. P. 41(a). Any Deputy Assistant Attorney General in the Justice Department's Criminal Division may authorize an application for electronic surveillance under title III. 18 U.S.C. § 2516(1).

[3] The only exceptions are for (1) surveillance or searches of communications used exclusively among foreign powers in which there is no substantial likelihood of intercepting a U.S. person's communications, 50 U.S.C. §§ 1802, 1822; (2) surveillance or searches conducted in emergency situations for 72 hours, after which a court order is required, 50 U.S.C. §§ 1805(f), 1824(e); and (3) testing of surveillance equipment, 50 U.S.C. § 1805(g). See House Report 23.

Justice from among the judges on United States District Courts, who as United States district judges are protected by Article III of the Constitution. 50 U.S.C. §§ 1803(a), 1822(c).

A second round of judicial review occurs before the Government may use FISA information in any proceeding. The Government must provide notice to the FISA target or other person whose communications were intercepted or whose property was searched before using any information obtained or derived from the surveillance or search in any proceeding against that person "before any court, department, officer, agency, regulatory body, or other authority of the United States." 50 U.S.C. §§ 1806(c), 1825(d). After receiving notice, the person may file a motion to suppress in a United States District Court and may seek discovery of the FISA applications filed by the Government and the authorization orders issued by the FISC. 50 U.S.C. §§ 1806(e)-(f), 1825(f)-(g). Discovery may be granted freely unless the Attorney General personally files an affidavit under oath asserting that discovery would harm the national security. If the Attorney General files such an affidavit, as he has in every case litigated to date, the district judge must review the FISA application and order in camera, without granting discovery, unless "disclosure is necessary to make an accurate determination of the legality" of the search or surveillance. 50 U.S.C. §§ 1806(f), 1825(g). If discovery is granted, the court must impose "appropriate security procedures and protective orders." *Ibid.* No court has ever ordered disclosure.

Congress established this standard for discovery after extensive and careful deliberation in 1978. See H.R. Rep. No. 1283, Part I, 95th Cong., 2d Sess. 90 (1978) (hereinafter House Report); S. Rep. No. 604, 95th Cong., 1st Sess. 57-59 (1977) (hereinafter Senate Judiciary Report); S. Rep. No. 701, 95th Cong., 2d Sess. 62-65 (1978) (hereinafter Senate Intelligence Report). As the 1978 conference report on FISA explains, "an in camera and ex parte proceeding is appropriate for determining the lawfulness of electronic surveillance in both criminal and civil cases . . . [and] the standard for disclosure . . . adequately protects the rights of the aggrieved person." H.R. Rep. No. 1720, 95th Cong., 2d Sess. 32 (1978) (hereinafter Conference Report). As the Senate Judiciary Committee explained in 1978: "The Committee views the procedures set forth in this subsection as striking a reasonable balance between an entirely *in camera* proceeding which might adversely affect the defendants's ability to defend himself, and mandatory disclosure, which might occasionally result in the wholesale revelation of sensitive foreign intelligence information." Senate Judiciary Report at 58.

The proposal would replace FISA's current standard with a new one under which discovery is required unless it "would not assist in determining any legal or factual issue" in the litigation. The "would not assist" standard is inappropriate for use in FISA, in particular, because it is lower than the standard for disclosure of informants' names in ordinary criminal cases. That standard at least requires a balancing of the public interest in confidentiality against the individual defendant's interest in disclosure. As the Supreme Court explained in *McCray* v. *Illinois*, 386 U.S. 300, 311 (1967), extending its earlier decision in *Roviaro* v. *United States*, 353 U.S. 53, 60-61 (1957), "this Court was unwilling to impose any absolute rule requiring disclosure of an informer's identity even in formulating evidentiary rules for federal criminal trials [in

Roviaro]. Much less has the Court ever approached the formulation of a federal evidentiary rule of compulsory disclosure where the issue is the preliminary one of probable cause." Indeed, the "would not assist" standard is lower even than the standards that govern various civil privileges, all of which require some kind of balancing of the interests in disclosure against the interests in confidentiality. See, *e.g.*, *In re Sealed Case*, 121 F.3d 729, 738 (D.C. Cir. 1997). In effect, the "would not assist" standard is the appropriate standard for discovery of *unclassified* and *non-privileged* information, because *no* discovery of any kind is justified unless it would assist the litigation.

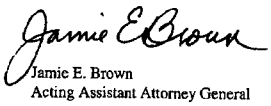
The "would not assist" standard could have very dangerous consequences for the national security. At the outset, we are concerned that the standard could lead to discovery being granted in nearly every case, because it is extremely hard to prove the negative fact that disclosure "would not assist" in any way. Such routine disclosure could be catastrophic: FISA applications contain some of the Government's most sensitive national security information, including information concerning human intelligence sources, sophisticated technical collection methods, and the details of ongoing investigations. Given the enormous sensitivity of that information, when the Attorney General personally files an affidavit under oath asserting that disclosure would harm the national security, ordering disclosure unless it "would not assist" in any way is inappropriate. In view of the protections in FISA and the requirement of an affidavit filed personally by the Attorney General, the "necessary" standard of current law should be retained.

Indeed, precisely because it may lead to discovery in virtually every case, the proposal would create an incentive for the Government to withhold sensitive information from its FISA applications. Under the "would not assist" standard, the Government might have to choose between excluding sensitive information from an application and risking a denial of search and surveillance authority from the FISC, or including the sensitive information and risking public disclosure of that information. Thus, the proposal could fundamentally alter the relationship between the Government and the FISC and could eviscerate the significance of the FISC's careful information security procedures, which are designed to give the Government confidence that full disclosure to the FISC will not result in a compromise of sensitive information.

Since the Government can never completely sanitize a FISA application, the "would not assist" standard would also create strong incentives to avoid suppression litigation and the expanded risk of discovery. That means the Government would lean away from prosecution of a FISA target, even where that was the best way to protect the country. It would thereby reduce the Government's ability to keep the country safe, distorting the vital tactical judgments that must be made. Indeed, the proposal would inhibit more than just prosecutions. In keeping with the scope of FISA's suppression remedy, the proposal would limit the use of FISA information in *any* proceeding, including immigration proceedings, or even in internal adjudications of security clearances under Executive Order 12968. Here again the Government would face a difficult choice between using FISA information to protect national security and risking disclosure of the information as the cost of doing so.

We appreciate your continuing leadership in ensuring that the Department of Justice and other Federal agencies have the authority they need to combat terrorism effectively. Please do not hesitate to contact me if I can be of further assistance. The Office of Management and Budget has advised us that from the perspective of the Administration's program, there is no objection to submission of this letter.

Sincerely,



Jamie E. Brown
Acting Assistant Attorney General

Enclosures:

Letter from Assistant Attorney General Daniel J. Bryant to the Honorable Bob Graham and the Honorable Richard C. Shelby (July 31, 2002)

Letter from Acting Assistant Attorney General Jamie E. Brown to the Honorable Orrin G. Hatch (March 5, 2003)

cc: The Honorable Patrick J. Leahy
Ranking Minority Member

LETTER FROM JAMIE E. BROWN, ACTING ASSISTANT ATTORNEY GENERAL, U.S. DEPARTMENT OF JUSTICE, DATED MARCH 5, 2003, TO THE HONORABLE ORRIN HATCH, CHAIRMAN, COMMITTEE ON THE JUDICIARY, UNITED STATES SENATE

U.S. Department of Justice

Office of Legislative Affairs

Washington, D.C. 20530

March 5, 2003

The Honorable Orrin G. Hatch
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

This is in response to your request for the Administration's views on S. 113, a bill "[t]To exclude United States persons for the definition of 'foreign power' under the Foreign Intelligence Surveillance Act of 1978 relating to international terrorism."

The Administration supports enactment of the bill, which makes clear that a non-United States person who is engaged in international terrorism or activities in preparation therefor, even if not known to be affiliated with an international terrorist group, falls within the definition of "foreign power" under the Foreign Intelligence Surveillance Act ("FISA"). This amendment to the FISA will strengthen the ability of the United States Government to protect the American people against terrorism.

The Administration understands that amendments may be offered to S. 113 that would amend the FISA in other ways. The Administration is not asking for additional authorities through amendments to FISA other than the amendment contained in S. 113 as introduced, at this time. We appreciate your continuing leadership in ensuring that the Department of Justice and other Federal agencies have the authority they need to combat terrorism effectively.

Sincerely,

Jamie E. Brown

Jamie E. Brown
Acting Assisting Attorney General

cc: The Honorable Patrick J. Leahy
Ranking Minority Member

LETTER FROM DANIEL J. BRYANT, ASSISTANT ATTORNEY GENERAL, U.S. DEPARTMENT OF JUSTICE, DATED JULY 31, 2002, TO THE HONORABLE BOB GRAHAM, CHAIRMAN, SELECT COMMITTEE ON INTELLIGENCE, UNITED STATES SENATE, AND THE HONORABLE RICHARD C. SHELBY, VICE-CHAIRMAN, SELECT COMMITTEE ON INTELLIGENCE, UNITED STATES SENATE

U.S. Department of Justice

Office of Legislative Affairs

Washington, D.C. 20530

July 31, 2002

The Honorable Bob Graham
Chairman
Select Committee on Intelligence
United States Senate
Washington, D.C. 20510

The Honorable Richard C. Shelby
Vice-Chairman
Select Committee on Intelligence
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman and Mr. Vice Chairman:

The letter presents the views of the Justice Department on S. 2586, a bill "[t]o exclude United States persons from the definition of 'foreign power' under the Foreign Intelligence Surveillance Act of 1978 relating to international terrorism." The bill would extend the coverage of the Foreign Intelligence Surveillance Act ("FISA") to individuals who engage in international terrorism or activities in preparation therefor without a showing of membership in or affiliation with an international terrorist group. The bill would limit this type of coverage to non-United States persons. The Department of Justice supports S. 2586.

We note that the proposed title of the bill is potentially misleading. The current title is "To exclude United States persons from the definition of 'foreign power' under the Foreign Intelligence Surveillance Act of 1978 relating to international terrorism." A better title, in keeping with the function of the bill, would be something along the following lines: "To expand the Foreign Intelligence Surveillance Act of 1978 ('FISA') to reach individuals other than United States persons who engage in international terrorism without affiliation with an international terrorist group."

Additionally, we understand that a question has arisen as to whether S. 2586 would satisfy constitutional requirements. We believe that it would.

FISA allows a specially designated court to issue an order approving an electronic surveillance or physical search, where a significant purpose of the surveillance or search is "to obtain foreign intelligence information." *Id.* §§ 1804(a)(7)(B), 1805(a). Given this purpose, the court makes a determination about probable cause that differs in some respects from the determination ordinarily underlying a search warrant. The court need not find that there is probable cause to believe that the surveillance or search, in fact, will lead to foreign intelligence information, let alone evidence of a crime, and in many instances need not find probable cause to believe that the target has committed a criminal act. The court instead determines, in the case of electronic surveillance, whether there is probable cause to believe that "the target of the electronic surveillance is a foreign power or an agent of a foreign power," *id.* § 1805(a)(3)(A), and that each of the places at which the surveillance is directed "is being used, or about to be used, by a foreign power or an agent of a foreign power," *id.* § 1805(a)(3)(B). The court makes parallel determinations in the case of a physical search. *Id.* § 1824(a)(3)(A), (B).

The terms "foreign power" and "agent of a foreign power" are defined at some length, *id.* § 1801(a), (b), and specific parts of the definitions are especially applicable to surveillances or searches aimed at collecting intelligence about terrorism. As currently defined, "foreign power" includes "a *group* engaged in international terrorism or activities in preparation therefor," *id.* § 1801(a)(4) (emphasis added), and an "agent of a foreign power" includes any person who "knowingly engages in sabotage or international terrorism or activities that are in preparation therefor, for or on behalf of a foreign power," *id.* § 1801(b)(2)(C). "International terrorism" is defined to mean activities that

> (1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State;
>
> (2) appear to be intended--
>
> (A) to intimidate or coerce a civilian population;
>
> (B) to influence the policy of a government by intimidation or coercion; or
>
> (C) to affect the conduct of a government by assassination or kidnapping; and
>
> (3) occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

Id. § 1801(c).

S. 2586 would expand the definition of "foreign power" to reach persons who are involved in activities defined as "international terrorism," even if these persons cannot be shown to be agents of a "group" engaged in international terrorism. To achieve this expansion, the bill would add the following italicized words to the current definition of "foreign power": "*any person other than a United States person who is, or* a group *that is,* engaged in international terrorism or activities in preparation therefor."

The courts repeatedly have upheld the constitutionality, under the Fourth Amendment, of the FISA provisions that permit issuance of an order based on probable cause to believe that the target of a surveillance or search is a foreign power or agent of a foreign power. The question posed by S. 2586 would be whether the reasoning of those cases precludes expansion of the term "foreign power" to include individual international terrorists who are unconnected to a terrorist group.

The Second Circuit's decision in *United States v. Duggan*, 743 F.2d 59 (2d Cir. 1984), sets out the fullest explanation of the "governmental concerns" that had led to the enactment of the procedures in FISA. To identify these concerns, the court first quoted from the Supreme Court's decision in *United States v. United States District Court*, 407 U.S. 297, 308 (1972) ("*Keith*"), which addressed "domestic national security surveillance" rather than surveillance of foreign powers and their agents, but which specified the particular difficulties in gathering "security intelligence" that might justify departures from the usual standards for warrants: "[Such intelligence gathering] is often long range and involves the interrelation of various sources and types of information. The exact targets of such surveillance may be more difficult to identify than in surveillance operations against many types of crime specified in Title III [dealing with electronic surveillance in ordinary criminal cases]. Often, too, the emphasis of domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the government's preparedness for some possible future crisis or emergency. Thus the focus of domestic surveillance may be less precise than that directed against more conventional types of crime." *Duggan*, 743 F.2d at 72 (*quoting Keith*, 407 U.S. at 322). The Second Circuit then quoted a portion of the Senate Committee Report on FISA: "[The] reasonableness [of FISA procedures] depends, in part, upon an assessment of the difficulties of investigating activities planned, directed, and supported from abroad by foreign intelligence services and foreign-based terrorist groups. . . . Other factors include the international responsibilities of the United States, the duties of the Federal Government to the States in matters involving foreign terrorism, and the need to maintain the secrecy of lawful counterintelligence sources and methods." *Id.* at 73 (*quoting* S. Rep. No. 95-701, at 14-15, *reprinted in* 1978 U.S.C.C.A.N. 3973, 3983) ("Senate Report"). The court concluded:

> Against this background, [FISA] requires that the FISA Judge find probable cause to believe that the target is a foreign power or an agent of a foreign power, and that the place at which the surveillance is to be directed is being used or is about to be used by a foreign power or an agent of a foreign power; and it requires him to find that the application meets the requirements of [FISA]. These requirements make it reasonable to dispense with a requirement that the FISA Judge find

> probable cause to believe that surveillance will in fact lead to the gathering of foreign intelligence information.

Id. at 73. The court added that, *a fortiori*, it "reject[ed] defendants' argument that a FISA order may not be issued consistent with the requirements of the Fourth Amendment unless there is a showing of probable cause to believe the target *has committed a crime*." *Id.* at n.5. *See also, e.g., United States v. Pelton*, 835 F.2d 1067, 1075 (4th Cir. 1987); *United States v. Cavanagh*, 807 F.2d 787, 790-91 (9th Cir. 1987) (per then-Circuit Judge Kennedy); *United States v. Nicholson*, 955 F. Supp. 588, 590-91 (E.D. Va. 1997).

We can conceive of a possible argument for distinguishing, under the Fourth Amendment, the proposed definition of "foreign power" from the definition approved by the courts as the basis for a determination of probable cause under FISA as now written. According to this argument, because the proposed definition would require no tie to a terrorist group, it would improperly allow the use of FISA where an ordinary probable cause determination would be feasible and appropriate – where a court could look at the activities of a single individual without having to assess "the interrelation of various sources and types of information," *see Keith*, 407 U.S. at 322, or relationships with foreign-based groups, *see Duggan*, 743 F.2d at 73; where there need be no inexactitude in the target or focus of the surveillance, *see Keith*, 407 U.S. at 322; and where the international activities of the United States are less likely to be implicated, *see Duggan*, 743 F.2d at 73. However, we believe that this argument would not be well-founded.

The expanded definition still would be limited to collecting foreign intelligence for the "international responsibilities of the United States, [and] the duties of the Federal Government to the States in matters involving foreign terrorism." *Id.* at 73 (*quoting* Senate Report at 14). The individuals covered by S. 2586 would not be United States persons, and the "international terrorism" in which they would be involved would continue to "occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum." 50 U.S.C. § 1801(c)(3). These circumstances would implicate the "difficulties of investigating activities planned, directed, and supported from abroad," just as current law implicates such difficulties in the case of foreign intelligence services and foreign-based terrorist groups. *Duggan*, 743 F.2d at 73 (*quoting* Senate Report at 14). To overcome those difficulties, a foreign intelligence investigation "often [will be] long range and involve[] the interrelation of various sources and types of information." *Id.* at 72 (*quoting Keith*, 407 U.S. at 322). This information frequently will require special handling, as under the procedures of the FISA court, because of "the need to maintain the secrecy of lawful counterintelligence sources and methods." *Id.* at 73 (*quoting Keith*, 407 U.S. at 322). Furthermore, because in foreign intelligence investigations under the expanded definition "[o]ften . . . the emphasis . . . [will be] on the prevention of unlawful activity or the enhancement of the government's preparedness for some possible future crisis or emergency," the "focus of . . . surveillance may be less precise than that directed against more conventional types of crime." *Id.* at 73 (*quoting Keith*, 407 U.S. at 322). Therefore, the same interests and considerations that support the constitutionality of FISA as it now stands would provide the constitutional justification for the S. 2586.

Indeed, S. 2586 would add only a modest increment to the existing coverage of the statute. As the House Committee Report on FISA suggested, a "group" of terrorists covered by current law might be as small as two or three persons. H.R. Rep. No. 95-1283, at pt. 1, 74 and n.38 (1978). The interests that the courts have found to justify the procedures of FISA are not likely to differ appreciably as between a case involving such a group of two or three persons and a case involving a single terrorist.

The events of the past few months point to one other consideration on which courts have not relied previously in upholding FISA procedures – the extraordinary level of harm that an international terrorist can do to our Nation. The touchstone for the constitutionality of searches under the Fourth Amendment is whether they are "reasonable." As the Supreme Court has discussed in the context of "special needs cases," whether a search is reasonable depends on whether the government's interests outweigh any intrusion into individual privacy interests. In light of the efforts of international terrorists to obtain weapons of mass destruction, it does not seem debatable that we could suffer terrible injury at the hands of a terrorist whose ties to an identified "group" remained obscure. Even in the criminal context, the Court has recognized the need for flexibility in cases of terrorism. *See Indianapolis v. Edmond*, 531 U.S. 32, 44 (2000) ("the Fourth Amendment would almost certainly permit an appropriately tailored roadblock set up to thwart an imminent terrorist attack"). Congress could legitimately judge that even a single international terrorist, who intends "to intimidate or coerce a civilian population" or "to influence the policy of a government by intimidation or coercion" or "to affect the conduct of a government by assassination or kidnapping," 50 U.S.C. § 1801(c)(2), acts with the power of a full terrorist group or foreign nation and should be treated as a "foreign power" subject to the procedures of FISA rather than those applicable to warrants in criminal cases.

Thank you for the opportunity to present our views. Please do not hesitate to call upon us if we may be of additional assistance. The Office of Management and Budget has advised us that from the perspective of the Administration's program, there is no objection to submission of this letter.

Sincerely,

for Patrick A. O'Brien, DOJ

Daniel J. Bryant
Assistant Attorney General

cc: The Honorable Charles E. Schumer
The Honorable Jon L. Kyl

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, for holding this hearing on Sections 206 and 215 of the USA PATRIOT Act. These are some of the more controversial sections of the bill that up for renewal consideration. They are controversial because of the extraordinary extent of virtually unchecked powers they allow the government to use to invade the privacy of individuals. Section 215 is particularly disturbing, given its breadth of authority it allows for law enforcement officers to obtain private records on no more that representation that it is relevant to foreign intelligence or international terrorism for espionage.

And even though section 505 of the PATRIOT Act is not under a sunset, you really can't talk about the problems with 215 without discussing the same problems with 505. Section 505 allows a host of private records and information to be obtained through the issuance by line level officers of National Security Letters (NSL's)on the mere representation they are relevant to an investigation of foreign intelligence, international terrorism, or espionage. There need be no crime, no probable cause, no reason to believe, no credible or particular facts—just a representation in the case of 215, and the FISA court has no choice but to issue the order for the production of the records. And in the case of NSL's, there is no court issuance or oversight—just the line officer's issuance, in terms of the requirements of the law.

For both 215 and 505, all of this is done in secrecy with no explicit right to challenge the orders and with permanent gag orders on the keepers of the records sought, even to the extent of consulting with an attorney. And with our liberalized information sharing rules, the information obtained can be distributed all over town. This means your neighbors who are law enforcement agents may know a lot more about your private medical, organizational affiliation, reading and video viewing activities than you ever imagined.

With respect to section 206, FISA roving wiretaps, I have often noted the difficulties I see. Again, under the law, no crime need even be alleged, and under the "John Doe" wiretap, no person or particular device need be shown, and in either case, no effort has to be made to ascertain whether the target is actually using the device before communications can be intercepted. And, again, all of this is in secret in a secret court with limited oversight and reporting requirements when compared to criminal wiretap processes. Department of Justice witnesses often use the powers extended on the criminal court side to justify the same powers on the FISA side. However, they don't call for the same oversight and reporting requirements as on the criminal side, and I think that's where we need to pay a lot more attention in considering renewal of these powers.

So, Mr. Chairman, I look forward to the testimony of our witnesses for enlightenment on why we should consider renewing these extraordinary powers and under what circumstances and conditions. And I look forward to working with you on implementing their recommendations. Thank you.

PREPARED STATEMENT OF THE HONORABLE JOHN CONYERS, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN, AND RANKING MEMBER, COMMITTEE ON THE JUDICIARY

Today we will hear testimony on two of the most controversial sections of the PATRIOT Act. I look forward to hearing why the Justice Department must have these provisions reauthorized wholesale without any safeguards put in place to make sure that rights of suspects are not abused.

Section 206 creates roving "John Doe" wire taps. We will most likely hear testimony today that this provision is already widely used in criminal investigations. However, I am unaware of a court sanctioning a roving wiretap without a clearly identified target. I hope to hear where exactly this authority is coming from to better understand how the Justice Department is using its new authority. I also expect the Justice Department to explain why it believes it should be able to use criminal investigation techniques in intelligence investigations, without supplying the parcel of rights and procedures that have always gone along with those techniques.

Section 215 allows the government to secretly get any thing from any business only upon the showing of relevance to a terror or intelligence information. The Justice Department, in its usual shroud of secrecy, refuses to explain how this section has been used. It will only confirm that it has been used 35 times, and not against libraries. This information comes on the eve of the sunset, after three years of press-

ing national security that required a secret classification. Without more information, I say: too little, too late.

While National Security Letters have been suspiciously left off this Committee's oversight list, I hope to hear from our panelists today about their use. It appears from a redacted FOIA request that this provision has been used hundreds of times. The less-famous brother of Section 215, national security letters are unusually dangerous because in addition to adding a complete gag order on the recipient, they are issued without any oversight from even the FISA court. Because the Justice Department admits to getting information from libraries, I suspect that National Security Letters may be the source, and must have more information about their use as we look at the PATRIOT Act.

Finally, I would like to publicly reiterate my concern that the Judiciary Committee has left many important terror-related policies off its oversight schedule this year. From the practice of rendition, to the abuse of the material witness statute, to unsuccessful racial profiling, this Committee is ignoring the most pressing matters within its jurisdiction. We cannot limit our oversight to the few sections of the U.S. code that will expire at the end of the year. Clearly, the Justice Department has shifted the weight of its terror pursuit to other authorities, or even in the absence of lawful authority at all. If we are truly going to do our constitutional duty of overseeing the executive's use of criminal and intelligence laws, we must look at these issues.

REDACTED DOCUMENT ACLU RECEIVED IN RESPONSE TO A REQUEST UNDER THE FREEDOM OF INFORMATION ACT TO DISCLOSE ACTIVITY RELATED TO TRANSACTIONAL RECORDS NATIONAL SECURITY LETTERS ISSUED SINCE OCTOBER 26, 2001

SECRET

Transactional Records NSLs Since 10/26/2001

Project Number	*NSL to Field Date*
[redacted]	[redacted]

ALL INFORMATION CONTAINED HERE IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

b1

(S)

CLASSIFIED DECISIONS FINALIZED
BY DEPARTMENT REVIEW COMMITTEE (DRC)
DATE: 1-24-03 ACLU 62033 CK/CH
CA # 02-CV-2077

Tuesday, January 21, 2003

Page 1 of 6

Dervied From: G-3
Declassify on: X1

SECRET

JAN 22 2003 ACLU 62033
CLASSIFIED BY: CK/CH
REASON: 1.5 (C)
DECLASSIFY ON: X1
CA # 02-CV-2077

38

~~SECRET~~

Project Number *NSL to Field Date*

[redacted]

b1

(S)

Derived From: G-3
Declassify on: X1

~~SECRET~~

SECRET

Project Number	NSL to Field Date
[redacted]	[redacted]

b1

(S)

Derived From: G-3
Declassify on: X1

SECRET

40

~~SECRET~~

Project Number *NSL to Field Date*

[redacted]

(S) b1

Tuesday, January 21, 2003 *Page 4 of 6*

Dervied From: G-3
Declassify on: X1
~~SECRET~~

41

SECRET

Project Number *NSL to Field Date*

[redacted]

b1

(S)

Tuesday, January 21, 2003

Page 5 of 6

Derived From: G-3
Declassify on: X1

SECRET

42

SECRET

Project Number	NSL to Field Date
[redacted]	[redacted]
Grand Total:	[redacted]

(S) b1

(S)

Derived From: G-3
Declassify On: X1

SECRET

SECRET

43

LETTER FROM WILLIAM E. MOSCHELLA, ASSISTANT ATTORNEY GENERAL, U.S. DEPARTMENT OF JUSTICE TO THE HONORABLE RICHARD B. CHENEY, PRESIDENT OF THE SENATE, UNITED STATES SENATE

U. S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

April 1, 2005

The Honorable Richard B. Cheney
President of the Senate
United States Senate
Washington, D.C. 20510

Dear Mr. President:

This report is submitted pursuant to the Foreign Intelligence Surveillance Act of 1978, Title 50, United States Code, Section 1807, as amended.

During calendar year 2004, 1,758[1] applications were made to the Foreign Intelligence Surveillance Court for electronic surveillance and physical search. The 1,758 applications include applications made solely for electronic surveillance, applications made solely for physical search, and combined applications requesting authority for electronic surveillance and physical search simultaneously. The Court approved 1,754 applications.

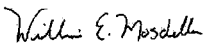
The Government withdrew three of the 1,758 applications made to the Court prior to the Court ruling on the applications. The Government later resubmitted one of the three applications, which was approved by the Court as a new application. The Court did not deny, in whole or in part, any application submitted by the Government in 2004.

Section 1807 also requires that the Government report, in addition to the number of applications approved or denied, the number of applications modified by the Court. During calendar

[1] One application, which is reflected in the 1758 applications made to the Court, was approved in 2003 and received a docket number in 2004.

year 2004, the Court made substantive modifications to the Government's proposed orders in 94 applications presented to the Court.

Sincerely,



William E. Moschella
Assistant Attorney General

LETTER FROM WILLIAM E. MOSCHELLA, ASSISTANT ATTORNEY GENERAL, U.S. DEPARTMENT OF JUSTICE TO L. RALPH MECHAM, DIRECTOR, ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS

U.S. Department of Justice
Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

April 30, 2004

Mr. L. Ralph Mecham
Director
Administrative Office of
the United States Courts
Washington, D.C. 20544

Dear Mr. Mecham:

This report is submitted pursuant to the Foreign Intelligence Surveillance Act of 1978, Title 50, United States Code, Section 1807, as amended.

During calendar year 2003, 1727 applications were made to the Foreign Intelligence Surveillance Court for electronic surveillance and physical search. The 1727 applications include applications made solely for electronic surveillance, applications made solely for physical search, and combined applications requesting authority for electronic surveillance and physical search simultaneously. The Court approved, in whole or in part, 1724 applications.

The Court denied four applications. The Government did not appeal any of those decisions.

Of the four applications that the Court denied, two merit additional discussion:

(1) In one case, the Court issued supplemental orders with respect to its denial, and the Government filed with the Court a motion for reconsideration of its rulings. The Court subsequently vacated its earlier orders and granted in part and denied in part the Government's motion for reconsideration. The Government has not appealed that ruling. In 2004, the Court approved a revised application regarding this target that incorporated modifications consistent with the Court's prior order with respect to the motion for reconsideration.

(2) In another case, the Court initially denied the application without prejudice. The Government presented amended orders to the Court later the same day, which the Court approved. Because the Court eventually approved this application, it is included in the 1724 total referenced above.

Section 1807 also requires that the Government report, in addition to the number of applications approved or denied, the number of applications modified by the Court. During calendar year 2003, the Court made substantive modifications to the Government's proposed orders in 79 applications presented to the Court.

Sincerely,

William E. Moschella

William E. Moschella
Assistant Attorney General

FORM NATIONAL SECURITY LETTER FROM THE U.S. DEPARTMENT OF JUSTICE

SECRET

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to
File No

[Drafting] Field Division
[Street Address]
[City, State, Zip]

[Month Date, Year]

[Mr /Mrs.] [COMPANY POINT OF CONTACT]
[TITLE]
[COMPANY]
[STREET ADDRESS]
[CITY, STATE No Zip Code]

Dear [Mr /Mrs] [LAST NAME]:

Under the authority of Executive Order 12333, dated December 4, 1981, and pursuant to Title 18, United States Code (U S.C), Section 2709 (as amended, October 26, 2001), you are hereby directed to provide the Federal Bureau of Investigation

[redacted] b2-2 b7E-1

In accordance with Title 18, U.S.C., Section 2709(b), I certify that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, and that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment of the Constitution of the United States

You are further advised that Title 18, U.S C , Section 2709(c), prohibits any officer, employee or agent of yours from disclosing to any person that the FBI has sought or obtained access to information or records under these provisions.

[redacted] b2 b7E-1

CLASSIFIED DECISIONS FINALIZED BY DEPARTMENT REVIEW COMMITTEE (DRC) DATE: 07-01-2004

CA# 03-2522

CLASSIFIED BY 65179 dmh/bcl/aaw 6/5/2004
REASON: 1.4 (c)
DECLASSIFY ON: X 6/5/2029

Patriot Act II-828

SECRET

DECLASSIFIED BY 65179 dmh/bcl/aaw
ON 8/3/2004

SECRET

[Mr /Mrs] [COMPANY POINT OF CONTACT]

Your cooperation in this matter is greatly appreciated.

Sincerely,

[ADIC/SAC Name]
Assistant Director/Special
Agent in Charge

CLASSIFIED DECISIONS FINALIZED BY
DEPARTMENT REVIEW COMMITTEE (DRC)
DATE: 07-01-2004

CA# 03-2522

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

CLASSIFIED BY 65179 dah/bcs/sew 6/30/2004
REASON: 1.5 (c)
DECLASSIFY ON: 6/30/2029

SECRET

DECLASSIFIED BY 65179 dah/bcs/sew
ON 8/3/2004

Section 2709 Before the Patriot Act

18 U.S.C. § 2709 Counterintelligence access to telephone toll and transactional records

(a) Duty to provide.--A wire or electronic communication service provider shall comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.

(b) Required certification.--The Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director, may--

(1) request the name, address, length of service, and local and long distance toll billing records of a person or entity if the Director (or his designee in a position not lower than Deputy Assistant Director) certifies in writing to the wire or electronic communication service provider to which the request is made that--

(A) the name, address, length of service, and toll billing records sought are relevant to an authorized foreign counterintelligence investigation; and

(B) there are specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801); and

(2) request the name, address, and length of service of a person or entity if the Director (or his designee in a position not lower than Deputy Assistant Director) certifies in writing to the wire or electronic communication service provider to which the request is made that--

(A) the information sought is relevant to an authorized foreign counterintelligence investigation; and

(B) there are specific and articulable facts giving reason to believe that communication facilities registered in the name of the person or entity have been used, through the services of such provider, in communication with--

(i) an individual who is engaging or has engaged in international terrorism as defined in section 101(c) of the Foreign Intelligence Surveillance Act or clandestine intelligence activities that involve or may involve a violation of the criminal statutes of the United States; or

(ii) a foreign power or an agent of a foreign power under circumstances giving reason to believe that the communication concerned international terrorism as defined in section 101(c) of the Foreign Intelligence Surveillance Act or clandestine intelligence activities that involve or may involve a violation of the criminal statutes of the United States. (footnote omitted)

(c) Prohibition of certain disclosure.--No wire or electronic communication service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.

(d) Dissemination by bureau.--The Federal Bureau of Investigation may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

(e) Requirement that certain congressional bodies be informed.--On a semiannual basis the Director of the Federal Bureau of Investigation shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, and the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate, concerning all requests made under subsection (b) of this section.

Section 2709 As Amended By the Patriot Act

18 U.S.C. § 2709 -- Counterintelligence access to telephone toll and transactional records

(a) Duty to provide.--A wire or electronic communication service provider shall comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.

(b) Required certification.--The Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, may--

(1) request the name, address, length of service, and local and long distance toll billing records of a person or entity if the Director (or his designee ~~in a position not lower than Deputy Assistant Director~~) certifies in writing to the wire or electronic communication service provider to which the request is made that--

~~(A)~~ the name, address, length of service, and toll billing records sought are relevant to an authorized foreign ~~counterintelligence~~ investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States; and ~~(B) there are specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801)~~

(2) request the name, address, and length of service of a person or entity if the Director (or his designee ~~in a position not lower than Deputy Assistant Director~~) certifies in writing to the wire or electronic communication service provider to which the request is made that--

~~(A)~~ the information sought is relevant to an authorized ~~foreign counterintelligence~~ investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States.; ~~(B) there are specific and articulable facts giving reason to believe that communication facilities registered in the name of the person or entity have been used, through the services of such provider, in communication with--~~

~~(i) an individual who is engaging or has engaged in international terrorism as defined in section 101(c) of the Foreign Intelligence Surveillance Act or clandestine intelligence activities that involve or may involve a violation of the criminal statutes of the United States; or~~

~~(ii) a foreign power or an agent of a foreign power under circumstances giving reason to believe that the communication concerned international terrorism as defined in section 101(c) of the Foreign Intelligence Surveillance Act or clandestine intelligence activities that involve or may involve a violation of the criminal statutes of the United States.~~

(c) Prohibition of certain disclosure.--No wire or electronic communication service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.

(d) Dissemination by bureau.--The Federal Bureau of Investigation may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

(e) Requirement that certain congressional bodies be informed.--On a semiannual basis the Director of the Federal Bureau of Investigation shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, and the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate, concerning all requests made under subsection (b) of this section.

Section 2709 After Doe v. Ashcroft

2709 -- Counterintelligence access
l and transactional records

(c) wire or electronic communication service
provider request for subscriber information and toll
billing recor ctronic communication transactional
records in its co made by the Director of the Federal
Bureau of Investig n (b) of this section.

(b) Required certificatio e Federal Bureau of
Investigation, or his designee r than Deputy
Assistant Director at Bureau head l Agent in Charge
in a Bureau field office designated b
(1) request the name, address, len cal and
long distance toll billing records of a p Director
(or his designee ~~in a position not lower tha~~
~~Director~~) certifies in writing to the wire or elec
service provider to which the request is made tha
~~(A)~~ the name, address, length of service, and to
records sought are relevant to an authorized ~~foreign~~
~~counterintelligence~~ investigation to protect against
international terrorism or clandestine intelligence activi
provided that such an investigation of a United Sta
not conducted solely on the basis of activities p
first amendment to the Constitution of the U
~~(B) there are specific and articulable fa~~
~~to believe that the person or entity~~ ation
~~sought pertains is a foreign pow~~ oreign
~~power as defined in section~~
~~Surveillance Act of 1978~~ telligence

(2) request the name of service of a person
or entity if the Dire ~~in a position not lower~~
~~than Deputy A~~ ities in writing to the wire or
electronic ce provider to which the request is
made

sought is relevant to an authorized
~~ntelligence~~ investigation to protect against
Terrorism or clandestine intelligence activities,
that such an investigation of a United States person
conducted solely on the basis of activities protected by
the first amendment to the Constitution of the Unit
~~(B) there are specific and articulable facts giv~~
~~to believe that communication facilities re~~
~~name of the person or entity have bee~~
~~services of such provider, in commu~~
~~(i) an individual who is engag~~ in
~~international terrorism as~~ (c) of the
~~Foreign Intelligence S~~ ndestine
~~intelligence activi~~ y involve a
~~violation of the~~ he United States; or
~~(ii) a foreig~~ of a foreign power
~~under~~ reason to believe that the
~~co~~ ned international terrorism as
~~s (c) of the Foreign Intelligence~~
~~or clandestine intelligence activities that~~
~~y involve a violation of the criminal statutes of~~
~~d States.~~

n of certain disclosure.--No wire or electronic
ution service provider, or officer, employee, or agent thereof,
close to any person that the Federal Bureau of Investigation
or obtained access to information or records under this

bureau.--The Federal Bureau of Investigation
may n and records obtained under this section
only as p approved by the Attorney General for
foreign intelli foreign counterintelligence
investigations co ral Bureau of Investigation, and,
with respect to dissem cy of the United States, only if
such information is clear thorized responsibilities of
such agency.

(e) Requirement that certain co informed.--On a
semiannual basis the Director of the Fe tigation
shall fully inform the Permanent Select Co se of the
House of Representatives and the Select Com of
the Senate, and the Committee on the Judiciary
Representatives and the Committee on the Judiciary
concerning all requests made under subsection (b) of this