AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

REAUTHORIZATION OF THE PATRIOT ACT

HEARING

BEFORE THE

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

MARCH 9, 2011

Serial No. 112–14

Printed for the use of the Committee on the Judiciary

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

U.S. GOVERNMENT PRINTING OFFICE

65–076 PDF WASHINGTON : 2011

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) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

LAMAR SMITH, Texas, *Chairman*

F. JAMES SENSENBRENNER, JR., Wisconsin
HOWARD COBLE, North Carolina
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
DANIEL E. LUNGREN, California
STEVE CHABOT, Ohio
DARRELL E. ISSA, California
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio
TED POE, Texas
JASON CHAFFETZ, Utah
TOM REED, New York
TIM GRIFFIN, Arkansas
TOM MARINO, Pennsylvania
TREY GOWDY, South Carolina
DENNIS ROSS, Florida
SANDY ADAMS, Florida
BEN QUAYLE, Arizona

JOHN CONYERS, JR., Michigan
HOWARD L. BERMAN, California
JERROLD NADLER, New York
ROBERT C. "BOBBY" SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
PEDRO PIERLUISI, Puerto Rico
MIKE QUIGLEY, Illinois
JUDY CHU, California
TED DEUTCH, Florida
LINDA T. SÁNCHEZ, California
DEBBIE WASSERMAN SCHULTZ, Florida

SEAN MCLAUGHLIN, *Majority Chief of Staff and General Counsel*
PERRY APELBAUM, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

F. JAMES SENSENBRENNER, JR., Wisconsin, *Chairman*
LOUIE GOHMERT, Texas, *Vice-Chairman*

BOB GOODLATTE, Virginia
DANIEL E. LUNGREN, California
J. RANDY FORBES, Virginia
TED POE, Texas
JASON CHAFFETZ, Utah
TIM GRIFFIN, Arkansas
TOM MARINO, Pennsylvania
TREY GOWDY, South Carolina
SANDY ADAMS, Florida
BEN QUAYLE, Arizona

ROBERT C. "BOBBY" SCOTT, Virginia
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
PEDRO PIERLUISI, Puerto Rico
JUDY CHU, California
TED DEUTCH, Florida
DEBBIE WASSERMAN SCHULTZ, Florida
SHEILA JACKSON LEE, Texas
MIKE QUIGLEY, Illinois

CAROLINE LYNCH, *Chief Counsel*
BOBBY VASSAR, *Minority Counsel*

CONTENTS

MARCH 9, 2011

Page

OPENING STATEMENTS

The Honorable F. James Sensenbrenner, Jr., a Representative in Congress from the State of Wisconsin, and Chairman, Subcommittee on Crime, Terrorism, and Homeland Security 1
The Honorable Robert C. "Bobby" Scott, a Representative in Congress from the State of Virginia, and Ranking Member, Subcommittee on Crime, Terrorism, and Homeland Security 2
The Honorable Lamar Smith, a Representative in Congress from the State of Texas, and Chairman, Committee on the Judiciary 4
The Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan, and Ranking Member, Committee on the Judiciary 5

WITNESSES

Todd M. Hinnen, Acting Assistant Attorney General, National Security Division, Department of Justice
Oral Testimony 8
Prepared Statement 10
Robert S. Litt, General Counsel, Office of the Director of National Intellilgence
Oral Testimony 16
Prepared Statement 18
Nathan A. Sales, Assistant Professor of Law, George Mason University
Oral Testimony 24
Prepared Statement 26
Julian Sanchez, Research Fellow, Cato Institute
Oral Testimony 36
Prepared Statement 38

LETTERS, STATEMENTS, ETC., SUBMITTED FOR THE HEARING

Report by the American Civil Liberties Union (ACLU) submitted by the Honorable Henry C. "Hank" Johnson, Jr., a Representative in Congress from the State of Georgia, and Member, Subcommittee on Crime, Terrorism, and Homeland Security 61

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Prepared Statement of the Honorable Henry C. "Hank" Johnson, Jr., a Representative in Congress from the State of Georgia, and Member, Subcommittee on Crime, Terrorism, and Homeland Security 99
Letter from Debra Burlingame, Co-Founder, and Timothy Killeen, Executive Director, Keep America Safe 101
Letter from J. Adler, National President, the Federal Law Enforcement Officers Association (FLEOA) 102
Letter from Konrad Motyka, President, the Federal Bureau of Investigation Agents Association 105

REAUTHORIZATION OF THE PATRIOT ACT

WEDNESDAY, MARCH 9, 2011

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

The Subcommittee met, pursuant to notice, at 1:30 p.m., in room 2141, Rayburn Office Building, the Honorable F. James Sensenbrenner, Jr. (Chairman of the Subcommittee) presiding.

Present: Representatives Sensenbrenner, Smith, Gohmert, Lungren, Poe, Chaffetz, Griffin, Marino, Gowdy, Adams, Quayle, Scott, Conyers, Johnson, Chu, Wasserman Schultz, and Quigley.

Staff present: (Majority) Caroline Lynch, Subcommittee Chief Counsel; Sarah Allen, Counsel; Arthur Radford Baker, Counsel; Sam Ramer, Counsel; Lindsay Hamilton, Clerk; (Minority) Bobby Vassar, Subcommittee Chief Counsel; Sam Sokol, Counsel; and Veronica Eligan, Professional Staff Member.

Mr. SENSENBRENNER. The Subcommittee will come to order.

And welcome to today's hearing on the reauthorization of the PATRIOT Act. I would like to especially welcome our witnesses and thank you for joining us today.

Presently I am joined by the distinguished Ranking Member and Chairman emeritus of the Subcommittee, Bobby Scott of Virginia. There will be more Members that will be coming later on.

I yield myself 5 minutes for an opening statement.

Today's hearing on the reauthorization of the PATRIOT Act will focus on three provisions set to expire May 27th: section 206, roving authority; section 215, business records; and the "lone wolf" definition.

Last month, Congress approved a 90-day extension of these provisions to ensure their continued use by the intelligence community. The extension also affords this Committee the opportunity to review how these provisions are used and how to assist our national security investigations and to ensure that they are not being misused. The Committee plans to hold an additional hearing later this month on the permanent provisions of the PATRIOT Act.

As the then Chairman of the House Judiciary Committee, I oversaw the enactment of the USA PATRIOT Act in response to the 9/11 terrorist attacks. Title 2 of the act addressed enhanced foreign intelligence and law enforcement surveillance authority. 14 of the 16 sections of that title were made permanent by the 2005 PATRIOT Act reauthorization. The roving wiretap and business

records provisions were extended to December 31st, 2009. Also set to expire on that date was section 6001 of the Intelligence Reform and Terrorist Prevention Act of 2004, which we call IRTPA, the lone wolf definition. Congress did not enact a reauthorization in 2009. Instead the expiring provisions were extended three times, first for 60 days, then for a year, and now for 90 days, and it is time for Congress to reauthorize this law.

Congress should make permanent the lone wolf definition. This provision closes a gap in FISA that if allowed to expire could permit an additional terrorist to slip through the cracks and carry out his plot undetected. It has nothing to do whatsoever with any type of surveillance on these people. That is in other parts of the act.

When FISA was originally enacted in 1978, America was concerned largely with collecting intelligence from foreign nations such as the Soviet Union or terrorist groups like the FARC in Colombia. Therefore, the law authorized intelligence gathering to foreign powers and their agents.

The intelligence landscape has changed dramatically in the last 30 years. Today we are confronted with threats from individuals who may subscribe to certain beliefs but do not belong to a specific terrorist group. Without the lone wolf definition, our surveillance tools will be powerless against this growing threat to America's security.

Section 206 of the PATRIOT Act authorizes the use of roving or multi-point wiretaps for national security and intelligence investigation. This allows the Government to use a single wiretap order to cover any communications device that the target is using or about to use. Without roving wiretap authority, investigators are required to seek a new court order each time a terrorist or spy changes cell phones or computers.

Section 215 of the act allows FISA Courts to issue orders granting the Government access to business records and foreign intelligence, international terrorism, and clandestine intelligence cases. The 2005 reauthorization expanded congressional oversight and added additional procedural requirements and judicial review.

Since the PATRIOT Act was enacted, these provisions have been scrutinized by Congress and have been either unchallenged or found constitutional. The lone wolf definition has never been challenged. Section 206 roving authority has never been challenged. The criminal roving wiretap authority was upheld under the Fourth Amendment to the Constitution by the Ninth Circuit in 1992. Section 215 business records was challenged, but after Congress made changes to that provision in the 2005 reauthorization, the lawsuit was withdrawn. Each of these provisions is integral to defending America against enemy nations, terrorist groups, and individual terrorists and must be kept intact.

I wish to welcome our witnesses and thank you for joining us today.

And now I would like to recognize for his opening statement the gentleman from Virginia, Mr. Scott, who is the Ranking Member of the Subcommittee.

Mr. SCOTT. Thank you, Mr. Chairman. I thank you for holding this hearing on the reauthorization of the expiring provisions of the USA PATRIOT Act. We are here on a temporary 3-month exten-

sion. The House passed a much longer extension. I am pleased that it was shorter extension, but I remain opposed to the extension of these provisions without changes to them to better ensure the rights of innocent Americans are not trampled upon.

Three sections scheduled to sunset are deeply troubling. Section 215 of the PATRIOT Act authorizes the Government to secretly obtain any tangible thing so long as it provides, in an ex parte proceeding, a statement of facts showing that there is reasonable grounds to believe that the tangible things are relevant to a foreign intelligence, international terrorism, or espionage investigation. No showing of probable cause, no direct connection to a foreign power or agent is needed, and any tangible thing includes business records, library records, tax records, educational records, medical records, or anything else.

Before the enactment of section 215, only specific types of records were subject to such orders and the Government had to show specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power. While these extraordinary powers were authorized and defended under the rubric that they are necessary to protect us from patriotism, the secret dragnet style approach allows the Government to review personal records even if there is no specific and articulable facts giving reason to believe that the individual targeted had anything to do with terrorism. The justification of these extraordinary powers is to protect us from terrorism. Congress should either ensure that things collected with this power have a meaningful connection to at least suspected terrorism or the provision should expire.

Section 206 provides for roving wiretaps, including a John Doe roving wiretap, which permit the Government to secretly tap phones it believes a non-U.S. person may use. The order may be against any phone, including a phone of a neighbor if the person has visited before and used the phone whether or not he is determined to be using the phone again or if the officials represent to a judge, on an ex parte basis, that the person is evasive in the use of phones.

Section 6001, the so-called "lone wolf" provision, permits secret intelligence gathering of non-U.S. persons in the U.S. even if they are not affiliated with a foreign government or terrorist organization. We have traditionally limited this kind of Government power to situations that involve agents of foreign governments or foreign terrorist organizations. With the necessity for business people to operate in a global economy and the frequency with which American citizens interact with people from around the world, the risk that this provision poses for ordinary activities of such Americans to be subject to spying is unacceptable, especially since the Government testimony indicates that the lone wolf provision is rarely, if ever, used. And even if there was a case where there was good cause for the Government to keep tabs on such people, there is no reason to jeopardize the safeguards that protect the traditional rights and freedoms of Americans when we can pursue such persons under existing authorities which allow emergency warrants and just about any other Government action that is reasonably based on pursuing a suspect.

It is encouraging that there was significant bipartisan opposition to the extension of these PATRIOT Act provisions. It shows a healthy skepticism of unrestrained Government power to spy on people in the United States. We need to restore our traditional respect for the right of every individual to be secure from unchecked Government intrusion. I hope that we can arrive at ways of doing so in our review of these authorities. We did so before under your leadership, Mr. Chairman, when we arrived at a version of the PATRIOT Act when it was originally passed that every Member of the House Judiciary Committee voted for, and I am confident that we can again under your leadership do the same thing.

Thank you and I yield back.

Mr. SENSENBRENNER. The time of the gentleman has expired.

The Chair now recognizes the Chairman of the Committee, the gentleman from Texas, Mr. Smith.

Mr. SMITH. Thank you, Mr. Chairman.

The September 11th attack—and this September 11th marks the 10-year anniversary of the worst terrorist attack in U.S. history. America is fortunate not to have suffered another attack of such magnitude and devastation in the past decade. This does not mean that the terrorists have given up their plot to destroy America or that we should no longer be prepared for another large-scale attack. As we have seen in recent years, the absence of a major attack does not mean that America is secure.

To avoid detection, terrorists have shifted their tactics away from complex, coordinated attacks by a group of terrorists to smaller, individualized plots by rogue terrorists.

On Christmas Day 2009, a foreign terrorist from Nigeria attempted to detonate a bomb hidden under his clothes on a plane on the way to Detroit.

Last spring, a radicalized American citizen from Pakistan tried to explode a car bomb in Times Square.

Plots to attack both the Washington, D.C. Metro and New York subway systems have also been thwarted.

And just 2 weeks ago, a 20-year-old student from Saudi Arabia was arrested in my home State of Texas for attempting to use weapons of mass destruction. Khalid Aldawasari entered the United States in 2008 on a student visa to complete English language training, but in reality, he came to the United States to carry out violent jihad on innocent Americans. Aldawasari had been planning his bombing plot for years, even seeking out a particular scholarship to attend school in the U.S. while carrying out this plot. According to prosecutors, Aldawasari obtained two of the three chemicals needed for a bomb over the last 3 months and had attempted to buy the third. He had also researched potential targets, including the Dallas residence of former President George W. Bush, several dams in Colorado and California, and the homes of three former military guards who served in Iraq.

The PATRIOT Act was enacted to prevent both large-scale attacks and terrorist plots by individual terrorists acting alone like the one in Dallas. Unfortunately, the myths surrounding the PATRIOT Act often overshadow the truth, but this is not "Law and Order" or some criminal justice show painting the PATRIOT Act as a tool of "Big Brother" just for their ratings. This is the real world

where we must address the real threat from foreign terrorists. As we review these expiring provisions, Congress must set aside fiction and focus on the facts.

The three expiring national security provisions that Congress will consider this year are both constitutional and common sense. For example, the roving wiretap provision allows intelligence officials, after receiving approval from a Federal court, to conduct surveillance on terrorist suspects regardless of how many communication devices they use. We know terrorists use many forms of communication to conceal their plots, including disposable cell phones.

Roving wiretaps are nothing new. Domestic law enforcement agencies have had roving authority for criminal investigations since 1986. If we can use this authority to track down a drug lord, why shouldn't we also use it to prevent a terrorist attack?

The business records provision allows the FBI to access tangible items, including business records in foreign intelligence, international terrorism, and espionage cases. Again, this provision requires the approval of a Federal judge. That means the FBI must prove to a Federal judge that the documents are needed as part of a legitimate national security investigation.

The third provision amends the legal definition of an agent of a foreign power to include a lone wolf provision. National security laws allow intelligence gathering on foreign governments, terrorist groups, and their agents. But what about a foreign terrorist who either acts alone or cannot be immediately tied to a terrorist organization? The lone wolf definition simply brings our national security laws into the 21st century to allow our intelligence officials to answer the modern day terrorist threat.

We cannot fight terror in this century with the tools of the last century. Congress must reauthorize these important national security laws. We simply cannot afford to leave our intelligence community without the resources it needs to dismantle terrorist organizations, identify threats from both groups and individuals, and interrupt terrorist plots of all sizes.

Mr. Chairman, let me say in conclusion that I personally appreciate all the work that you have done on the PATRIOT Act. You were the Chairman of this Committee when it first passed. You have conducted oversight of the PATRIOT Act in the past. You are continuing to do so today. And I hope the results of all of our efforts will be to reassure individuals that these three provisions need to be extended and that they are doing a lot to protect the lives of Americans today.

I yield back.

Mr. SENSENBRENNER. The Chair recognizes the most recent Chairman emeritus of the Committee, the gentleman from Michigan, Mr. Conyers.

Mr. CONYERS. I want to thank the most senior Chairman emeritus for recognizing me and to let you know that I do not know if you are, as our present Chairman, about to move the discussion of the PATRIOT Act from the Constitution Subcommittee to the Crime Subcommittee. That is your prerogative. And I noticed that is what the senior Chairman emeritus did when he was Chair. And here we are doing it again.

Now, it is my understanding that many Members in the Subcommittee opposed this 3-month extension. They wanted it longer. I am satisfied with 3 months and apparently so is the other body.

So we are here today. And I guess no one else has to recount all the horror stories of terrorism, incidents of terrorists, people arrested for terrorism and not yet prosecuted. That has all been done. But I am not sure if that is the main issue that surrounds us today because the most basic questions raised to me are what intrusions on our freedom and privacy will we accept, how much will we accept in this fight against terrorism. I noticed that the Chairmen of the Subcommittee and the full Committee have failed to even comment on that, which I consider to be the crux of us coming together. It is commented on by one of the witnesses here from the Cato Institute.

What we are trying to do here today is reach a balance between protection and our liberties. I just want to read you what came from a former Senator from Minnesota—Wisconsin: "Of course, there is no doubt that if we lived in a police state, it would be easier to catch terrorists. If we lived in a country that allowed the police to search your home at any time for any reason, if we lived in a country that allowed the Government to open your mail, eavesdrop on your conversations, intercept your email, if we lived in a country that allowed the Government to hold people in jail indefinitely based on what they write or think or based on mere suspicion that they are up to no good, then the Government would, no doubt, discover and arrest more terrorists. But that is not a country which we would want to live in and that would not be a country for which we could, in good conscience, ask our young people to fight and die for. In short, it would not be America." And so it is that set of concerns that to me bring us here today.

And for all of us, I keep remembering that the Chairman's original PATRIOT bill was passed unanimously out of this Committee, and then not so mysteriously substituted in the Rules Committee for a bill that no one had ever seen before. And so it is against that backdrop that I join in welcoming all of the witnesses today for this discussion.

Thank you.

Mr. SENSENBRENNER. The time of the gentleman has expired.

Without objection, Members' opening statements will be made a part of the record.

And also without objection, the Chair will be authorized to declare recesses during votes on the House floor.

It is now my pleasure to introduce today's witnesses.

Todd Hinnen is the Acting Assistant Attorney General for National Security at the Department of Justice. Prior to assuming this position, Mr. Hinnen was the Deputy Assistant Attorney General for Law and Policy at the National Security Division of the Department of Justice. He also has previously served as chief counsel to then Senator Joseph Biden, Jr., and as a director in the National Security Council's Combating Terrorism Directorate and as a trial attorney in the Department of Justice's Computer Crime and Intellectual Property Section.

Mr. Hinnen clerked for Judge Richard Tallman on the Ninth Circuit Court of Appeals and he is a graduate of Amherst College and Harvard Law School.

Robert Litt is the General Counsel in the Office of the Director of National Intelligence. Before joining ODNI, Mr. Litt was a partner with the law firm of Arnold & Porter, LLP. He served as a member of the governing body of the American Bar Association's Criminal Justice Section and is a member of the advisory committee to the standing Committee on Law and National Security.

From 1993 to 1999, Mr. Litt worked at the Department of Justice where he served as the Deputy Assistant Attorney General in the Criminal Division and then as the Principal Associate Deputy Attorney General. His duties at DOJ included FISA applications, covert action reviews, computer security, and other national security matters.

He started his legal career as a clerk for Judge Edward Weinfeld of the Southern District of New York and Justice Potter Stewart of the United States Supreme Court. From 1978 to 1984, he was an assistant U.S. attorney for the Southern District of New York. He also spent 1 year as a special advisor to the Assistant Secretary of State for European and Canadian Affairs.

He holds a B.A. from Harvard college and an M.A. and J.D. from Yale University.

Nathan Sales is an Assistant Professor of Law at the George Mason University School of Law where he teaches national security and administrative law. Prior to coming to George Mason, he was a Deputy Assistant Secretary for Policy Development at the U.S. Department of Homeland Security.

He has previously served as counsel and then senior counsel in the Office of Legal Policy at the U.S. Department of Justice. In 2002, he received the Attorney General's Award for exceptional service for his role in drafting the USA PATRIOT Act.

He graduated from Duke Law School magna cum laude where he joined the Order of the Coif and was research editor of the Duke Law Journal.

He clerked for the Honorable David B. Sentelle of the U.S. Court of appeals for the D.C. Circuit, and from 2003 to 2005, he practiced at the Washington, D.C. law firm of Wiley, Rein & Fielding. He was the John N. Olin Fellow at Georgetown University Law Center in 2005 and 2006.

Julian Sanchez is a research fellow at the Cato Institute who studies the intersection of privacy, technology, and public policy. He has written extensively about surveillance and the intelligence community for publishers across the political spectrum, from National Review to Newsweek and The Nation. As a journalist, Sanchez has covered these same issues as Washington editor of the technology site, Ars Technica, a blogger for the Economist, and an editor for Reason magazine. He studied philosophy and political science at New York University.

Without objection, the witnesses' statements will appear in the record in their entirety. Each witness will be recognized for 5 minutes to summarize their written statement, and the Chair now recognizes Mr. Hinnen.

TESTIMONY OF TODD M. HINNEN, ACTING ASSISTANT ATTORNEY GENERAL, NATIONAL SECURITY DIVISION, DEPARTMENT OF JUSTICE

Mr. HINNEN. Thank you, Mr. Chairman.

Mr. SENSENBRENNER. The Chair may withdraw his recognition of Mr. Hinnen, seeing if we have some votes on the floor. We have three votes on the floor. We will wait until the votes are over with and then I will recognize you for 5 minutes.

The Committee is recessed. Would Members please come back here promptly following the last vote?

[Recess.]

Mr. SENSENBRENNER. The Subcommittee will be in order, and the Chair will re-recognize Mr. Hinnen for 5 minutes.

Mr. HINNEN. Thank you, Mr. Chairman.

Chairman Sensenbrenner, Ranking Member Scott, Ranking Member Conyers, and Members of the Subcommittee, thank you for inviting me to testify today concerning the three provisions of the Foreign Intelligence Surveillance Act currently scheduled to sunset in May: the roving wiretap provision, the lone wolf definition, and the business records provision.

I will make four general observations about these provisions and then discussion each of them briefly.

First, these provisions are constitutional. Two of them, the roving wiretap provision and the business records provision have close analogues in criminal law: Title III roving wiretaps, and grand jury subpoenas. The courts have upheld each of these criminal analogues as constitutional. The lone wolf definition is simply a specific application of FISA surveillance authority which the courts have also upheld as constitutional.

Second, they are important to our ability to conduct effective national security investigations. Allowing them to expire even for a brief time would make America less safe from international terrorism and other foreign threats.

Third, they are subject to robust protections for privacy and civil liberties that involve all three branches of Government. Each requires the Government to make certain showings to an independent court, the FISA Court. Each imposes strict rules governing how the Government handles information regarding United States persons. Each is subject to extensive executive branch oversight, and each is subject to congressional reporting requirements.

Fourth, these authorities have been subject to extensive discussions between Congress and the executive branch, and Congress has already renewed them several times.

My written testimony sets forth a detailed explanation of how each of them works. Let me summarize it briefly.

First, the roving wiretap provision. Ordinarily when the Government demonstrates probable cause that a subject is an agent of a foreign power and is using a facility such as a telephone number, the FISA Court issues two orders. One order is to the Government authorizing the surveillance, and the second order is to the provider, the telephone company, directing it to assist the Government. When we demonstrate to the court that the subject may take steps to thwart surveillance, such as by switching telephone companies, the court can issue a roving order, directing any telephone

company to assist the Government. When the Government identifies the new phone number that the subject is using and initiates surveillance, it must notify the court within 10 days and provide the facts indicating that the subject is using that phone number.

As courts have repeatedly held in the criminal context, a roving order is not a general warrant. The Government may use roving surveillance only against that specific agent of a foreign power and on a specific phone number that person is using. The Government obtains roving authority about 20 times a year on average, generally where the subject is a highly trained foreign intelligence officer or a terrorist with particularly sophisticated tradecraft.

Second, the lone wolf definition permits surveillance when the Government demonstrates probable cause that a subject is engaged in international terrorism, even if the Government does not demonstrate a connection to a terrorist organization. The Government may not use this authority against a United States citizen or lawful permanent resident. Although we have not used this authority to date, it fills an important gap in our collection capabilities. It allows us to collect on an individual engaged in terrorist activity who is inspired by but not a member of a terrorist group.

Third, the business records provision allows the Government to apply to the FISA Court for an order directing the production of tangible things that are relevant to an authorized national security investigation. This authority is analogous to grand jury subpoena authority in criminal cases. In fact, the Government can only obtain records that could be obtained by subpoena in criminal cases. But this authority imposes more demanding requirements on the Government than a criminal subpoena. The Government must demonstrate relevance and obtain an order from an independent court. This provision is used about 40 times per year on average. It has never been used to obtain library circulation records or the titles of books borrowed.

In closing, Mr. Chairman, it is appropriate to discuss these authorities which are so important to our national security and to Americans' privacy and civil liberties, and we appreciate the opportunity to do so. Congress based these provisions on well-established, time-tested authorities in the criminal context and has refined them since they were enacted. All three are on solid constitutional footing. All three are important to protect this country from international terrorism and other foreign threats, and all three are subject to robust protections for privacy and civil liberties. The Department urges Congress to renew them.

I look forward to the Subcommittee's questions.

[The statement of Mr. Hinnen follows:]

Department of Justice

STATEMENT

OF

STATEMENT OF
TODD M. HINNEN
ACTING ASSISTANT ATTORNEY GENERAL
DEPARTMENT OF JUSTICE

BEFORE THE
SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY
COMMITTEE ON THE JUDICIARY
UNITED STATES HOUSE OF REPRESENTATIVES

AT A HEARING ENTITLED
"USA PATRIOT ACT REAUTHORIZATION"

PRESENTED ON
MARCH 9, 2011

Statement of
Todd M. Hinnen
Acting Assistant Attorney General
Department of Justice
Before the
Subcommittee on Crime, Terrorism and Homeland Security
Committee on the Judiciary
United States House of Representatives
At a Hearing Entitled
"USA PATRIOT Act Reauthorization"
Presented on
March 9, 2011

Chairman Sensenbrenner, Ranking Member Scott, and members of the House Judiciary Subcommittee on Crime, Terrorism and Homeland Security, thank you for inviting me to testify today concerning the three provisions of the Foreign Intelligence Surveillance Act ("FISA") that were recently reauthorized but are scheduled to sunset again in May. Two of these provisions have been part of FISA since the USA PATRIOT Act was enacted nearly a decade ago, and the third has been in FISA since 2004. They have all been reauthorized several times since enactment. As you know, we continue to believe these are critical tools for national security investigations that facilitate the collection of vital foreign intelligence and counterintelligence information. Consequently, we strongly support their continued reauthorization. The Attorney General and Director of National Intelligence have written to the leadership of both houses of Congress urging that Congress grant a reauthorization of sufficient duration to provide those charged with protecting our nation with reasonable certainty and predictability.

Today I will briefly describe the three expiring provisions (the "roving" surveillance provision, the "lone wolf" definition, and the "business records" provision), explain how they have typically been used in practice, and identify some of the safeguards that ensure that these authorities are used responsibly.

Roving Surveillance

FISA's "roving" electronic surveillance provision allows the Government to continue surveillance where the target of the surveillance switches from a facility (*e.g.*, a telephone) associated with one service provider (*e.g.*, a telephone company) to a different facility associated with a different provider. This provision, now codified at 50 U.S.C. § 1805(c)(2)(B), was enacted in the USA PATRIOT Act to correspond to roving authority that has applied to law-enforcement surveillance since 1986. *See* 18 U.S.C. § 2518(11).

To explain the significance of FISA's roving surveillance provision, I need first to describe how FISA functions in ordinary, non-roving cases, and then highlight the differences in roving cases. In an ordinary FISA surveillance case, the Government must demonstrate to the FISA Court probable cause that the target of the surveillance is a foreign power or an agent of a foreign power, and that he is using, or about to use, a facility, such as a telephone. *See* 50 U.S.C. §1805(a)(2).

If it finds probable cause and approves the Government's application, the FISA Court then issues two separate orders. One order goes to the Government, and actually authorizes the surveillance. The other, referred to as a "secondary" order, goes to the provider – the telephone company – and directs it to assist the Government in conducting the surveillance. *See* 50 U.S.C. § 1805(c)(1)-(2). The secondary order is necessary because, in most cases, we need the affirmative assistance of the phone company to implement the surveillance. In an ordinary case, if the target switches to a new provider the Government must submit a new application and obtain a new set of FISA orders, because the new provider will – rightly – refuse to honor a secondary order directed at another company. However, where the Government can demonstrate in advance to the FISA Court that the *target's actions may have the effect of thwarting surveillance, such as by changing providers*, FISA's roving surveillance provision allows the FISA Court to issue a generic secondary order that we can serve on the new provider to commence surveillance without first going back to Court. The Government's probable cause showing that the target is an agent of a foreign power remains the same, and the Government must also demonstrate to the FISA Court, normally within 10 days of initiating surveillance of the new facility, probable cause that that specific agent is using, or is about to use, that new facility.

This provision is, as noted above, modeled on similar "roving" authority that has applied to law enforcement wiretaps since 1986 and has repeatedly been upheld in the courts. *See, e.g.*, *United States v. Jackson,* 207 F.3d 910, 914 (7th Cir. 2000), *vacated on other grounds*, 531 U.S. 953 (2000); *United States v. Gaytan,* 74 F.3d 545, 553 (5th Cir. 1996); *United States v. Bianco*, 998 F.2d 1112, 1122-1123 (2d Cir. 1993); *United States v. Petti*, 973 F.2d 1441, 1445 (9th Cir. 1992). These courts have expressly rejected the argument that roving surveillance violates the Fourth Amendment's "particularity" requirement.

In sum, there are three key points with respect to roving authority: first, in a roving case, just as in an ordinary case, the Government must establish (and the Court must find) probable cause that the target of the surveillance is a foreign power or an agent of a foreign power, and only that particular target's use of a new facility will justify a roving wire tap. *See* 50 U.S.C.
§ 1805(a)(2). Even where we do not know the target's name, we must provide the court sufficient detail to identify him with particularity. Second, we can obtain roving authority only where the FISA Court "finds, based upon specific facts in the application," that the actions of the target "may have the effect of thwarting" our ability to conduct surveillance with the aid of a specified provider or other third party. *See* 50 U.S.C. § 1805(c)(2)(B). Third, whenever we implement roving authority, we must report to the FISA Court, normally within 10 days, with the probable cause that ties the target to the new facility. *See* 50 U.S.C. § 1805(c)(3).

The authority to conduct roving electronic surveillance under FISA has proven operationally useful in a small but steady number of national security investigations each year. Typically, these situations involve highly-trained foreign intelligence officers operating in the United States, or other investigative subjects who have already shown an

apparent propensity to evade electronic surveillance. Between 2001 and 2010, the Government has sought roving surveillance authority in about 20 cases per year, on average.

Lone Wolf

The next expiring provision is the so-called "lone-wolf" definition, contained in section 1801(b)(1)(C) of Title 50. This definition allows us to conduct surveillance and physical search of *non-U.S. persons* engaged in international terrorism without demonstrating that they are affiliated with a particular international terrorist group.

There are two key points to understand about this provision. First, it applies only to non-U.S. persons (not to American citizens or green-card holders), *see* 50 U.S.C. § 1801(b)(1)(C), and only when they engage or prepare to engage in "international terrorism." *See* 50 U.S.C.
§ 1801(c). In practice, the Government must know a great deal about the target, including the target's purpose and plans for terrorist activity (in order to satisfy the definition of "international terrorism"), but need not establish probable cause to believe the target is engaging in those activities for or on behalf of a foreign power..

Second, although we have not used this authority to date, it is designed to fill an important gap in our collection capabilities by allowing us to collect on an individual foreign terrorist who is inspired by – but not a member of – a terrorist group. For example, it might allow surveillance when an individual acts based upon international terrorist recruitment and training on the internet without establishing a connection to any terrorist group. It might also be used when a member of an international terrorist group, perhaps dispatched to the United States to form an operational cell, breaks with the group but nonetheless continues to plot or prepare for acts of international terrorism. If such cases arise, which seems increasingly likely given the trend toward independent extremist actors who "self-radicalize," we might have difficulty obtaining FISA collection authority without the lone-wolf provision.

Business Records

The third expiring provision is the so-called "business records" provision, enacted in section 215 of the USA PATRIOT Act. This part of the statute allows the Government to apply to the FISA Court for an order directing the production of business records or tangible things that are relevant to an authorized national security investigation. *See* 50 U.S.C. § 1861. This authority allows the Government to obtain under FISA in a national security investigation the same types of records that can be obtained by a grand jury subpoena in an ordinary criminal investigation, though unlike a grand jury subpoena, it requires an order from the FISA Court. *See* 50 U.S.C. § 1861(c)(2)(D).

Section 215 has been used to obtain driver's license records, hotel records, car rental records, apartment leasing records, credit card records, and the like. It has never been used against a library to obtain circulation records. Some orders have also been used to support important and highly sensitive intelligence collection operations, on which this committee and others have been separately briefed. On average, we seek and obtain section 215 orders less than 40 times per year. Many of these are cases where FBI

investigators need to obtain information that does not fall within the scope of authorities relating to national security letters and are operating in an environment that precludes the use of less secure criminal authorities.

To obtain a business records order from the Court, the Government generally must show three main things. First, the Government must show that it is seeking the information in certain authorized national security investigations conducted pursuant to guidelines approved by the Attorney General. *See* 50 U.S.C. § 1861(a)(2)(A). Second, where the investigative target is a U.S. person, the Government must show that the investigation is not based solely on activities protected by the First Amendment. *See* 50 U.S.C. § 1861(a)(1), (a)(2)(B). Third, the Government must show that the information sought is relevant to the authorized investigation. *See* 50 U.S.C. § 1861(b)(2)(A). In addition, under the language of section 215, the Government must adhere to minimization procedures that limit the retention and dissemination of the information that is obtained concerning U.S. persons. *See* 50 U.S.C. § 1861(b)(2)(B) and (g).

The business records provision also bars the recipient of a business records order from disclosing it. However, the recipient of the order may challenge its legality, as well as any non-disclosure requirement, in court. To date, no recipient of a FISA business records order has challenged the validity of the order or a non-disclosure requirement.

Some have argued that section 215 runs afoul of the Fourth Amendment because it allows the Government to obtain records upon a showing of "relevance" to an authorized investigation rather than "probable cause." However, for constitutional purposes, a business records order is not a "search" within the meaning of the Fourth Amendment. It does not authorize the Government to enter premises and seize records or other tangible things. Instead, like a grand jury subpoena or administrative subpoena, it requires the recipient to identify the responsive items and provide them to the Government. Therefore, the probable cause requirement is inapplicable in this context. *Cf. Zurcher v. Stanford Daily*, 436 U.S. 547 (1978) (grand jury subpoenas "do not require proof of probable cause"); *Oklahoma Press Pub. Co. v. Walling*, 327 U.S. 186 (1946) (orders for the production of records "present no question of actual search and seizure"). The "relevance" standard for business records orders under FISA parallels the standards that Congress has authorized for administrative subpoenas in health care fraud. *See* 18 U.S.C. § 3486; 21 U.S.C. § 876. In addressing administrative subpoenas, the Supreme Court has explained that "[i]t is not necessary, as in the case of a warrant, that a specific charge or complaint of violation of law be pending or that the order be made pursuant to one. It is enough that the investigation be for a lawfully authorized purpose, within the power of Congress to command." *Oklahoma Press Pub. Co.*, 327 U.S. at 208-09.

****

In closing, we continue to believe that these three authorities are critical to national security investigations and should be reauthorized for a period that will provide our intelligence professionals confidence that these important tools will continue to be available to protect national security. Robust substantive standards and procedural protections are in place to ensure that these tools are used responsibly and in a manner that safeguards Americans' privacy and civil liberties. All three authorities require

approval of the FISA Court before they can be used. If Congress feels that there are ways that those protections can be further enhanced while maintaining the effectiveness of these and other intelligence tools, we remain open to such measures.

Thank you again for inviting me to this hearing and I am happy to answer any questions you may have.

Mr. SENSENBRENNER. Thank you, Mr. Hinnen.
Mr. Litt?

TESTIMONY OF ROBERT S. LITT, GENERAL COUNSEL, OFFICE OF THE DIRECTOR OF NATIONAL INTELLILGENCE

Mr. LITT. Thank you, Mr. Chairman. Chairman Sensenbrenner, Ranking Member Scott, Ranking Member Conyers, Members of the Subcommittee, thank you for inviting me here to testify today about the three expiring provisions of the Foreign Intelligence Surveillance Act.

Mr. Chairman, I particularly want to thank you for your leadership on PATRIOT Act issues since 2001 which have been so helpful for the intelligence community.

I want to start by making clear that the three expiring provisions are tools that are critical to help us defend our national security and they must be reauthorized. At the same time, I want to say that I think the distinguished Ranking Member of the full Committee correctly identified the issue which is what is the proper balance to strike between the tools to protect national security and the protection of civil liberties. I think our position is—and I hope to be able to persuade you—that these tools in fact do that.

I do want to begin by giving you a couple of unclassified examples of how these tools have been used.

For roving taps, I can tell you that we are currently using one against a foreign agent who changes cellular phones frequently. Without roving surveillance, there would be a gap in collection each time this agent switched phones because of the time we would need to get a new court order.

The business records provision is also important. For example, recently a business record order was used to obtain information that was essential in the investigation of Khalid Aldawasari, which Chairman Smith referred to earlier, who was subsequently arrested in Texas.

In another case, hotel records that we obtained under a business records order showed that over a number of years a suspected spy had arranged lodging for other suspected intelligence officers. These records provided information about the subject that helped the FBI ultimately to get full FISA coverage.

As you know, many uses of the authorities under FISA are classified and we cannot discuss them publicly. This has led to some myths and misconceptions about FISA and the PATRIOT Act, and I want to take a couple of minutes to dispel some of those.

First, although the lone wolf definition has not been used, it is nonetheless an important tool to have in our toolbox in light of the constantly evolving terrorism threat that we face. Michael Leiter, the Director of the National Counterterrorism Center, has testified that the availability of sophisticated extremist propaganda on the Internet means that terrorist organizations can reach out and incite individual extremists to attack us even when those extremists may not actually be agents of the terrorist organization. This is the kind of situation that the lone wolf definition applies to, and I want to reiterate what Todd Hinnen just said, which is that this applies only to foreigners, not to U.S. citizens or lawful permanent residents.

Second, criminal law authorities are not always an adequate substitute for FISA authorities. In particular, criminal wiretaps under Title III have to be disclosed to the target which may make it impossible to protect critical intelligence sources and methods. And in some cases, for example, in many instances when we are tracking foreign spies, we may not have a criminal predicate to support a Title III wiretap.

Third, despite what some claim, we cannot get a roving wiretap without identifying the target. The statute requires that we provide the identity, if known, or a description of the specific target of FISA electronic surveillance.

Finally, it is critical that the public understand that these are not unchecked or unrestrained authorities. We recognize that effective oversight of the intelligence community is essential both because of the powers the intelligence community has and because those powers are often exercised in secret. And we welcome that oversight. There is, in fact, extensive and effective oversight of these provisions by all three branches of Government. The legal framework requires that we can't predicate investigations on activity that is protected by the First Amendment, that information we collect under these authorities has to be minimized in accordance with procedures that are approved by the court, and intelligence agencies are governed by rules that limit the collection, retention, and dissemination of information about U.S. persons.

Each of these authorities, as Todd said, requires prior approval by the FISA Court, and I can say from my experience in a year and a half on this job, that the FISA Court is not a rubber stamp but gives a searching review to each application that comes before it and often requires changes and modifications. In addition, FISA applications get extensive high-level review within the executive branch even before they are submitted to the court. Agents and analysts who work in this area get regular training in the requirements of the law, and use of these authorities is subject to oversight by inspectors general, by the National Security Division of the Department of Justice, and by my office, the Office of the Director of National Intelligence.

And finally, the use of these authorities, including classified details that we can't disclose publicly, is regularly reported to the appropriate committees of Congress in a variety of ways. So there is really an extensive oversight framework.

And I just want to close by reiterating that, first, as the Attorney General and the DNI have said, we are prepared to consider appropriate additional protections for civil liberties that don't compromise the operational utility of these provisions, but it is important that these provisions be reauthorized and reauthorized for as long a period as possible.

Thank you.

[The statement of Mr. Litt follows:]

Statement for the Record

House Judiciary Subcommittee on
Crime, Terrorism and Homeland Security

Hearing

on

Reauthorizing the Patriot Act

Statement for the Record

Robert S. Litt
General Counsel
Office of the Director of National Intelligence
9 March 2011

Statement of
The Honorable Robert S. Litt
General Counsel
Office of the Director of National Intelligence

Before the
House Judiciary Subcommittee
on Crime, Terrorism and Homeland Security
on "USA PATRIOT Act Reauthorization"
March 9, 2011

Chairman Sensenbrenner, Ranking Member Scott and members of the House Judiciary Subcommittee on Crime, Terrorism and Homeland Security, thank you for inviting me to testify today concerning the three provisions of the Foreign Intelligence Surveillance Act (FISA) that are scheduled to sunset again on May 27, 2011. The Department of Justice has provided a brief overview of the three expiring provisions (the "roving" surveillance provision, the "lone wolf" definition, and the "business records" provision) and has explained in general terms how these authorities have been used in practice. I will focus on two things: (1) the Intelligence Community's need for these authorities to keep the Homeland safe and (2) the safeguards that are in place to ensure that the authorities are used responsibly, in a manner consistent with the law and with appropriate protections for Americans' privacy and civil liberties.

The threat to the Homeland from violent extremists is growing. As Director of National Intelligence Clapper testified recently, counterterrorism is the Intelligence Community's top priority. Since 9/11, the Intelligence Community has helped thwart many potentially devastating attacks, apprehend numerous known and suspected terrorist throughout the world and greatly weaken much of al-Qa'ida's core capabilities. The nature of the terrorism threat that we face is evolving. Our adversaries are constantly adapting their strategies and communication techniques. As Mr. Hinnen noted in his testimony, the provisions that are expiring — the roving wiretap provision, the "lone wolf" definition, and the business records authority — along with other critical intelligence tools, provide valuable tools needed to help us detect and disrupt plots directed against the United States.

One aspect of this evolution that is particularly relevant to the "lone wolf" definition is the growing threat from individuals, both at home and abroad, whose affiliation with foreign terrorist organizations, if any, is often vague. Although such violent extremists come in many forms, they often operate independent of one another and largely independent of any organized terrorist group overseas such as al-Qa'ida.

Increasingly sophisticated propaganda that is easily accessible and downloaded through the Internet and social media can quickly shape the views of extremists and provide them guidance, inspiration or justification to carry out attacks, even when they may not have received direct instruction or assistance from foreign terrorist organizations. Indeed, some al-Qa'ida organizations — in particular al-Qa'ida in the Arabian Peninsula (AQAP) — have actually

sought to encourage and "virtually" recruit such actors through their propaganda.

In some instances, these individuals come to our attention when they take direction or get training and equipment from international terrorists, whether in Pakistan, Yemen or elsewhere. But we may encounter some potential terrorists about whom we know only that they are inspired by the foreign terrorist organizations, and perhaps seek guidance from them, but we have insufficient intelligence to conclude that they are acting for or on behalf of an international terrorist organization. This would include violent extremists who are inspired by the international terrorist organizations — who seek to further their objectives — but who may not be agents of those organizations.

It is this situation — one which the Intelligence Community believes is a realistic possibility — the "lone wolf" definition can provide us critical intelligence capabilities. As Mr. Hinnen explained, absent the "lone wolf" definition, the United States Government is required to establish probable cause to show that a person is acting as an agent of a specific foreign power, which could include an international terrorist organization, before the United States can initiate electronic surveillance in the United States against the person for foreign intelligence purposes. In certain cases, we might encounter a non-United States person within this country, have information that indicates he is planning a terrorist attack, using the aims and means of international terrorism, but not have information sufficient to establish probable cause that he is acting "for or on behalf of" an international terrorist organization. In some cases, the United States Government may be able to nonetheless proceed with criminal electronic surveillance under Title III and thereby be able to monitor and ultimately thwart the subject's terrorist plans. But in other cases, Title III coverage might not be available and the Government would be forced to delay the institution of electronic surveillance until further information can be acquired from other sources. In the face of an active terrorist threat, such a delay could have profound consequences. Moreover, while Title III coverage might be available in some such cases, it may be impossible to use that tool and still protect critical intelligence sources and methods. In this case, the "lone wolf" definition may provide the only opportunity to track a potential terrorist and prevent a damaging attack on the homeland.

Over the years, a number of myths have developed about these authorities. At times, these myths have overshadowed the truth. It is easy to understand how some of these myths have developed. I will be the first to admit that FISA is a complicated statute. In addition, while transparency is important to the functioning of our government, so is the ability to conduct certain activities in secret so that our adversaries will not be able to take countermeasures and avoid detection. Therefore, certain uses of these authorities have remained classified, and although they have been fully briefed to the appropriate committees of Congress, this has made it more difficult to understand the complexities of FISA. Therefore, I think it is important to try to clarify some of the common misunderstandings regarding the expiring provisions.

- First, I want to reiterate what the Department of Justice has told the Committee and re-emphasize that contrary to some public reports, none of the provisions up for renewal provide the Intelligence Community with unchecked authority. Each of these provisions — the "lone wolf" definition, the roving wire tap provision and the FISA Business Records provision — requires that before the Intelligence Community undertakes

collection, a federal court must review the matter and issue an order authorizing collection. The requirement of independent judicial review helps ensure that the balance is appropriately struck in each case between the government's need to acquire information to protect the country from potential threats and the need to safeguard the constitutional rights and civil liberties of U.S. persons.

- Second, these are critical tools that help the Intelligence Community disrupt terrorist plots and without these authorities we hamper our ability to keep America safe by detecting and disrupting the next attack before it happens.

- Third, although Title III wiretaps, grand jury subpoenas and criminal search warrants are important tools, they cannot substitute for the FISA. Most notably, the procedural requirements associated with Title III wiretap, including disclosure to the target and full discovery of the basis for the surveillance may make it impossible to protect critical intelligence sources and methods.

- Fourth, the concerns about "Roving John Doe" wiretaps are misplaced. While the government may not always have the name of the person to be targeted, we must always be able to provide the FISA Court sufficient detail to identify the person with particularity. If we are not able to do that, we have failed to meet the statutory requirements and the FISA Court will not authorize the use of the authority.

- Fifth, the roving authority is not, and cannot, be used to, for example, wiretap an entire neighborhood in the hopes of acquiring intelligence information. Even when the FISA Court has granted authority for a roving wiretap, we can only conduct surveillance on a phone if we believe the target of the surveillance is using it.

- Sixth, Congress, though the appropriate oversight committees, is aware of how the FISA authorities are used.

- Seventh, the FISA Court is not a "rubber stamp" for the government. It is true the Court operates in secret and on an ex parte basis since it is almost always necessary to keep the identities of the targets and the intelligence used to identify the targets secret. But the judges and staff of that Court give a searching review to every application that comes before them, and frequently require changes or limitations on proposed orders.

I want to take that last point, and place it in the broader context of the oversight process that exists to ensure that the expiring authorities and FISA in general, are used in compliance with the Constitution and the law.

The Executive Branch understands its obligation to ensure that it exercises the powers granted it in accordance with the law and in a manner that protects civil liberty and privacy rights. We believe that vigorous and effective oversight — by all three branches of government — is essential to help ensure that the American people have confidence in our ability to protect both their civil liberties and their security. The public has entrusted the Intelligence Community with

important powers and it is our collective duty to ensure that those powers are exercised responsibly.

The legal framework we operate under is founded on the Constitution and in particular the First and Fourth Amendments. It includes the FISA itself, which prescribes specific and detailed requirements that must be met for the exercise of these authorities. It also includes Executive Orders governing the Intelligence Community which limit the collection, retention and dissemination of information concerning U.S. persons. Taken together, these provide an extensive legal framework protecting individual privacy and liberty. This framework is overseen by all three branches of the government.

First, the judiciary. The FISA Court is composed of eleven Article III judges selected from districts around the country and appointed by the Chief Justice of the United States for seven-year terms. As noted above, the judges of the FISA Court engage in a thorough and searching review of every FISA application to ensure that the application complies with the statutory standards. Moreover, the FISA Court not only approves the use of these authorities, it also takes an active role in ensuring that the government is complying with the FISA Court orders, by regularly reviewing the activities approved, prescribing procedures that agencies must follow in executing their orders and by requiring that violations of these procedures be reported.

In addition to the oversight by the FISA Court, the Executive Branch has developed its own robust oversight regime. First, FISA applications, which require a high level of approval within the Executive Branch, receive extensive and detailed review before the application is submitted to the FISA Court. In fact, FISA applications receive far more extensive review than criminal search warrants or electronic surveillance orders. Moreover, the National Security Division of the Department of Justice conducts regular training and oversight to ensure that FISA Court orders are properly implemented. In addition, agencies that use these authorities require personnel to participate in comprehensive training programs to ensure that they understand what is permissible under the law, and are implementing automated systems to help ensure that the authorities are properly used. Finally, the use of these FISA authorities is subject to oversight by the appropriate Offices of General Counsel, Inspectors General, and intelligence oversight offices. The Office of the Director of National Intelligence, (including the ODNI's Civil Liberties Protection Officer and his office) has statutory responsibility to ensure that the elements of the Intelligence Community comply with the Constitution and laws of the United States. It works closely with the National Security Division of the Department of Justice to provide oversight of FISA activities.

Finally, Congress is an active player in FISA oversight. Starting with our confirmation hearings, the DNI and I have steadfastly committed to keeping Congress, through the appropriate committees, informed of intelligence activities. This includes keeping Congress fully informed of how these FISA authorities are being used, including classified activities. In addition to the requirements to provide Congress several reports each year on the use of these collection authorities and copies of significant FISA Court opinions, the Congress regularly receives information concerning the use of these authorities to ensure that the authorities are used in compliance with the law and in a manner that protects privacy and civil liberties.

****

In closing, I would stress that these three authorities are critical to national security investigations and the protection of our nation. They should be reauthorized. Robust substantive standards and procedural protections are in place to ensure that these tools are used responsibly, in a manner consistent with the law, and in a manner that safeguards Americans' privacy and civil liberties. We are committed to working with Congress to obtain reauthorization. We think it is essential that the extension be long enough to provide our intelligence professionals confidence that these important tools will continue to be available to protect national security.

Thank you again for inviting me to this hearing and we are happy to answer any questions you may have.

Mr. SENSENBRENNER. Mr. Sales?

TESTIMONY OF NATHAN A. SALES, ASSISTANT PROFESSOR OF LAW, GEORGE MASON UNIVERSITY

Mr. SALES. Thank you, Mr. Chairman. Chairman Sensenbrenner, Ranking Member Scott, Ranking Member Conyers, thank you for your time. Members of the Subcommittee, thank you for your time.

My name is Nathan Sales. I am a law professor at George Mason Law School.

My testimony today is that the three provisions that are up for renewal, roving wiretaps, business records, and lone wolf, are actually quite modest. Generally speaking, these tools simply let counter-terrorism investigators use some of the same investigative methods that ordinary cops have been using for decades, tools in fact that the Federal courts repeatedly have upheld. Plus, the law contains elaborate safeguards. In several respects, these safeguards under the PATRIOT Act are even stronger than the laws that apply in the ordinary criminal context.

Take, for instance, roving wiretaps. Sophisticated criminals like drug dealers and mobsters sometimes try to evade surveillance by using burner cell phones or swapping out their SIM cards. The result is a drawn-out game of cat and mouse. Investigators get a court order to tap a particular phone, only to find out that he already switched to an even newer one. So it is back to the courthouse for a fresh warrant.

Now, in 1986, Congress solved this problem for criminal investigators by letting them use roving wiretaps, basically a wiretap—a court order that applies to particular people rather than to particular devices. Agents, thus, can monitor a cell phone—a suspect regardless of what cell phone he happens to be using without first heading back to court for yet another order.

Now, roving wiretaps have been upheld by no fewer than three Federal appellate courts, the Ninth, the Fifth, and the Second Circuits. To my knowledge, no appellate court has disagreed.

So what the PATRIOT Act did was allow the same sort of investigative technique in terrorism cases. The basic idea is to level the playing field. If a roving wiretap is good enough for Tony Soprano, it is good enough for Mohamed Atta.

In addition, the law contains strict safeguards. A court order is necessary. FBI agents can't unilaterally eavesdrop on every phone a person uses. They have to convince a judge that there is probable cause first. Agents also have to follow minimization procedures. That means they have to follow rules that limit their collection, retention, and sharing of information about innocent Americans, information that is inadvertently collected.

Now, there may be cases where agents don't yet know the precise name of a terrorist. Indeed, that's one of the reasons why you investigate the terrorist. But even then, the law requires agents to provide the FISA Court with—and I am quoting now—a description of the specific target. They cannot just run a dragnet under the law.

Second, let us focus on the business records provision. In criminal cases, grand juries routinely subpoena documents from entities like online retailers and banks. The PATRIOT Act lets investiga-

tors do the same sort of thing in national security cases, but only if they persuade the FISA Court that the documents they seek are relevant to an ongoing and authorized investigation. This provision isn't aimed at libraries, though it conceivably might be applied to them, although as we have heard, it has not yet been so. Still, that is not unusual. Grand juries sometimes demand business records from libraries in ordinary criminal investigations. Indeed, the Iowa Supreme Court once upheld a library subpoena in a case involving cattle mutilation. If we can investigate cattle mutilators, hopefully we can investigate international terrorists using the same technique.

In fact, the PATRIOT Act's protections are even stronger than the protections that apply to grand jury rules. Federal prosecutors can issue grand jury subpoenas more or less on their own, but PATRIOT requires the FBI to get a court's approval first. In addition, PATRIOT expressly bars investigators from investigating Americans based on their First Amendment protected activities. It also imposes special limits when investigators seek sensitive records such as medical records or library records. Grand jury rules offer no such guarantees.

Finally, there is lone wolf, which wasn't in the PATRIOT Act but which Congress adopted in 2004. Sometimes it is difficult to prove that a suspect is formally linked to a terrorist organization overseas. The FBI faced a similar problem just before 9/11. It was suspected that Zacarias Moussaoui was up to no good, but agents hadn't yet connected him to any foreign terrorists. As a result, it was unclear whether they had legal authority under FISA to search his apartment or search his laptop. The 9/11 Commission would go on to speculate later that if agents had been able to investigate Moussaoui, they might have unraveled the entire 9/11 plot.

There is another reason for lone wolf: the growing danger of what might be called "entrepreneurial terrorism." Solitary actors who are inspired by al Qaeda are on the rise, and they are capable of causing just as much death and just as much destruction as those who are formally members of that group.

PATRIOT fixes these problems. Now investigators can get a court order to monitor any target who is engaging in international terrorism. There is no need to make the additional showing that he is engaging in international terrorism on behalf of a foreign power. Again, PATRIOT provides robust protection for civil liberties, perhaps the most important of which is that investigators can't start monitoring a lone wolf who is engaging in domestic terrorism. There is still a foreign nexus. Investigators can only investigate international terrorism.

Thank you, Mr. Chairman. Thank you, Members of the Subcommittee. I would be happy to answer any questions.

[The statement of Mr. Sales follows:]

The Reauthorization of the PATRIOT Act

Subcommittee on Crime, Terrorism, and Homeland Security
Committee on the Judiciary
United States House of Representatives

March 9, 2011

Statement of Nathan A. Sales
Assistant Professor of Law
George Mason University School of Law

Chairman Sensenbrenner, Ranking Member Scott, and Members of the Subcommittee, thank you for inviting me to testify on this important issue. My name is Nathan Sales, and I am a law professor at George Mason University School of Law, where I teach national security law, administrative law, and criminal law. Previously, I was Deputy Assistant Secretary in the Office of Policy at the U.S. Department of Homeland Security. I also served in the Office of Legal Policy at the U.S. Department of Justice, where I was a member of the team that helped draft the USA PATRIOT Act[1] after the terrorist attacks of September 11, 2001. The views I will express in this hearing are mine alone, and should not be ascribed to any past or present employer or client.

The gist of my testimony is as follows. The USA PATRIOT Act is a vital set of tools in our ongoing struggle against al Qaeda and like-minded terrorists. This is especially true of the three authorities that are up for renewal this year: "roving wiretaps," "business records," and "lone wolf." Notwithstanding the PATRIOT Act's controversial reputation, these three provisions are actually quite modest. In many cases, they simply let counterterrorism agents use some of the same techniques that ordinary criminal investigators have been using for decades – techniques that the federal courts repeatedly have upheld. Plus, each of these authorities contains elaborate safeguards – including prior judicial review – to help prevent abuses from taking place. Indeed, some of the PATRIOT Act's protections are even *stronger* than the ones from the world of ordinary law enforcement.

I. Roving Wiretaps

The policy rationale for "roving wiretaps" – in essence, court orders that apply to particular *people*, rather than particular *devices* – is fairly straightforward. Sophisticated targets like drug kingpins, mob bosses, spies, and terrorists are trained to thwart electronic surveillance by constantly switching communications devices or methods. They might use "burner" cell phones, for instance, or they might repeatedly swap out their phones' SIM cards. The result is a drawn-out game of cat and mouse.[2] Investigators obtain a court order to tap a suspect's new

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

[2] S. Rep. No. 99-541, at 31, *reprinted in* 1986 U.S.C.C.A.N. 3555, 3585 ("[L]aw enforcement officials may not know, until shortly before the communication, which telephone line will be used by the person under surveillance.").

phone only to discover that he has already switched to an even newer one. So it's back to the judge for a fresh warrant. Not only is this cycle a waste of investigators' scarce time and resources, it also runs the risk that agents will miss critical communications in the gap before the court can issue an updated order.

Congress largely solved this problem for criminal investigators two and a half decades ago. The Electronic Communications Privacy Act of 1986 (ECPA) amended the federal wiretap statute – Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III) – to allow investigators to conduct electronic surveillance when they cannot meet the ordinary statutory requirement of specifying "the facilities from which or the place where the communication is to be intercepted."[3] Instead, investigators may obtain a court order to operate a roving wiretap if, among various other things, they establish "probable cause to believe that the person's actions could have the effect of thwarting interception from a specified facility."[4] In effect, a single court order permits surveillance regardless of what device the target might be using.[5] Investigators may continue to monitor a suspect even if he switches phones, without first heading back to court to obtain further judicial approval.

Of course, terrorists and spies can be just as adept at evading surveillance as drug dealers and mobsters. Maybe even more so. And so the PATRIOT Act allows national security investigators to use the same sort of technique as their law enforcement counterparts. Section 206 of the law permits roving wiretaps under the Foreign Intelligence Surveillance Act of 1978 (FISA) where "the actions of the target of the application may have the effect of thwarting the identification of a specified person."[6] The basic idea here is to level the playing field between criminal cases and terrorism cases. If a roving wiretap is good enough for Tony Soprano, Congress concluded, it's good enough for Mohamed Atta.

Significantly, the PATRIOT Act's roving wiretaps authority contains exacting safeguards to protect privacy and civil liberties. As in the criminal context, a prior court order is necessary. FBI agents can't unilaterally decide to eavesdrop on every phone a person uses. They have to appear before the Foreign Intelligence Surveillance Court and convince a federal judge that there is probable cause to believe that the target is a "foreign power" (such as a foreign country or a foreign terrorist organization) or an "agent of a foreign power" (such as a spy or a terrorist).[7] In other words, Congress has interposed a "neutral and detached magistrate"[8] between investigators and targets – the same sort of protection that we have long trusted to strike the right balance between security and privacy in the law enforcement context. Agents also must demonstrate probable cause to believe that "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign

[3] 18 U.S.C. § 2518(1)(b)(ii).

[4] *Id.* § 2518(11)(b)(ii).

[5] United States v. Hermanek, 289 F.3d 1076, 1087 (9th Cir. 2002).

[6] 50 U.S.C. § 1805(c)(2)(B).

[7] *Id.* § 1805(a)(2)(A).

[8] Johnson v. United States, 333 U.S. 10, 14 (1948).

power."[9] The government has to adopt "minimization procedures" – i.e., procedures to ensure that private information about innocent Americans is not collected, retained, or disseminated.[10] (To be precise, this requirement applies to any "United States person" – i.e., a citizen or lawful permanent resident alien.[11] For simplicity's sake, this testimony will use the term "American" as a shorthand for "United States person.") And, again, roving wiretaps aren't available in every national security case as a routine matter. They may only be used where the FISA court finds, "*based upon specific facts provided in the [government's] application*, that the actions of the target of the application may have the effect of thwarting the identification of a specified person."[12]

Federal courts agree that Title III's roving wiretaps authority is constitutional, and that consensus provides strong support for the constitutionality of roving wiretaps under the PATRIOT Act. For instance, in *United States v. Petti*,[13] the Ninth Circuit held that roving wiretaps are perfectly consistent with the Fourth Amendment's particularity requirement.[14] The court went on to emphasize that Title III presents "virtually no possibility of abuse or mistake."[15] This is so, it explained, because the statute only allows monitoring of telephones that the suspect is using, it requires minimization, and it only applies when the suspect is trying to evade surveillance.[16] (Roving wiretaps under PATRIOT feature virtually identical safeguards.) The Fifth Circuit expressly adopted the *Petti* court's reasoning a few years later,[17] and the Second Circuit likewise has upheld the use of roving wiretaps.[18] To my knowledge, no appellate court has reached a contrary conclusion. In short, there is a broad judicial consensus that, as the Ninth Circuit put it in another case, "[r]oving wiretaps are an appropriate tool to investigate individuals . . . who use cloned cellular phone numbers and change numbers frequently to avoid detection."[19]

Finally, let me say a few words about "John Doe" roving wiretaps – surveillance in which the FISA court order describes the target but does not indicate his precise name or the precise facilities to be tapped. The risk of misuse under the PATRIOT Act seems to me fairly low. There may be times when investigators don't yet know the specific identity of the terrorist in question.[20] (Indeed, the need to learn more about the target is precisely why one conducts

---

[9] 50 U.S.C. § 1805(a)(2)(B).

[10] *Id.* § 1801(h).

[11] *Id.* § 1801(i).

[12] *Id.* § 1805(c)(2)(B) (emphasis added).

[13] 973 F.2d 1441 (9th Cir. 1992).

[14] U.S. CONST. amend. IV ("[N]o warrants shall issue, but upon probable cause, supported by oath or affirmation, and *particularly describing the place to be searched*." (emphasis added)).

[15] *Petti*, 973 F.2d at 1445.

[16] *Id.*

[17] United States v. Gaytan, 74 F.3d 545, 553 (5th Cir. 1996).

[18] United States v. Piggott, 141 F.3d 394 (2d. Cir. 1997).

[19] United States v. Hermanck, 289 F.3d 1076, 1087 (9th Cir. 2002).

[20] 50 U.S.C. § 1805(c)(1)(A), (B) (directing the FISA court to specify the target's identity "if known," and the facilities to be surveilled "if known").

surveillance in the first place.) In these circumstances, investigators need not indicate his name, but they still must provide the FISA court with a "description of the specific target,"[21] which might include the names of his terrorist associates, his age, his country of origin, or other biographical details. (This was true even before the PATRIOT Act became law, incidentally.) Second, investigators still must comply with the bedrock requirement that they establish, to the satisfaction of the FISA court, probable cause to believe that the person to be surveilled is a foreign power or an agent of a foreign power.[22] They also must demonstrate probable cause that each of the "facilities or places" to be monitored "is being used, or is about to be used," by a foreign power or agent.[23] Nothing in PATRIOT did away with these basic rules.

Third, any risk of overcollection – i.e., the possibility that investigators might inadvertently intercept communications involving innocent third parties – is mitigated by FISA's minimization requirement: Investigators must follow a rigorous set of procedures that "minimize the acquisition and retention, and prohibit the dissemination," of Americans' private data.[24] Fourth, the active involvement of the FISA court stands as a significant bulwark against any misuse. Not only does the court provide oversight before any surveillance is approved, in the form of ex ante judicial review. It also provides ongoing oversight while the surveillance is taking place: Investigators who operate a roving wiretap must alert the FISA court no more than ten days after they begin monitoring any new facility, and they must explain the "facts and circumstances" that justify their "belief that each new facility or place at which the electronic surveillance is directed is or was being used, or is about to be used, by the target."[25] The combination of these safeguards should adequately ensure that roving wiretaps do not infringe upon important privacy interests.

II. Business Records

Section 215 of the PATRIOT Act – the so-called "business records" provision – authorizes the national security equivalent of grand jury subpoenas. Criminals often leave behind trails of evidence in their everyday interactions with banks, credit card companies and other businesses. Federal grand juries routinely issue subpoenas to these entities in investigations that range from narcotics crimes to health care fraud. When a subpoena is issued, the recipient is required to turn over "any books, papers, documents, data, or other objects the subpoena designates."[26] The recipient must do so whenever there is a "reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury's investigation."[27]

---

[21] *Id.* § 1804(a)(2).

[22] *Id.* § 1805(a)(2)(A).

[23] *Id.* § 1805(a)(2)(B).

[24] *Id.* § 1801(h).

[25] *Id.* § 1805(c)(3).

[26] Fed. R. Crim. Pro. 17(c)(1).

[27] United States v. R. Enterprises, Inc., 498 U.S. 292, 301 (1991).

The PATRIOT Act amended FISA to establish a comparable mechanism for national security investigators to obtain the same sorts of materials. In particular, the FISA court may issue an order that directs a third party to produce "any tangible things (including books, records, papers, documents, and other items)."[28] To obtain such an order, the government must establish "reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation."[29] (This is virtually identical to the standard that applies in the grand jury context; the Supreme Court has held that a subpoena is valid if there is a "*reasonable possibility*" that it will result in relevant information.[30]) In addition, agents must comply with a detailed set of minimization procedures that restrict the retention and distribution of private data about innocent Americans.[31] Once again, the basic idea behind this provision is to level the playing field. If officials investigating drug dealers and crooked insurance companies can subpoena business records, then officials investigating international terrorists should be able to as well.[32]

Like other parts of the PATRIOT Act, the business records provision features an extensive set of protections. In fact, there are several respects in which section 215's safeguards are even stricter than those that apply in the grand jury context:

- First, the PATRIOT Act has a narrower scope. Section 215 may only be used in national security investigations,[33] whereas a grand jury can issue a subpoena "merely on suspicion that the law is being violated, or even just because it wants assurance that it is not."[34]

- Second, PATRIOT provides for ex ante judicial review; investigators cannot acquire business records unless they first appear before the FISA court and convince it that they are entitled to them.[35] Grand jury practice is very different. Although subpoenas *in theory* are issued in the name of the grand jury and the overseeing court, *in practice* they are issued more or less unilaterally by Assistant U.S. Attorneys; judicial review does not occur until after the subpoena has issued, if at all.[36]

---

[28] 50 U.S.C. § 1861(a)(1).

[29] *Id.* § 1861(b)(2)(A).

[30] *R. Enterprises*, 498 U.S. at 301(emphasis added); *see id.* at 297 (stressing that "the Government cannot be required to justify the issuance of a grand jury subpoena by presenting evidence sufficient to establish probable cause because the very purpose of requesting the information is to ascertain whether probable cause exists").

[31] 50 U.S.C. § 1861(g).

[32] The pre-PATRIOT version of FISA's business records authority was considerably narrower than the grand jury rules. It only applied to certain types of entities (such as airlines, hotels, and car rental companies), and it was only available when investigators established "specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power." Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272 § 602, 112 Stat. 2396, 2410-12 (1998). The PATRIOT Act brought FISA closer in line with grand jury practices.

[33] 50 U.S.C. § 1861(a)(1).

[34] United States v. Morton Salt, 338 U.S. 632, 642-43 (1950).

[35] 50 U.S.C. § 1861(c).

[36] Fed. R. Crim. Pro. 17(c)(2) ("On motion made promptly, the court may quash or modify the subpoena if compliance would be unreasonable or oppressive.").

- Third, the PATRIOT Act requires minimization, thereby protecting the privacy of innocent Americans[37]; the grand jury rules do not.

- Fourth, the PATRIOT Act forbids the government from investigating an American "solely upon the basis of activities protected by the first amendment to the Constitution."[38] The grand jury rules offer no such guarantee.

- Fifth, PATRIOT offers heightened protections when investigators seek materials that are especially sensitive, such as medical records and records from libraries or bookstores.[39] (This provision was added in 2006.[40]) The grand jury rules lack any comparable restrictions.

- Finally, PATRIOT provides for robust congressional oversight: The government must "fully inform" the House and Senate Intelligence Committees, as well as the Senate Judiciary Committee, concerning "*all*" uses of this provision.[41] The grand jury rules contain no such notification requirement.

The constitutional principles concerning government access to third party records have been settled for decades, and these precedents strongly support the PATRIOT Act's business records authority. A long line of Supreme Court case law confirms that there is no "reasonable expectation of privacy"[42] in the information a person conveys to businesses and other third parties. As a result, the government's efforts to acquire such data – as with grand jury subpoenas, for example – do not amount to "searches" within the meaning of the Fourth Amendment. Investigators therefore need not secure a warrant or demonstrate probable cause. For instance, in the 1979 case *Smith v. Maryland*,[43] the Supreme Court ruled that police officers' use of a pen register – which records the numbers dialed by a particular telephone, but not the content of the resulting conversations – did not require a warrant or probable cause. "This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[44] A few years earlier, in *United States v. Miller*,[45] the Court similarly ruled that police could obtain a person's financial records from a bank without a warrant or probable cause. According to the Court, "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government

[37] 50 U.S.C. § 1861(g).

[38] *Id.* § 1861(a)(1).

[39] *Id.* § 1861(a)(3).

[40] USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177 § 106(a)(2), 120 Stat. 192, 196 (2006).

[41] 50 U.S.C. § 1862(a) (emphasis added).

[42] Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

[43] 442 U.S. 735 (1979).

[44] *Id.* at 743-44.

[45] 425 U.S. 435 (1976).

authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[46] If mere relevance is all that's required to obtain business records in ordinary criminal investigations, it is not readily apparent why something more than that should be required to obtain the same materials in national security investigations.

Section 215 isn't just known as the "business records" provision, of course. It's also known, unflatteringly, as the "libraries" provision. Section 215 isn't aimed at libraries, and the Justice Department has indicated to Congress that the provision has never been used to obtain library or bookstore records.[47] While section 215 conceivably might be applied to libraries or bookstores, it isn't unique in that respect: It's not unusual for grand juries to demand library records in regular criminal cases. For instance, during the Unabomber investigation, grand juries issued subpoenas to a half dozen university libraries; investigators wanted to know who had checked out various works that were cited in the "Unabomber Manifesto."[48] In the 1990 Zodiac gunman investigation, a New York grand jury subpoenaed records from a Manhattan library. Investigators believed that the gunman was inspired by a Scottish occult poet, and wanted to learn who had checked out his books.[49] In the 1997 Gianni Versace murder case, a Florida grand jury subpoenaed records from public libraries in Miami Beach.[50] The Iowa Supreme Court even upheld the use of library subpoenas in an investigation of cattle mutilations.[51] If libraries and bookstores aren't exempt from grand jury subpoenas in ordinary criminal cases, there is no obvious reason to exempt them from business records orders in terrorism cases – especially since the PATRIOT Act offers even more robust protections than the grand jury rules.

III. Lone Wolf

The third provision that is up for renewal this year is known as the "lone wolf" fix. (Note that lone wolf wasn't part of the PATRIOT Act. Congress adopted it in the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), and also subjected it to PATRIOT's sunset provision.[52]) As a result of this measure, counterterrorism investigators may obtain the FISA court's approval to conduct electronic surveillance of certain international terrorists even if there is not yet enough evidence to formally link them to a foreign terrorist organization.

Two distinct yet related policy considerations suggest a need for lone wolf surveillance. First, there's the evidentiary problem. It may be difficult for investigators to establish that a given suspect is a member of, or otherwise has ties to, a foreign terrorist organization. The

---

[46] *Id.* at 443.

[47] CRS Report for Congress, *USA PATRIOT Improvement and Reauthorization Act of 2005: A Legal Analysis* 4-5 n.18 (Dec. 21, 2006).

[48] *Library Records Led to Break in Unabomber Case*, NPR, June 2, 2005.

[49] Eric Lichtblau, *Libraries Say Yes, Officials Do Quiz Them About Users*, N.Y. TIMES, June 20, 2005.

[50] Al Baker & Soraya Sarhaddi Nelson, *Death & Drama / Cops: Body on Fla. Houseboat Looks Similar to Cunanan*, NEWSDAY, July 24, 1997.

[51] Brown v. Johnston, 328 N.W.2d 510 (Iowa 1983).

[52] Pub. L. No. 108-458 § 6001(a), (b), 118 Stat. 3638, 3742 (2004).

problem is likely to be especially acute during the early stages of an investigation, when agents are just beginning to assemble a picture of the target's intentions. According to the 9/11 Commission, the FBI faced this predicament in the weeks before 9/11. Agents believed that Zacarias Moussaoui – then in federal custody on immigration charges – was a terrorist.[53] Among other reasons for their suspicions, Moussaoui had paid cash at a flight school to learn how to fly a Boeing 747 jumbo jet, but he had no interest in becoming a commercial pilot. Investigators hadn't yet connected Moussaoui to any foreign terrorists, so it was unclear whether they could use FISA to search his apartment or laptop.[54] The 9/11 Commission later speculated that, if agents had investigated Moussaoui more fully, they might have unraveled the entire September 11 plot.[55]

Second, there's the growing danger of entrepreneurial terrorism. As Homeland Security Secretary Janet Napolitano warned last month, "[t]he terrorist threat facing our country has evolved significantly in the last 10 years – and continues to evolve"; we now "face a threat environment where violent extremism is not defined or contained by international borders."[56] Solitary actors who are inspired by foreign terrorist organizations like al Qaeda, or radical clerics like Anwar al-Awlaki, are capable of causing just as much death and destruction as those who are formally members of such networks. Indeed, some of the most chilling terrorist plots to emerge in recent years have involved operatives who may have been acting on their own, not at the direction of an overseas group. In November 2009, U.S.-born Army physician Nidal Malik Hasan opened fire on dozens of unarmed soldiers at Fort Hood, Texas, wounding 32 and killing thirteen.[57] In late February, a Saudi student named Khalid Aldawsari was arrested after planning to bomb the homes of former president George W. Bush and several soldiers who had served at Abu Ghraib prison in Iraq.[58] This trend toward entrepreneurial terrorism is on the rise and shows no signs of abating. (Candidly, the lone wolf provision could not be used to investigate all of these plots. A number of solitary terrorists are U.S. citizens or lawful permanent resident aliens, and the present version of lone wolf does not apply to them.[59])

The lone wolf fix helps investigators overcome these evidentiary difficulties, and meet this evolving terrorist threat, through a simple change to the Foreign Intelligence Surveillance Act. In particular, FISA provides that agents may not conduct surveillance unless they persuade the FISA court that there is probable cause to believe that the target is a "foreign power" or an "agent of a foreign power."[60] Lone wolf tweaked the latter definition. The term "agent of a

---

[53] NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT 273 (2004).

[54] *Id.* at 276.

[55] *Id.*

[56] Keith Johnson, *Officials Warn of Domestic Terrorism Threat*, WALL ST. J., Feb. 10, 2011.

[57] Richard A. Serrano, *Failures by FBI, Pentagon Contributed to Ft. Hood Massacre, Report Says*, L.A. TIMES, Feb. 3, 2011.

[58] Peter Finn, *FBI: Saudi Student Bought Materials for Bomb, Considered Bush Home as Target*, WASH. POST, Feb. 25, 2011.

[59] 50 U.S.C. § 1801(b)(1).

[60] *Id.* § 1805(a)(2).

foreign power" has always included a non-American who is a "member" of "a group engaged in international terrorism or activities in preparation therefor."[61] Now, the term also includes a non-American who "engages in international terrorism or activities in preparation therefor."[62] As a result of this change, investigators may obtain a FISA court order to monitor any target who is engaging in international terrorism. There is no longer any need to make the additional showing that he is acting on behalf of a foreign terrorist organization. Note that this authority has a critical restriction: It does not apply to United States persons – i.e., persons who are either U.S. citizens or lawful permanent resident aliens. Americans cannot be surveilled under the lone wolf provision as it currently stands.[63]

As with the other two authorities that are up for reauthorization, lone wolf features important protections for privacy and civil liberties. Chief among them is the requirement of ex ante judicial approval. FBI agents cannot start monitoring a suspected lone wolf on their own; they must appear before the FISA court and convince it to authorize the surveillance.[64] Second, lone wolf still requires investigators to establish that a given target has a foreign nexus. The tool can only be used to investigate people who are engaging in "*international* terrorism."[65] This means it must be shown, among other things, that the suspects' activities involve "violent acts or acts dangerous to human life" that either "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."[66] Lone wolf thus cannot be used to investigate persons suspected of engaging in domestic terrorism.[67] Finally, FISA's minimization requirement applies to lone wolf surveillance, offering protection to the innocent Americans with whom the lone wolves come into contact.[68]

* * *

The terrorist threat isn't going away anytime soon. Al Qaeda and its followers are still mortal dangers to Americans at home and abroad, and Congress should make sure that our counterterrorism agents have the tools they need to detect and disrupt our enemies' bloody plots. This is no time to dismantle the USA PATRIOT Act. The three provisions that are on the verge of expiring – roving wiretaps, business records, and lone wolf – have been on the statute books for years without compromising vital privacy interests or civil liberties. Not only does the PATRIOT Act let counterterrorism agents use some of the same investigative techniques that

---

[61] *Id.* § 1801(a)(4), (b)(1)(A).

[62] *Id.* § 1801(b)(1)(C).

[63] *Id.* § 1801(b)(1).

[64] *Id.* § 1805(a).

[65] *Id.* § 1801(b)(1)(C) (emphasis added).

[66] *Id.* § 1801(c)(1), (3).

[67] *Cf.* United States v. United States District Court ("Keith"), 407 U.S. 297, 309 n.8 (1972) (using the term "domestic organization" to refer to "a group or organization (whether formally or informally constituted) composed of citizens of the United States and which has no significant connection with a foreign power, its agents or agencies").

[68] 50 U.S.C. § 1801(h).

regular cops and prosecutors have had in their arsenal for years. The act's safeguards and protections are at least as robust as – and in some cases are even more robust than – their law enforcement counterparts. Congress should promptly reauthorize these authorities before they sunset later this year.

Al Qaeda hasn't given up. We can't afford to either.

Mr. SENSENBRENNER. Thank you, Mr. Sales.
Mr. Sanchez?

TESTIMONY OF JULIAN SANCHEZ, RESEARCH FELLOW, CATO INSTITUTE

Mr. SANCHEZ. Thank you, Mr. Chairman, and thanks again to the Committee for soliciting Cato's perspective on these important issues.

I am drawing in my remarks today on a forthcoming Cato paper focusing on these issues, which I hope to be able to make available within the next few days. I just want to pull out a few important issues about each provision here.

With respect to lone wolf, I think it is important to recall that prior to the passage of this provision, the architecture of FISA tracked the constitutionally salient distinction made by a unanimous Supreme Court in the Keith case between ordinary national security investigations and those involving foreign powers which present special challenges and obstacles to investigations. In the absence of those special needs, which may justify the extraordinary breadth and secrecy of FISA surveillance, I think the criminal authority that a bipartisan Senate report found would have been available and, indeed, was used on 9/11 to obtain records and the laptop of Zacarias Moussaoui should be the norm. It is just hard to see why that authority is justified when we are dealing with persons who don't have access to the resources of a global terror network.

With respect to roving wiretaps, I think it is important to emphasize that everyone agrees that roving authority should be available to intelligence investigators as it is in criminal cases, but that the same requirement of identifying a named target that the Ninth Circuit emphasized was crucial to allowing that criminal authority to meet the particularity requirements of the Fourth Amendment and limit the discretion of investigators so that, as the Ninth Circuit put it, there was virtually no possibility of error or abuse, be added on this side to match.

Now, again, the roving surveillance constitutes about 22 of the FISA warrants issued every year, which is a tiny fraction of FISA surveillance. Most of those cases we have to assume do, in fact, involve a named target. So closing this loophole would affect a relatively tiny percentage of FISA warrants issued.

I think it is also important to recognize that on the criminal side, there are important structural differences between the way surveillance is subject to scrutiny after the fact. The FISA Court may be informed about the nature of roving surveillance, but what we don't have on the FISA side is the assumption that surveillance collection is for the purpose of criminal trial where the parties will learn that they have been targeted by surveillance, where defense counsel will have an opportunity to seek disclosure and have an incentive to impose that kind of distributed surveillance of the enormous volume of collection. Again, recall, we are talking about surveillance that takes in essentially hundreds of years' worth of audio every year, millions of digital files. Without that kind of distributed scrutiny, there is much greater need for checks on the front end limiting the discretion of agents, especially in the context of online surveillance where I think, again, we are not in the situation at all where there is, as the Ninth Circuit put it, virtually no possibility of error or abuse.

Finally, with respect to section 215—and I want to suggest that 215 orders and national security letters be grouped together. These are complementary orders, and so changes to one authority are likely to affect the scope of the other. The Inspector General found that it is the extraordinary breadth of national security letters that account for the relatively sparing use that has been made of section 215.

I would like to see greater use made of 215 insofar as that would replace essentially agency fiat with judicial scrutiny. I don't need to recount for the Committee the widespread and serious abuse that the Inspector General has found in the case of national security letters. I do want to mention that former Senator Russ Feingold believes that 215 has been misused but was unable to specify in an unclassified setting what that might consist of.

But I think it may actually be a mistake to focus too much on formal misuses of authorities that are already so broad and that after the PATRIOT Act permit records to be acquired that pertain to people who have no even suspected connection to the target of a terror investigation. This creates a situation where we have enormous and ever-growing databases consisting of billions of records about Americans who again are not under suspicion. These third party records are generally subject to less Fourth Amendment scrutiny which is why the probable cause standard here as a general rule doesn't apply. But in the last decade, we have seen courts increasingly finding that certain categories of third party records like location information do, in fact, merit Fourth Amendment protection in a way that has previously been assumed not to obtain. And there are other First Amendment interests often implicated by, in particular, telecommunication records. And so I would suggest that the analogy between these criminal side authorities is not always appropriate.

[The statement Mr. Sanchez follows:]

Statement of Julian Sanchez
Research Fellow
Cato Institute
Before the United States Senate Judiciary Committee
Subcommittee on Crime, Terrorism and Homeland Security
"The Reauthorization of the PATRIOT Act"
March 9, 2011

It is nearly a decade now since Congress responded to the terror attacks of September 11th by passing the USA PATRIOT Act, a sprawling piece of legislation comprising hundreds of amendments to an array of complex intelligence and law enforcement statutes. As The Washington Post noted at the time, "members of both parties complained they had no idea what they were voting on, were fearful that aspects of the ... bill went too far—yet voted for it anyway."

In recognition of the great haste with which that legislation had been approved, Congress wisely established sunset provisions designed to force review of several of the most controversial elements of Patriot and its successors. While a number of judicious improvements to the original statue have already been made, these emergency powers should not be made permanent until they are further tailored to ensure that the tools employed to investigate and apprehend terrorists are consistent with our Constitutional tradition of respect for the privacy and civil liberties of innocent Americans.

My testimony today is based on a forthcoming Cato policy paper that examines these provisions in much greater detail, and with the indulgence of the chair, I request that it be included in the record.

Lone Wolf

The extraordinary tools available to investigators under the Foreign Intelligence Surveillance Act (FISA), passed over 30 years ago in response to revelations of endemic executive abuse of spying powers, were originally designed to cover only "agents of foreign powers." The Lone Wolf provision severed that necessary link for the first time, authorizing FISA spying within the United States on any "non-U.S. person" who "engages in international terrorism or activities in preparation therefor," and allowing the statute's definition of an "agent of a foreign power" to apply to suspects who, bluntly put, are not in fact agents of any foreign power. As of late 2009, the Justice Department indicated that it had not had a need to invoke Lone Wolf authority.

The original impetus for Lone Wolf was the concern that the absence of such authority had prevented the FBI from obtaining a FISA warrant to search the laptop of so-called "20th Hijacker" Zacarias Moussaui. But as with so many of the intelligence gaps that preceded 9/11, it now appears that the real problem was a failure to connect the dots, not an inability to collect enough dots. A bipartisan 2003 report from the Senate Judiciary Committee notes that on 9/11, investigators were

able to obtain a conventional warrant on Moussaui using evidence already in their possession. More importantly, the report concluded that a FISA warrant could, in fact, have been sought earlier, but supervisors at FBI Headquarters had failed to link related reports from different field offices, or to pass those reports on to the lawyers in charge of processing FISA applications.

That it had not been used at the time of the last reauthorization debate suggests that the provision remedied no dire gap in existing surveillance authorities. Lone Wolf does, however, threaten to blur the vital and traditional distinction in American law between domestic national security investigations and foreign intelligence, where courts have always extended greater deference to the executive branch. In the seminal "Keith" case, holding that the Fourth Amendment's warrant requirement applied with full force to domestic national security investigations, the Supreme Court stressed that there was no "evidence of any involvement, directly or indirectly, of a foreign power," suggesting that this was the key factor separating two constitutionally distinct realms.

While the statutory definition of "international terrorism" does still require some international nexus, a recent analysis by the Transactional Records Access Clearinghouse at Syracuse University suggests that government entities apply this classification inconsistently—with a substantial percentage of cases categorized as "terror related" by the Justice Department not identified that way by courts or federal prosecutors. It is not unreasonable to worry that, without the anchor of a demonstrable connection to a foreign power, it may be used in the future to invoke the sweeping powers of FISA for investigations involving non-citizens that would more properly be classified as ordinary criminal inquiries.

Once someone is designated an "agent of a foreign power," as the FISA court has explained, information collection is "heavily weighted toward the government's need for foreign intelligence information," meaning "acquisition of nearly all information from a monitored facility or a searched location," with the result that "large amounts of information are collected by automatic recording to be minimized after the fact." This is in sharp contrast to the more narrowly targeted surveillance authorized under the aegis of title Title III's criminal wiretap provisions.

These significant differences may make sense in the context of spying aimed at targets who have the resources of a global terror network to draw upon, and who will often be trained to employ sophisticated countersurveillance protocols in their communications with each other. But they also necessarily entail that any investigation authorized under FISA will tend to sweep quite broadly, collecting a more substantial volume of information about innocent Americans than would be the norm in the criminal context. While this may be necessary in light of the special challenges of investigating the heightened threat posed by sophisticated teams of Al Qaeda–trained terrorists, there is little reason to think the FBI cannot deal with loners radicalized by watching foreign YouTube videos using more conventional investigative tools.

By its own terms, Lone Wolf authority would only be available in circumstances where the standard for Title III surveillance has already been met. In the absence of the special needs created by the involvement of foreign powers, therefore, reliance on that authority should be the norm.

Roving Wiretaps

Section 206 of the Patriot Act established authority for "multipoint" or "roving" wiretaps under the auspices of the Foreign Intelligence Surveillance Act. In 2009, FBI Director Robert Mueller testified that roving authority under FISA had been used 147 times.

Roving wiretaps have existed for criminal investigations since 1986, and even the staunchest civil libertarians agree that similar authority should be available for terror investigations conducted under the supervision of the Foreign Intelligence Surveillance Court.

But in order to meet the "particularity" requirements of the Fourth Amendment, criminal roving wiretaps are required to name an identified target. As the Ninth Circuit explained in upholding that authority:

> The statute does not permit a "wide-ranging exploratory search," and there is virtually no possibility of abuse or mistake. Only telephone facilities actually used by an identified speaker may be subjected to surveillance, and the government must use standard minimization procedures to ensure that only conversations relating to a crime in which the speaker is a suspected participant are intercepted.

The Patriot Act's roving wiretap provision, however, includes no parallel requirement that an individual target be named in a FISA warrant application, giving rise to concerns about what have been dubbed "John Doe" warrants that specify neither a particular interception facility nor a particular, named target. Even with the safeguards imposed during the previous reauthorization, this is disturbingly close to the sort of "general warrant" the Founders were so concerned to prohibit when they crafted our Bill of Rights.

The breadth of FISA surveillance makes inadvertent overcollection especially likely when a description of an unknown target initially linked to a particular "facility" is used as the basis for interception across an ever-growing variety of diverse online services. With criminal roving wiretaps, the discretion of the investigator is generally limited to one inferential leap—that this same known person is making use of a new facility—limiting the probability of error. But since same username, account, or IP address will often—sometimes unwittingly—be used by multiple people at different times or places, that inferential gap is dramatically widened without the anchor of a named target.

Moreover, intelligence wiretaps lack an important type of distributed after-the-fact safeguard that exists in the criminal context, where the purpose of surveillance is

generally to produce admissible evidence at trial. Investigators know that their targets will eventually be notified of the wiretap, and defense attorneys armed with a right of discovery will have an incentive to uncover any improprieties. FISA surveillance normally remains covert, and post-hoc scrutiny by the FISA Court or sporadic Inspector General audits cannot realistically provide a substitute. Bear in mind that, in fiscal 2008 alone, the FBI collected 878,383 hours (or just over 100 years) of audio, much of it in foreign languages; 1,610,091 pages of text; and 28,795,212 electronic files—the bulk of it pursuant to FISA warrants. The Inspector General has found that much of that material cannot be reviewed in a timely fashion by the Bureau itself—never mind independent overseers.

At the very least, then, the absence of these systemic "back-end" safeguards entails that the "front-end" checks on the scope of interception need to be as strong under FISA as they are under the parallel criminal authority.

§215 Orders and National Security Letters

Unlike the enhanced authority to obtain business records and other "tangible things" under section 215 of the Patriot Act, expanded National Security Letters are not currently scheduled to sunset. But I believe it is important to consider these two complimentary powers together. As the Inspector General has made clear, the use of judicially authorized 215 orders has been limited by both internal awareness of the continuing political controversy surrounding them and—more importantly—the extraordinary breadth of National Security Letters.

There would be little point in tightening the requirements on a tool used a few dozen times per year with judicial supervision without also reforming the authority invoked *tens of thousands* of times annually, at the discretion of FBI supervisors, to acquire the sensitive financial and telecommunications records of Americans who are not even suspected of involvement in terrorism. Conversely, whatever changes to NSL authority may be contemplated in light of the "widespread and serious misuse" of that authority uncovered by the Inspector General, it is important to bear in mind that limitations on NSLs are likely to increase reliance on §215. That would be welcome development insofar as it would substitute judicial approval for administrative fiat, but may reduce what currently appears to be a high level of engagement by the FISC in narrowing overbroad applications.

While both powers have been expanded along multiple dimensions since 9/11, the main cause for concern in both cases has been the removal of the requirement that there be some evidence—not "probable cause," but *some* evidence—linking the people whose records are sought to terrorism or espionage. Now records need only be "relevant" to an investigation, and in the case of §215 orders the court is *required* to deem records "relevant" if they pertain to someone connected, however tenuously, to a suspect under investigation. As the Justice Department readily acknowledges, these tools are used in the early phases of an investigation to broadly

sweep in large amounts of data, mostly about innocent people, which is then stored indefinitely in classified government databases.

Here, again, we should bear in mind that while the easiest and most obvious response to any intelligence failure is always to grant more power to collect more information, the evidence is very thin that the problem before 9/11 was a lack of raw data. On the contrary, reflexively expanding collection authorities can exacerbate what has been colorfully characterized as the problem of "drinking from a firehose." This can even lead to a vicious cycle, where it comes to seem that more and more data is needed to close down all the dead-end leads generated by indiscriminate data collection.

Since these powers are often compared by their proponents to administrative or grand jury subpoenas—on the premise that they only provide "the same" authorities already available to criminal investigators—some crucial distinctions should be borne in mind. First, those tools are generally focused on either the activities of heavily regulated corporate entities (in the first case) or on some specific crime that already has been or is being committed, and in the latter case, the grand jury is meant to serve—in theory if not always in practice—as a "buffer or referee between the government and the people," to borrow the words of Justice Scalia.

Second, it is impossible to overstate the significance of the *transparency* that normally surrounds the acquisition of documents by those means. This acts as a powerful check on government overreach in itself, but also creates a vital incentive to challenge improper demands. The recent case of *Google v. Gonzales* is illuminating here: In an effort to gather information for litigation over the Child Online Protection Act, the government served Google with a subpoena for a sample of the search queries entered by users in a particular time period. Google moved to quash the subpoena on the grounds that it would lose the trust of users if it were publicly seen to comply with such a broad request. The court—emphasizing its independent concern for the privacy of those users more than the potential harm to Google's reputation—agreed.

By contrast, the widespread misuse of National Security Letter authority described by the Inspector General took place with not just the compliance, but often the enthusiastic encouragement of the telecommunications companies. Many of the violations of these powers that have been reported involve the overproduction of records by custodians who have every incentive to err on the side of turning over the maximum amount of information.

Finally, the last decade has seen the courts beginning, however belatedly, to recognize the need for exceptions to the so-called "Third Party Doctrine" established in the very different technological context of the 1970s, according to which people lack a Fourth Amendment "reasonable expectation of privacy" in records maintained by third parties. This was the basis for the federal statute recently invalidated by the Sixth Circuit, which allowed e-mail to be obtained without a

probable cause warrant under some circumstances. Similarly, a growing number of courts are concluding that the information about people's physical location contained in cell phone records is subject to Fourth Amendment protection.

There are also important First Amendment interests implicated by monitoring of communications records in particular. The Supreme Court has long held that the rights of free expression protected by the First Amendment encompass a right to anonymous political speech—and I should point out here that the Cato Institute itself is named for a famous series of pseudonymous political pamphlets defending individual liberty against government power—a right to "receive information and ideas," and a right to "expressive association" without state scrutiny into the membership lists of the political organizations through which it is exercise, especially when those organizations are unpopular. Here, too, courts are increasingly recognizing the need for heightened standards when subpoenas would burden these vital interests.

In the intelligence context, associational interests would appear to be implicated by the routine use of business record authorities to map "communities of interest" or conduct "link analysis" using telecommunications records at two or three removes from the actual target of investigations. Judicial scrutiny can mitigate these concerns somewhat: Thanks again to the Inspector General, we know of at least one case in which the FISA court rejected a §215 application on the grounds that it targeted protected speech. Undeterred, however, the FBI went ahead and obtained the same information using National Security Letters.

Of special concern here is a "sensitive collection program" involving §215 alluded to by Acting Assistant Attorney General Hinnen last year in his testimony on these authorities. Though the Senate had previously unanimously approved an amendment limiting §215 authority to records pertaining to the activities of terror suspects or their associates, a similar reform appears to have been abandoned last year following claims by the Justice Department that such a change would hamper that secret program. Soon afterward, Sen. Russ Feingold purported to have knowledge of clear misuse of §215 unknown to the general public.

If nothing else, I would urge those with access to the relevant details to take a long, hard look at that. But I would also suggest that we should be highly skeptical of any intelligence program that cannot function within even those very modest limitations. The United States was able to observe the time-tested principle of individualized suspicion in a decades-long conflict with a hostile empire armed with nuclear weapons. We should not assume it is an insuperable handicap against scattered bands of religious fanatics.

Conclusion

As a final observation, I want to suggest that formal improprieties at the acquisition stage—while certainly very serious, especially in the case of National Security Letters—are not the sole cause for concern about these broad surveillance powers.

It would be more worrying, after all, if standards were lowered and safeguards weakened so far that *nothing* counted as a "misuse." The real danger is that the formally lawful collection of records is giving rise to a set of ever-growing databases—the FBI's comprising billions of records at last count—overflowing with potentially sensitive information about innocent Americans and their constitutionally protected activities.

As the recent publication of classified military and State Department records by Wikileaks demonstrates all too clearly, just one of the thousands of people with access to a database—whether inspired by misguided idealism or more sinister motives—can compromise an enormous amount of information. When that information is published on the Internet for all to see, however, it's at least possible to assess the extent of the harm and seek to identify the responsible parties. Similarly, when information obtained for intelligence purposes, subject to intelligence rules, is passed on to criminal prosecutors, we at least know that the safeguards of the criminal justice system remain in place.

But the ugly history of American intelligence abuses suggests that the gravest threat in this sphere involves the *secret* deployment of information for political purposes—the most notoroious example being the attempt to exploit recordings of Martin Luther King's extramarital liaisons to drive the civil rights leader to suicide. It was a commonplace, in my former life as a journalist, to say that fact-checking will catch a sloppy reporter, but not one intent upon deception. By the same token, internal oversight and auditing are reasonably good at catching honest mistakes. But under the veil of secrecy surrounding intelligence, the only sure way to prevent willful misuse of information about innocent Americans is to

You sometimes hear it said that civil libertarians are trapped in a "pre-9/11 mindset," stubbornly refusing to adapt to the demands of a world where non-state adversaries wield terrifying destructive capabilities. I would like to believe that's not true: With at respect to at least two of the three authorities under consideration today, I would not question whether the government should *have* these tools to investigate terrorists—but only how they should be tailored to ensure that they are focused on *terrorists* without intruding on the privacy of innocent Americans any further than is necessary to safeguard national security.

But I think it would be an equally serious mistake to lapse into what we might call a "pre–Church Committee mindset", to forget *why* we established a series of safeguards against overbroad surveillance, and to assume that abuse of intelligence powers can only happen in places like Egypt or China or Iran. As our Founders understood, and as the history of the 20th century teaches us, it can—and indeed did—happen here. If we lose sight of that historical lesson, history suggests it may be decades more before we know our mistake.

Mr. SENSENBRENNER. Thank you very much.

The Chair will now recognize the Members alternatively by sides in the order in which they appear after Mr. Scott and I are able to question the witnesses. And I yield myself 5 minutes.

Mr. Sanchez, you really haven't complained very much about the section 215 orders and have taken off after the national security letters to a much greater extent. Are you aware that the national security letters were authorized in 1986 legislation sponsored by Senator Leahy?

Mr. SANCHEZ. I am, of course. But I believe it is important——

Mr. SENSENBRENNER. No, no. Okay. You know that that was not a part of the original PATRIOT Act.

Are you aware that there were civil liberties protections that were put into the national security letter statute at the time of the 2006 reauthorization?

Mr. SANCHEZ. Certainly.

Mr. SENSENBRENNER. What is wrong with those protections?

Mr. SANCHEZ. Well, I think the problem here is that as, for example, the recent WikiLeaks disclosures have made clear, when databases, however protected or classified they may be, are allowed to contain so many records about so many different people without the requirement of some sort of individualized suspicion, it takes only really one bad actor to enable enormous disclosure of——

Mr. SENSENBRENNER. But does that mean that the tools of section 215 and the national security letters should be completely thrown out the window because of one bad actor?

Mr. SANCHEZ. No. What I would suggest, however——

Mr. SENSENBRENNER. Okay. Well, then when the reauthorization was done, section 215 was declared unconstitutional by a Federal court. I believe it was in Michigan. And after the Congress did the reauthorization that many of my friends opposed, the plaintiffs withdrew their lawsuit. Now, were the changes that caused the plaintiffs to withdraw their lawsuit inadequate in any respect, and if so, how?

Mr. SANCHEZ. Well, I would suggest, again to return to what I alluded to——

Mr. SENSENBRENNER. Answer the question if they were inadequate in any respect.

Mr. SANCHEZ. I believe that one the changes that was considered by not implemented ultimately but that was approved by the Senate unanimously creating a requirement that there be at least a one-removed nexus to a terror suspect would have narrowed that authority in a way that——

Mr. SENSENBRENNER. But section 215 is directed at people who hold business records, and the courts have already determined that they are not subject to the protections of the Fourth Amendment because the potential criminal defendant or terrorist, if you would, was not in possession of those records. And there is a pretty significant difference that the courts have recognized.

Now, you know, again I am asking if the protections were inadequate.

Mr. SANCHEZ. Well, let me suggest two differences.

Mr. SENSENBRENNER. No. Just tell me how they were inadequate because there hasn't been a ruling of unconstitutionality.

Mr. SANCHEZ. Nor, of course, covert authorities and so——

Mr. SENSENBRENNER. You know, yes, they are, but in the amendments, we gave anybody who got a section 215 FISA Court order

the opportunity to go to court and to get it quashed or cancelled, and to my knowledge, there has been no court that has done that.

Mr. SANCHEZ. Well, if you look at what the Inspector General has found about——

Mr. SENSENBRENNER. No. I am looking at what the courts have been saying, sir. You know, the Inspector General has got an opinion just as the Attorney General has an opinion. I don't know that since the changes in 2006 were made there has been any finding by a court that there is unconstitutionality.

Mr. SANCHEZ. One problem is that in the criminal context where——

Mr. SENSENBRENNER. But we are not talking about the criminal context. We are talking about FISA here.

Mr. SANCHEZ. But I wanted to suggest a contrast in that——

Mr. SENSENBRENNER. No. There is no need for a contrast because we are talking about either extending a provision of FISA or letting a provision of FISA drop.

Mr. SANCHEZ. The third option, though, would be to extend it suitably narrowed to compensate for the fact that third party record custodians, where the acquisition of records does not ultimately become public, lack the incentive that they have on the criminal side and we see frequently in challenges to subpoenas for records that——

Mr. SENSENBRENNER. Well, just because they don't have the incentive doesn't take away their right to go to court to get it quashed.

Okay. Let me talk about roving wiretaps. You know, we have heard from the previous witnesses that if roving wiretaps are okay for the Sopranos, you know, why not for Mohamed Atta. Why not for Mohamed Atta?

Mr. SANCHEZ. I do not oppose these roving wiretaps in intelligence investigations.

Mr. SENSENBRENNER. Okay, thank you very much.

My time has expired.

The gentleman from Virginia, Mr. Scott?

Mr. SCOTT. Thank you, Mr. Chairman.

Mr. Hinnen, on the lone wolf provision, it is my understanding that these cannot be used against U.S. persons. Is that right?

Mr. HINNEN. That is correct.

Mr. SCOTT. Are they limited to terrorism as opposed to routine foreign intelligence?

Mr. HINNEN. Yes. The statutory definition requires that the individual be engaged in or preparing for international terrorism.

Mr. SCOTT. And what do you need to represent to a court to get a lone wolf——

Mr. HINNEN. You need to demonstrate to the court probable cause that the individual is engaged in or preparing for international terrorism and probable cause that he is using or is about to use the telephone that you want to surveil.

Mr. SCOTT. The information that you have to show that—would that not be sufficient to get a Title III normal criminal warrant?

Mr. HINNEN. It might in some cases.

Mr. SCOTT. How can you have that information and it not be sufficient? How could it not be sufficient?

Mr. HINNEN. It may in most cases be sufficient. I think that because the criminal statute requires proof of probable cause that a crime is being committed, whereas the FISA statute requires probable cause that the individual be engaged in or preparing to engage in international terrorism, there is a possibility that there might be some slight difference, but I will certainly grant the Congressman's point——

Mr. SCOTT. International terrorism is a crime.

Mr. HINNEN [continuing]. That they are very similar.

Mr. SCOTT. International terrorism is a crime. Is that right?

Mr. HINNEN. There are jurisdictional elements to criminal statutes as well, and we need to ensure that those are satisfied.

Mr. SCOTT. On 215, you are entitled to get information relevant to foreign intelligence. Is that right?

Mr. HINNEN. That is correct.

Mr. SCOTT. Is that limited to terrorism?

Mr. HINNEN. No, that is not limited to terrorism. That includes counter-intelligence as well and information regarding the national defense or foreign affairs.

Mr. SCOTT. Foreign affairs, diplomacy.

Mr. HINNEN. Correct.

Mr. SCOTT. What was done before the USA PATRIOT Act in getting information? What do you get under the PATRIOT Act that you couldn't get otherwise?

Mr. HINNEN. Under these specific authorities?

Mr. SCOTT. Right.

Mr. HINNEN. I think these authorities provide an opportunity for the intelligence community to obtain in a secure way, while at the same time protecting classified information and sources and methods, records that are relevant to national security investigations.

Mr. SCOTT. You couldn't get that before USA PATRIOT Act?

Mr. HINNEN. We could get it before the USA PATRIOT Act. Certainly the grand jury subpoena authority was available then. Of course, the——

Mr. SCOTT. What about just FISA?

Mr. HINNEN. You know, I don't know the answer to that question. I wasn't practicing in this area before the PATRIOT Act.

Mr. SCOTT. Mr. Litt, were you practicing then?

Mr. LITT. I am going out on a limb here. I have a recollection that there may have been some authority prior to the PATRIOT Act that was expanded in the PATRIOT Act, but I am not certain of that. I wouldn't want to be quoted on that. There certainly was NSL authority.

Mr. SCOTT. But, Mr. Hinnen, what you get is information relevant to foreign intelligence. Do you need to show any probable cause of any crime or speculation or terrorism?

Mr. HINNEN. You don't for a business records order. As with the grand jury subpoena——

Mr. SCOTT. Do you have show that the records are connected to a foreign agent?

Mr. HINNEN. Collected through a foreign agent?

Mr. SCOTT. Connected to a foreign agent.

Mr. HINNEN. You need to show that they are relevant to a national security investigation.

Mr. SCOTT. Which includes foreign intelligence, not just terrorism.

Mr. HINNEN. Correct.

Mr. SCOTT. When people hear of national security, they think terrorism, but you are talking just normal diplomacy kind of stuff.

Mr. HINNEN. No. It includes spies and espionage and that sort of thing as well.

Mr. SCOTT. Now, on the roving wiretap, how is the standard to get a roving wiretap different from the normal Title III warrant?

Mr. HINNEN. The difference with respect to a roving wiretap is that the Government has to demonstrate, in addition to probable cause, that the individual is an agent of a foreign power and is using or is about to use a telephone number. The Government also has to demonstrate to the court that the individual may take steps to thwart the surveillance.

Mr. SCOTT. Now, is the roving wiretap under this authority limited to terrorism as opposed to 215 which is any kind of spying?

Mr. HINNEN. No.

Mr. SCOTT. Is the roving wiretap limited to——

Mr. HINNEN. Excuse me. It too permits the collection of foreign intelligence information.

Mr. SCOTT. Which——

Mr. HINNEN. Which is the broad definition that we have been discussing, Congressman.

Mr. SCOTT. And the minimization. You said collection, dissemination, and retention. Does the minimization include collection?

Mr. HINNEN. It does for surveillance, yes, Congressman.

Mr. SENSENBRENNER. The time of the gentleman has expired.

The gentleman from South Carolina, Mr. Gowdy.

Mr. GOWDY. Thank you.

Mr. Sanchez, you cited the Ninth Circuit which from my perspective is the most reversed, least likely to be correct circuit in the country. Can you cite any other authority for your concerns?

Mr. SANCHEZ. As Mr. Sales mentioned, there are three Federal appellate courts that have examined roving wiretaps in the criminal context, and I think—back me up—that all three have stressed the additional requirement in the case of roving taps that a named target be identified as important to allowing those taps to meet the particularity standard.

Mr. GOWDY. Would you agree with me that the United States can indict Fnu Lnu?

Mr. SANCHEZ. Yes.

Mr. GOWDY. Well, then why can't they investigate Fnu Lnu?

Mr. SANCHEZ. I am not opposed to investigation and certainly of persons who are reliably believed to be connected to terror groups. The issue is not whether the investigation should happen but what constraints should exist to narrow the investigation to ensure that the information pertaining to innocent people is not swept up especially given the relative lack of the kind of back-end constraints that exist in the criminal context.

Mr. GOWDY. Well, if you don't know the name of the person, if his first name is unknown and his last name is unknown, how are you going to investigate him under your recommendations?

Mr. SANCHEZ. Well, if his first name is unknown and the last name unknown, how are you sure you are investigating that person?

Mr. GOWDY. There are lots of people in the criminal context that you know a crime was committed. You don't have any idea what their first name or last name is. Trust me from 16 years of doing it. A name is sometimes the last piece of information that you get.

Mr. SANCHEZ. And what can be done in that context is to target a facility. Again, both FISA and criminal warrants permit a facility where there is an evidentiary nexus connecting it to a crime or in this case an agent of a foreign power can be specified. The question is whether the agent in a case where the target is not known, where there isn't that anchor, has discretion to choose new facilities not——

Mr. GOWDY. When you say the target is not known, there is a difference between not being known and not being identified. Correct?

Mr. SANCHEZ. It borders on metaphysics, but yes.

Mr. GOWDY. Well, it doesn't border on metaphysics. It is a fact. You can not know the identity of someone and still know that that person exists. Correct?

Mr. SANCHEZ. Certainly.

Mr. GOWDY. So there is a difference between being identified and being known.

Mr. SANCHEZ. And when a target is known by description, which will often be connected to the facility which is originally monitored, I think that anchor should limit the extent of the warrant until identification of information about the identity of that person can be obtained.

Mr. GOWDY. You don't have serious concerns about the roving wiretap. Correct? If I understood your testimony correctly.

Mr. SANCHEZ. If it is narrowed to match the criminal authority, no.

Mr. GOWDY. You are upset about national security letters, but that is not part of what we are doing.

Mr. SANCHEZ. I was tying those with——

Mr. GOWDY. But that is not part of this reauthorization.

Mr. SANCHEZ. That is true.

Mr. GOWDY. So roving wiretaps, not that much of an issue with roving wiretaps.

Lone wolf——

Mr. SANCHEZ. There is potential for roving—for these John Doe warrants, but I think that is, again, a very narrow set of cases. And so closing that loophole would——

Mr. GOWDY. We have Fnu Lnu indictments. That would even be worse than a Fnu Lnu warrant. Wouldn't it? I mean, we indict unknown people.

Mr. SANCHEZ. In the context of a criminal investigation where the point is, of course, to identify that person and to have trial in a public fashion.

Mr. GOWDY. Business records. A Federal prosecutor can send a subpoena without going to any Article III judge and getting permission, without getting any permission from anyone, can do it on behalf of a grand jury anytime she or he wants to. Correct?

Mr. SANCHEZ. Yes.

Mr. GOWDY. So you would agree that there is an additional layer of protection in these cases that doesn't even exist in drug cases or child pornography cases or carjacking cases or bank robbery cases.

Mr. SANCHEZ. But there is an absent layer of protection insofar as there is no independent grand jury in these cases and also insofar as the secrecy removes——

Mr. GOWDY. Wait a second. What do you mean there is an absence? You think an Article III judge who has a job for life is less independent than a grand jury?

Mr. SANCHEZ. Well, there is a difference in terms of the nature of the scope of the investigation. Again, on the criminal side, we are talking about in most cases some kind of nexus to a crime that has been or is being committed. And then again——

Mr. GOWDY. But you would concede we cannot wait in these cases until a crime is committed. So that analogy falls. I mean, the goal is not to wait until a crime has been committed in these cases and then do a really good job prosecuting it. Correct?

Mr. SANCHEZ. But to the extent that scope difference creates more discretion, additional protections I think are appropriate.

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

The junior Chairman emeritus of the Committee, the gentleman from Michigan, Mr. Conyers?

Mr. CONYERS. Thank you, Mr. Chairman.

Mr. Hinnen and Mr. Litt, I understand that the Judiciary Committee in the other body is considering a bill that would make some changes in some of this law that we are discussing, S. 290. Do any of you have any operational concerns about anything in this bill that you would like to bring to our attention this afternoon?

Mr. HINNEN. Mr. Ranking Member, I am not sure exactly which bill S. 290 is. Who is the sponsoring Senator, please?

Mr. CONYERS. Chairman Leahy.

Mr. HINNEN. Congressman, Mr. Ranking Member, with the caveat that that bill is currently going through markup or at least was until very recently and we may not have reviewed the most recent set of changes, the Administration had reached a point where it was supporting a very similar bill to that at the end of the last Congress when these provisions were set to expire. So without knowing every jot and title that may have been changed in the recent markup, we are prepared to support a bill that is similar to the one that was considered at the close of the last Congress.

Mr. CONYERS. Mr. Litt?

Mr. LITT. Mr. Ranking Member, that bill—I think the provisions in there are examples of the kinds of provisions that I described in my statement as provisions that would provide enhanced protection for civil liberties without affecting operational utility. So, yes, that is our view on those.

Mr. CONYERS. Thank you both.

Mr. Sanchez, it has been a fairly difficult afternoon, hasn't it? [Laughter.]

Mr. SANCHEZ. I am having fun.

Mr. CONYERS. Could I inquire if you are an attorney?

Mr. SANCHEZ. I am not.

Mr. CONYERS. Well, that may account for some of the difficulty.

What would you tell a Member of this Committee this afternoon who might be thinking about voting against this 3-year extension?

Mr. SANCHEZ. Well, first of all, in terms of the operational impact, there is a grandfather clause. That means these powers would continue to be in effect for investigations already underway. So the immediate operational impact I think would likely be limited by that.

I would suggest that certainly all three appear to—well, in one case, not used at all; in the other cases, used in a fairly limited way.

But I would suggest that at least with respect to roving wiretaps in 215, what would be desirable is to sufficiently constrain them so that they are narrowed to minimize the collection of information about innocent Americans in a way to account, again, for the structural differences between intelligence and criminal investigations and that fixing these provisions so that they can be made permanent is actually preferable to allowing them to expire.

Mr. CONYERS. Does anyone here want to comment on that suggestion?

Mr. HINNEN. I would just say, Congressman, that I think the reference to a distinction in the constitutional architecture between a group and an individual—I actually, with due respect, disagree with the assertion that that is what Congress did in 1978 and that that is what the Keith case does. What those cases do and what the Fourth Amendment cases that focus on this do is distinguish between the Government's interest in criminal investigation and the Government's interest in protecting the national security. They don't distinguish between—the distinction of constitutional significance is not one between an individual and a group.

Mr. LITT. I think from the intelligence community's point of view, we certainly share the hope that we can reach the stage where these authorities can be authorized on a permanent basis. From our point of view, while we encourage oversight, having to run up against repeated expirations is not something that we particularly enjoy doing. I guess at the generic level, I can share the sentiment that I hope we get to the stage where we all agree on what the appropriate way is that we can authorize these permanently. We may disagree as to what the details of that are.

Mr. CONYERS. Professor?

Mr. SALES. I think, if I may—I know we are very short on time. So I will be as brief as I can, which is hard for a professor to do.

I think Congress has struck the right balance with the provisions as they exist. Since the PATRIOT Act was enacted, Congress has revisited these provisions time and time again, each time adding additional layers of oversight and additional safeguards. I think those additional mechanisms to protect privacy and civil liberties would justify a permanent extension of these provisions now without any additional tinkering.

Thank you, sir.

Mr. SENSENBRENNER. The time of the gentleman has expired.

The Vice Chair of the Subcommittee, the gentleman from Texas, Judge Gohmert?

Mr. GOHMERT. Thank you, Mr. Chairman.

I appreciate your all's testimony.

One of the things I got hit up—when we were talking about extending 206, 215 of the PATRIOT Act, was that under 206, apparently somebody had been talking about it on TV that that could allow the FBI to get a wiretap on an entire neighborhood because the person being pursued had used a neighbor's phone before and therefore might be likely to use other people's phones in the neighborhood. Has anybody here ever heard of an entire neighborhood being wiretapped under 206?

Mr. HINNEN. No, Congressman, and I think that would be inconsistent with the terms of the statute which require the Government to demonstrate probable cause that the specific agent of a foreign power is using a specific telephone number.

Mr. LITT. In addition to that, when you do get a roving wiretap order, every time the agents go up on a new telephone, they have to report that to the FISA Court within 10 days and they have to report the specific basis on which they believe that the particular facility was being used. And I would doubt that that would pass muster with the FISA Court if anybody tried that.

Mr. GOHMERT. In my understanding with the roving wiretap, the goals was to go after cell phones that could be disposed of quickly and not give time to go after the new phone. Is that correct?

Mr. HINNEN. And other similar kinds of tradecraft where individuals cycle through providers quickly in order to try and shake surveillance, yes.

Mr. GOHMERT. Professor, do you have any comment on that? Do you think it is plausible, possible even to get a wiretap of an entire neighborhood under 206?

Mr. SALES. No, sir. I think that would be inconsistent with the terms of FISA as it is written. As my colleagues have said, FISA is very clear about what is required in order to initiate surveillance. You must establish, in the case of 206, probable cause to believe that the target is engaging in international terrorism. I think it would be extraordinarily difficult to persuade the FISA Court that there is probable cause to believe that an entire neighborhood is engaging in international terrorism.

In addition, it must be shown that there is probable cause to believe that the target is using a specific facility in question. If there is a terrorist using a phone, then we should be listening to it, but it is inconceivable to me that the FISA Court would approve dragnet surveillance like this. I think that is the most important part. It is the court that decides, not the FBI.

Mr. GOHMERT. Well, Mr. Sanchez, you brought up NSL's. I think most of us were quite alarmed when the IG came in with a report that they had been badly abused and they were not getting the supervision we had been assured that NSL's would get. And you had FBI agents just doing fishing expeditions without proper supervision.

If I understood you correctly, you seem to think that 215 could take care of the needs that are currently given to—or the power that is currently under the national security letters. Is there anybody else that you know of that agrees with that? If you just did away with national security letter power——

Mr. SANCHEZ. I am not proposing doing away with the national security letter power.

Mr. GOHMERT. Oh, you are not? What is your specific proposal?

Mr. SANCHEZ. My suggestion is that if the national security letter authority were narrowed further, for example, as it previously did, to permit the acquisition of records that pertain to a suspected terrorist and in the case of communications records for basic subscriber information for persons believed to be in contact with a suspected terrorist, that narrower authority could allow the kind of initial investigation on the basis of relatively limited records that don't sweep in people 2 and 3 degrees removed. And if that kind of greater breadth is necessary, 215 orders could be employed for those categories of records.

Mr. GOHMERT. So you think national security letters do perform an important function. They just need to be narrowed. Is that correct?

Mr. SANCHEZ. I think that is accurate, yes.

Mr. GOHMERT. I see my time has expired and I yield back.

Mr. SENSENBRENNER. The time of the gentleman has expired.

The gentleman from Georgia, Mr. Johnson?

Mr. JOHNSON. Thank you, Mr. Chairman, for holding this very important hearing.

I have—well, before I go down that line, let me say that section 215, the business records section, can be used against Americans who are alleged to be an agent of a foreign power. Is that correct?

Mr. HINNEN. Yes, that is correct.

Mr. JOHNSON. And you would just simply need specific and articulable facts giving reason to believe that an American may be assisting a foreign power or an agent of a foreign power, in other words, not probable cause but a level below probable cause.

Mr. HINNEN. Certainly the relevant standard is a more lenient or a minimal standard as opposed to probable cause.

What the business records provision actually allows us to do is to get records from a third party custodian, to go to a bank and get an individual's bank records or that kind of thing. And so that is why the importance is demonstrating their relevance to a national security investigation, not necessarily anything specific about the individual because they don't actually act against the individual directly.

Mr. LITT. Let me here—just to be clear, in those FISA authorities which do depend upon a finding that somebody is an agent of a foreign power, that finding is based on probable cause by the court.

Mr. JOHNSON. The finding that the person is an agent of a foreign power looks to me that it simply requires a showing of specific and articulable facts as opposed to probable cause. I am correct on that, am I not?

Mr. HINNEN. That was the distinction, Congressman, I was trying to draw. I don't think I articulated it very well. What the business records provision requires the Government to show is something with respect to the investigation itself rather than something——

Mr. JOHNSON. Yes. Well, I understand that part. That is probable cause, the fact that it may be related to a terrorism or a security investigation, national security.

But the person whose documents are being subpoenaed, if you will—that person can be an American and they can be established as an agent of a foreign power merely through an articulable, reasonable suspicion as opposed to probable cause.

Now, I have serious concerns about the possible abuse and misuse of counter-terrorism technologies developed by Federal contractors under the authority of the PATRIOT Act and the Homeland Security Act. Are either one of you familiar with the recent Chamber leaks controversy?

Mr. LITT. I am sorry. The recent what?

Mr. JOHNSON. Chamber leaks, a situation where there was a group of——

Mr. LITT. The Chamber of Commerce?

Mr. JOHNSON. Yes.

Mr. LITT. I am familiar from reading it in the newspapers, yes.

Mr. JOHNSON. So the technologies that were developed by these security contractors which could have been unleashed on American citizens for domestic illegitimate purposes, the mining of social network sites, the planting of false personas and things like that, false documentation—these are technologies that are depended upon by individuals who are executing their authority under the PATRIOT Act. Correct?

Mr. LITT. Well, I don't specifically know what technologies those people planned to use, but I do know——

Mr. JOHNSON. Let me ask you are you familiar with Palantir Technologies, Bar Code technologies, or HBGary Federal and whether or not the Department of Justice or the national security agency which you belong to, Mr. Litt, contracts with any of those firms for their software?

Mr. LITT. I am familiar with the names of the companies. I don't know whether there are any contracts between the intelligence community and any of those companies.

Mr. JOHNSON. Well, I have asked for a congressional hearing to take place in Judiciary, and I look forward to hearing back from the Chairman of the full Committee as to whether or not there will be hearings held on this most important topic, which is directly related to our subject matter today.

Thank you.

Mr. SENSENBRENNER. The time of the gentleman has expired.

The gentleman from California, Mr. Lungren?

Mr. LUNGREN. Thank you very much, Mr. Chairman.

Mr. Sanchez, you talked about the Ninth Circuit. I am a little familiar with the Ninth Circuit. They were, during the time I had experience with them, the most reversed circuit in the entire United States. I think 1 year they had 19 out of 20 cases reversed; 1 year, 21 out of 22, a number of them that my office brought before the Supreme Court.

But I was interested in the language that you cited as exemplary for what we ought to be using. It really caught my attention because you quoted their language saying that they approved it in the criminal context because there is virtually no possibility of abuse or mistake. I guess my question is, should that be the standard that we use, virtually no possibility of mistake, before we are

allowed to have a roving wiretap in a case in which we are trying to stop an attempted terrorist attack?

Mr. SANCHEZ. Well, I should say in the context——

Mr. LUNGREN. I mean, that is the language that you used. So I assume that you meant that that is the kind of standard we ought to have, virtually no possibility of mistake.

Mr. SANCHEZ. I think in fact, again in particular when we are talking about online surveillance or surveillance of electronic communications, anytime a tap is roving, there is inherently some possibility of error, but that is dramatically magnified without the anchor of——

Mr. LUNGREN. So that would not be your standard. I appreciate that.

Mr. Litt and Mr. Hinnen, sort of the general talk about roving wiretap—can you tell me how many times it has been utilized under section 206?

Mr. HINNEN. I am afraid we don't have that number with us today. As I mentioned in my testimony, we obtain the authorization about 20 times a year. The set of circumstances doesn't always eventuate such that we need to use the authority despite the fact that we have gotten it. So it would be something less than 20 times a year.

Mr. LUNGREN. There would be some people that would believe perhaps, if they heard some of the commentary today, that my goodness, if we don't have the same restrictions that you have in a criminal case, this must give rise to your ability to have a wide-ranging, exploratory search with no specificity. As I read the statute, it doesn't allow that. Could you explain exactly what you have to do in order to obtain the authority for a roving wiretap in a section 206 case?

Mr. HINNEN. Sure. Thank you, Congressman.

The Government has to make three important showings in that case. It has to make the two showings that are required for regular FISA surveillance in any case: probable cause to believe the individual is an agent of a foreign power and probable cause that the individual will use the specific phone number——

Mr. LUNGREN. The individual. It is an individual even though you may not know the individual's name.

Mr. HINNEN. That is correct. I thought Congressman Gowdy did an excellent job of demonstrating the difference between being able to identify someone and being able——

Mr. LUNGREN. But I want to make sure that as you understand the statute, it requires you to have some specificity with respect to an individual who is the target of your inquiry.

Mr. HINNEN. That is correct, Congressman. Specificity both with respect to a specific individual and with respect to a specific phone number.

Mr. LUNGREN. And if in fact in the process of using the roving wiretap, you move it to another instrumentality, do you not have to then inform the court of that?

Mr. HINNEN. We do. We have to inform the court of the facts that lead us to believe that the target for whom we have already shown probable cause that he was an agent of a foreign power is using a specific phone number at that new provider.

Mr. LUNGREN. So there is a continuing oversight by the court in that context?

Mr. HINNEN. That is correct.

Mr. LUNGREN. And obviously in a criminal case and in a case such as this, when you allowed to have a roving wiretap, I assume you collect conversations with people who are not targets.

Mr. HINNEN. That is certainly correct that when the Government conducts surveillance, not every conversation relates to the conduct being——

Mr. LUNGREN. And the Government has done this for years and years in the criminal context. I presume that you handle it in this context in a similar manner, that is, you are required to minimize those conversations of people who are not targets. Correct?

Mr. HINNEN. Although the minimization process works slightly differently, yes, there is a strict minimization requirement in the FISA statute.

Mr. LUNGREN. Would you explain for the record what that minimization process is?

Mr. HINNEN. In a criminal context, real-time minimization is required. In other words, an agent literally listens to the phone call, and if it appears to be a call to mom about picking up milk on the way home, the call is dropped. Because Congress recognized that spies and terrorists don't always operate that way, there may be language issues, there may be issues of talking in code, there may be tradecraft issues, the FISA statute does not require real-time minimization. It requires after-the-fact minimization.

Mr. LUNGREN. But minimization nonetheless.

Mr. HINNEN. Minimization nonetheless.

Mr. SENSENBRENNER. The time of the gentleman has expired.

The gentlewoman from California, Ms. Chu?

Ms. CHU. I was interested in a couple of anecdotes from the Inspector General report, the first case where the FBI was collecting information about a certain telephone line. During this time the phone company assigned the number to a different person but failed to inform the FBI of this fact for several weeks, and as a result, the FBI collected information about an innocent person who was not connected to the investigation.

And then a second anecdote where the FBI learned that a source who had provided significant information about the target changed his mind and no longer believed that the target was involved with a particular terrorist group, but the change was not reported to the court until about a year later. Hence, all that information was collected.

Well, let me ask about these roving wiretaps, Mr. Hinnen or Mr. Litt. The criminal law also permits roving wiretaps, as it should, but it also includes a critical protection that section 206 of the PATRIOT Act does not. It requires the Government to specifically identify the target if it is not going to identify a device and rove with an individual. There have been legislative fixes proposed for almost 10 years to put this common sense protection into FISA. Do you oppose this proposal or do you support this proposal? Please explain what your position is on this.

Mr. LITT. I must say I think that proposal is entirely unnecessary. As Mr. Hinnen explained before, the FISA statute already re-

quires that we either identify the person by name or give a sufficient description of him so that we know who it is.

I must say I spent a number of years at the beginning of my career as an assistant U.S. attorney, and I encountered situations where we would wiretap somebody and the target of the wiretap would be, you know, John Doe, aka, Chico. All we knew was a nickname, but we knew enough to know who it was so that when we were listening to the phone, as Mr. Hinnen said, we could turn it off if we didn't have our target on the line.

It is the same principle here. We may not know the person's name and we certainly may not know that we know his true name, but we can't get a FISA order unless we know enough to convince the court that we know who the person is and that that person is an agent of a foreign power. And that requires particularity.

Ms. CHU. Well, another protection in criminal wiretaps is that the Government must ascertain that the subject is actually using the device before it begins recording, thereby greatly reducing the number of innocent people that are inadvertently recorded by the Government. As you can see here in the anecdote that I just named, the suspected person wasn't even using that particular phone.

Do you oppose putting this protection into FISA, and if so, why?

Mr. HINNEN. Congresswoman, that protection is in FISA for surveillance. The Government must show, in addition to probable cause that the targeted individual is an agent of a foreign power, probable cause that the individual is using or is about to use the phone. I suspect—and I am not familiar with that particular passage of the Inspector General's report, but I expect that that was a mistake. I won't sit here and tell you that mistakes never occur in this area of human endeavor, just like they occur in all others. But the FISA statute does require the Government to demonstrate probable cause that the individual is using or about to use the specific number that the Government wants to conduct surveillance on.

Ms. CHU. Mr. Sanchez, how do you respond to this?

Mr. SANCHEZ. I think what is crucial to keep in mind when talking about the equivalence between two powers is the larger framework in which they are embedded. So as Mr. Hinnen already discussed, collection in the first instance is much broader, is weighted toward, as the FISA Court has said, the Government's need to acquire foreign intelligence, and that even when it is minimized, often that doesn't entail the destruction of information. So there have been a number of cases where FISA recordings that were nominally minimized were when the Government was faced with the Brady obligation to provide exculpatory information, they were actually able to ultimately retrieve many, many times more hours of recording than had been not minimized.

So in particular, in the context of where you are talking about roving across facilities where I think the inherent possibility of using an identifier like Chico creates a lot more slippage, a lot more potential for error, the need to compensate on the front end means that the protections on the discretion of agents need to be at least as strong as they are on the criminal side where, again,

there is going to be a lot more back-end scrutiny in a distributed fashion if not by the court itself.

Mr. SENSENBRENNER. The time of the gentlewoman has expired.

The gentleman from Pennsylvania, Mr. Marino?

Mr. MARINO. Thank you, Mr. Chairman.

Gentlemen, I think you have been asked a question to a certain extent, but before I ask you to answer my question, am I correct there are two attorneys and two non-attorneys? Or there are three attorneys and one non-attorney. Got it. All right.

Just for the interest of brevity, I would like to start at the left end, my left, of the table. Could you please succinctly describe the difference between a Title III search warrant and a FISA warrant? I think that is critical at this point because as a U.S. attorney for 6 years and a district attorney for 12 years, to some extent I had more latitude as a district attorney in acquiring a Title III warrant than I did a FISA warrant.

Mr. HINNEN. Yes, Congressman. The principal differences between a Title III warrant and a FISA order are that in the first case the Government needs to demonstrate that the individual target is an agent of a foreign power, not an individual committing a crime but must show probable cause in both cases.

Second, Congress decided in 1978 that it would be harmful to foreign intelligence investigations if the strict notice requirements in Title III also existed in the criminal context. You would essentially in every case in which you conducted surveillance against a spy or a terrorist have to notify him within a certain amount of time after that surveillance had occurred.

And then the last is one that we have already discussed here today as well which is in the technical manner in which the minimization is applied to the information collected.

Mr. MARINO. Attorney Litt, please. Can you follow up on that?

Mr. LITT. I agree with that.

Mr. MARINO. Good.

Professor?

Mr. SALES. Thank you, Congressman.

I agree with that and one additional and important difference between the Title III context and the FISA context is the internal approval mechanism for a wiretap order. In the Title III context—let me talk about the FISA context first.

The FISA context requires incredibly high-level sign-off from the highest levels within the Justice Department. The FBI Director is involved. The Deputy Attorney General is personally involved. The Attorney General is personally involved. That is much more rigorous internal executive branch scrutiny than you have for a Title III wiretap which I suspect may explain your own experience of the relative ease of obtaining a Title III versus a FISA.

Mr. MARINO. And it hinges on the credibility of the United States attorney and the FBI agent or whatever agent requesting that. Okay.

Mr. MARINO. Sir?

Mr. SANCHEZ. I think they have covered it fairly well, but I would stress again the distinction between minimization in real time and minimization after the fact as again weighted toward broad acquisition of most of the information flowing through a fa-

cility unless it could not be foreign intelligence information which almost anything could. So again, just the idea that there is much broader initial collection.

Mr. MARINO. Broader initial collection where?

Mr. SANCHEZ. That is to say as opposed to the case where information is recorded only when there is some nexus to the predicate offense, there is generally recording of all communications.

Mr. MARINO. You know, with all due respect you are throwing out first-year law school criminal law terms, "predicate offense," "nexus," you know, the whole 9 yards, something that any one of us can get off the Internet. But you are not getting specifics. Do you understand, sir, with all due respect, the delineation between the two and what one has to go through for the FISA order compared to the Title III?

Mr. SANCHEZ. I do. I am referring only to, again, the question of when minimization occurs, which everyone else here has, I think, already alluded to.

Mr. MARINO. Thank you.

I yield my time.

Mr. SENSENBRENNER. The gentleman from Arkansas, Mr. Griffin?

Mr. GRIFFIN. Thank you, Mr. Chairman.

I want to follow up with some questions for you, Mr. Sanchez. I was reading in your written statement when you were talking about—and these pages are not numbered. You have a section here where you are talking about the transparency that normally surrounds the acquisition of documents via grand jury subpoena.

Mr. SANCHEZ. Yes.

Mr. GRIFFIN. And you indicate that it is impossible to overstate the significance of the transparency that normally surrounds the acquisition of documents by those means, those means being via the grand jury subpoena. Could you talk a little bit about what that transparency is?

Mr. SANCHEZ. Well, insofar as normally on the criminal side that those processes do not involve gag orders, as 215 orders and national security letters normally do, the incentives I believe are different for companies served with those orders. They are not always incentivized to stand up for the privacy rights of their customers, the people whose records they are in custody of. But we see frequently booksellers or companies like Google moving to quash subpoenas specifically citing the ground that they fear that their reputation would be damaged by the disclosure of the fact that they were turning over sensitive records without making any kind of move to limit the scope of the subpoenas.

By contrast, what we have seen, again, in at least the national security letter and 215 cases, is that often when there have been identified misuses, they have typically occurred with the enthusiastic collaboration of the record custodians, often violating the rules because of overproduction.

Mr. GRIFFIN. I am limited on time here.

So I guess in my experience, I haven't seen a lot of transparency, not that it is warranted. The whole nature of a grand jury process is secrecy. I am not sure where you are going with your transparency argument. But the grand jury issues the subpoena in se-

crecy. It is issued and complied with in secrecy. The documents are obtained and brought to the grand jury. So I am not exactly sure what that argument is that you are making there.

But I also want to go over here. You talk about the PATRIOT Act's roving wiretap provision includes no parallel requirement that an individual target be named. We just discussed that. We were given the example of at least identifying the individual even if we don't know the name.

But then you go on and you say, quote, this is disturbingly close to the sort of general warrant the Founders were so concerned to prohibit when they crafted our Bill of Rights. A little hyperbole there maybe.

Mr. Litt, would you comment on that?

And this gets me to the broader question, and this is what I have heard a lot back home. If you would each—I know I am running out of time—just briefly comment on the constitutionality of the three provisions that we just voted to extend. Do you any of you have constitutionality concerns? And if this was asked previously, I apologize.

Why do we not just start on the end and go down?

Mr. HINNEN. No, Congressman.

Mr. GRIFFIN. Mr. Litt?

Mr. LITT. No. No, I don't. I think the only two issues that have been raised—with respect to the lone wolf provision, I think there has been concern expressed that this may be beyond the national security powers as set out in the Keith case. And I think that when you have a situation where you are talking about non-U.S. persons who are engaged in international terrorism and a collection which is certified to be for the purpose of collecting foreign intelligence, I don't think that is a serious constitutional concern.

And similarly, for the reasons we previously discussed, I think that the roving wiretap adequately meets the particularity requirement of the Fourth Amendment.

Mr. GRIFFIN. Mr. Sales?

Mr. SALES. Thank you, Congressman.

I agree with that as well.

I think we are pretty far away from the days of King George III. FISA, as amended by the PATRIOT Act, doesn't allow the sort of general warrant dragnets that our founders justifiably worried about 200 years ago. That is not the situation that FISA authorizes. In all cases, FISA, as amended by the PATRIOT Act, requires probable cause to believe that the target is an agent of a foreign power, i.e., somebody who is a spy or a terrorist. That seems like it meets the particularity requirement pretty precisely to me.

Mr. SENSENBRENNER. The time of the gentleman has expired.

Mr. GRIFFIN. Thank you, Mr. Chairman.

Mr. SENSENBRENNER. I would like to thank all of our witnesses today for their testimony. I think it has been very enlightening and elucidating.

Without objection, all Members will have 5 legislative days to submit to the Chair additional written questions for the witnesses which we will forward and ask the witnesses to respond as promptly as they can so that their answers may be made part of the record.

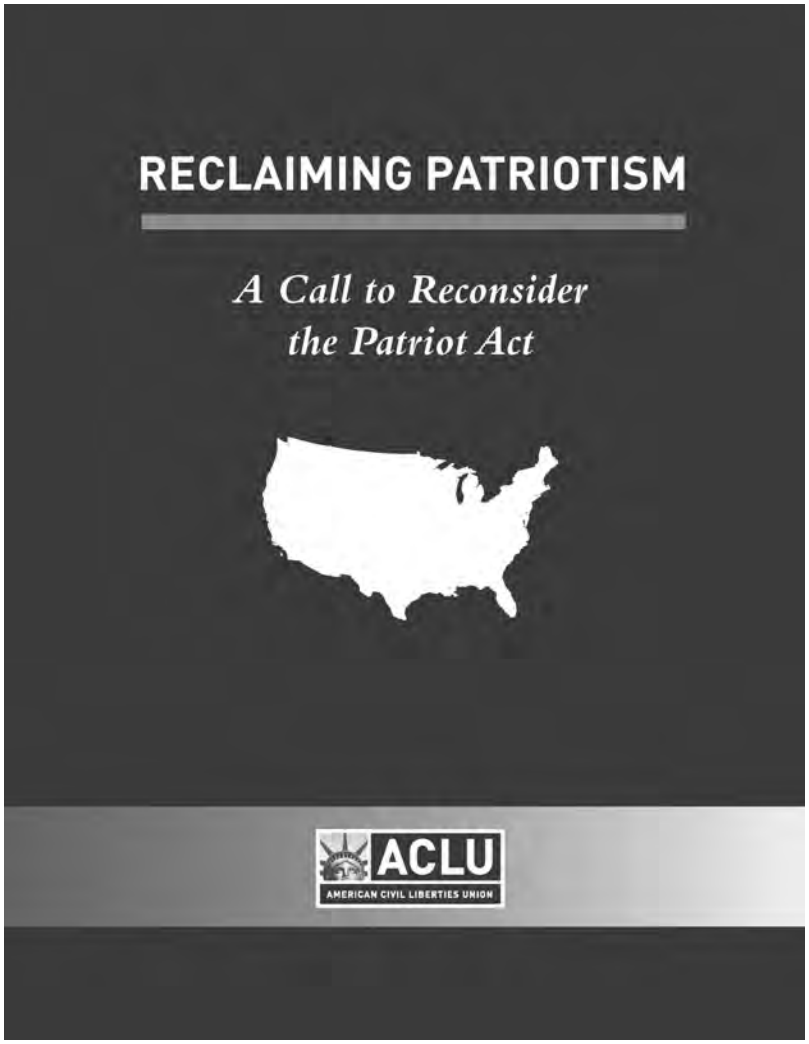
The gentleman from Georgia?

Mr. JOHNSON. Thank you, Mr. Chairman.

I would ask unanimous consent to introduce into the hearing record a report by the American Civil Liberties Union titled "Reclaiming Patriotism."

Mr. SENSENBRENNER. Without objection.

[The information referred to follows:]



RECLAIMING PATRIOTISM

A Call to Reconsider the Patriot Act

Reclaiming Patriotism
A Call to Reconsider the Patriot Act

Published March 2009

THE AMERICAN CIVIL LIBERTIES UNION is the nation's premier guardian of liberty, working daily in courts, legislatures and communities to defend and preserve the individual rights and freedoms guaranteed by the Constitution and the laws of the United States.

OFFICERS AND DIRECTORS
Susan N. Herman, President
Anthony D. Romero, Executive Director
Richard Zacks, Treasurer

ACLU NATIONAL OFFICE
125 Broad Street, 18th Fl.
New York, NY 10004-2400
(212) 549-2500
www.aclu.org

ACKNOWLEDGEMENTS

ACLU Policy Counsel Michael German and Legislative Counsel Michelle Richardson researched and wrote Reclaiming Patriotism: A Call to Reconsider the Patriot Act.

Willa Tracosas designed the publication.

Photo credits:
Peter Chase (pg. 13): Plainville (CT) Library Staff
Brewster Kahle (pg. 15): By Moira Davis of Internet Archive
Tariq Ramadan (pg. 17): Provided by Mr. Ramadan's office
Konstanty Hordynski (pg. 19): By Rick Rocamora
Wanda Guthrie (pg. 21): Provided by Ms. Guthrie
Brandon Mayfield (pg. 25): AP Images

TABLE OF CONTENTS

EXECUTIVE SUMMARY	5
INTRODUCTION	7
REAL PATRIOTS DEMAND THEIR RIGHTS	8
EXCESSIVE SECRECY THWARTS CONGRESSIONAL OVERSIGHT	10
Increasing Levels of Surveillance	11
More Collection Does Not Result in More Prosecutions	13
NEW SUNSET DATES CREATE OVERSIGHT OPPORTUNITY	14
EVIDENCE OF ABUSE: THE INSPECTOR GENERAL AUDITS	16
National Security Letters	16
Section 215 Orders	18
UNCONSTITUTIONAL: COURT CHALLENGES TO THE PATRIOT ACT	21
National Security Letter Gag Orders	21
Material Support for Terrorism Provisions	22
Ideological Exclusion	26
Relaxed FISA Standards	27
ONLY ONE PIECE OF THE PUZZLE	29
CONCLUSION—IT IS TIME TO RECLAIM PATRIOTISM	30
APPENDIX—THE PATRIOT ACT AT A GLANCE	31
ENDNOTES	34

EXECUTIVE SUMMARY

More than seven years after its implementation, there is little evidence to demonstrate that the Patriot Act has made America more secure from terrorists. But there are many unfortunate examples that the government abused these authorities in ways that both violated the rights of innocent people and squandered precious security resources. Three Patriot Act-related surveillance provisions will expire in December 2009, which will give the 111th Congress an opportunity to review and thoroughly evaluate all Patriot Act authorities – as well as any other post-9/11 domestic intelligence programs – and to rescind, repeal or modify provisions that are unused, ineffective or prone to abuse.

The framers of the Constitution recognized that giving the government unchecked authority to pry into our private lives risked more than just individual property rights. These patriots understood from their own experience that political rights could not be secured without procedural protections. The Fourth Amendment mandates prior judicial review and permits warrants to be issued only upon probable cause. The nation's founders saw these procedural requirements as the necessary remedies to the arbitrary and unreasonable assaults on free expression exemplified by King George's abuse of general warrants. Stifling dissent does not enhance security. The framers created our constitutional system of checks and balances to curb government abuse and, ultimately, to make the government more responsive to the needs of the people – in whom all government power resides. Limiting the government's power to intrude into private affairs, and checking that power with independent oversight, reduces the error and abuse that conspire to undermine public confidence. As the original patriots knew, adherence to the concepts set forth in the Constitution and the Bill of Rights makes our government stronger, not weaker.

The Patriot Act vastly – and unconstitutionally – expanded the government's authority to pry into people's private lives with little or no evidence of wrongdoing. Unfortunately, when the expiring provisions came up for review in 2005 there was very little in the public record for Congress to evaluate. Excessive secrecy surrounding the government's use of these authorities, enforced through unconstitutional gag orders, prevented any meaningful evaluation of the Patriot Act. Even without adequate supporting justification, in March 2006 Congress passed the USA Patriot Act Improvement and Reauthorization Act, making fourteen of the sixteen expiring provisions permanent.

Little is known about the government's use of many of its authorities under the Patriot Act, but raw numbers available through government reports reflect a rapidly increasing level of surveillance. The statistics show skyrocketing numbers of Foreign Intelligence Surveillance Court orders, National Security Letter (NSL) requests and Suspicious Activity Reports while terrorism prosecution numbers are down and declinations to prosecute FBI international terrorism investigations have increased. Moreover, Department of Justice Inspector General reports (mandated as part of the Patriot Act reauthorization) revealed the government's widespread misuse of NSL and section 215 authorities. Also, several courts have found parts of the Patriot Act unconstitutional, including the NSL gag provisions, enhancements to the material support and ideological exclusion statutes, and Section 218 of the Patriot Act, which lowered the standard for obtaining an individualized Foreign Intelligence surveillance Act (FISA) warrant.

This report identifies the Patriot Act provisions that require intensive oversight and modification to prevent abuse. It also contains specific legislative recommendations for reforming the NSL, FISA, material support and ideological exclusion statutes and section 215 of the Patriot Act.

NSLs and Section 215

- Repeal the expanded NSL and section 215 authorities that allow the FBI to demand information about innocent people who are not the targets of any investigation. Reinstate prior standards limiting the use of section 215 and NSL authorities to gather information only about terrorism suspects and other agents of foreign powers.
- Allow gag orders only upon the authority of a court, and only when necessary to protect national security. Limit scope and duration of such gag orders and ensure that their targets and recipients have a meaningful right to challenge them before a fair and neutral arbiter.
- Impose judicial oversight of all Patriot Act authorities.

Material Support

- Amend the material support statutes to require specific intent to further an organization's unlawful activities before imposing criminal liability.
- Remove overbroad and impermissibly vague language, such as "training,""service" and "expert advice and assistance," from the definition of material support.
- Establish an explicit duress exemption to remove obstacles for genuine refugees and asylum-seekers to enter and/or remain in the United States.
- Provide notice, due process and meaningful review requirements in the designation process, and permit defendants charged with material support to challenge the underlying designation in their criminal cases.

Ideological Exclusion

- Ban ideological exclusion based on speech that would be protected in the United States under the First Amendment.
- Repeal the "endorse or espouse" provision.

FISA Statutes

- Restore the primary purpose requirement to FISA.

While implementation of these recommendations would help fix some Patriot Act-related problems, Congress must examine the full panoply of intelligence activities, especially domestic intelligence gathering programs, and encourage a public debate about the proper nature and reach of government surveillance programs on American soil. The Patriot Act may have been the first overt expansion of domestic spying powers after September 11, 2001 – but it certainly wasn't the last, and arguably wasn't even the most egregious. There have been many significant changes to our national security laws over the past seven years, and addressing the excesses of the Patriot Act without examining the larger surveillance picture may not be enough to rein in an out-of-control intelligence-gathering regime. Fundamentally, Congress must recognize that overbroad, ineffective or abusive surveillance programs are counterproductive to long-term government interests because they violate constitutional standards and undermine public confidence and support of U.S. anti-terrorism programs. Congress should begin vigorous and comprehensive oversight hearings to examine all post-9/11 national security programs to evaluate their effectiveness and their impact on Americans' privacy and civil liberties. This oversight is essential to the proper functioning of our constitutional system of government and becomes even more necessary during times of crisis.

INTRODUCTION

On October 26, 2001, amid the climate of fear and uncertainty that followed the terrorist attacks of September 11, 2001, President George W. Bush signed into law the USA Patriot Act, and fundamentally altered the relationship Americans share with their government.[1] This act betrayed the confidence the framers of the Constitution had that a government bounded by the law would be strong enough to defend the liberties they so bravely struggled to achieve. By expanding the government's authority to secretly search private records and monitor communications, often without any evidence of wrongdoing, the Patriot Act eroded our most basic right – the freedom from unwarranted government intrusion into our private lives – and thwarted constitutional checks and balances. Put very simply, under the Patriot Act the government now has the right to know what you're doing, but you have no right to know what it's doing.

More than seven years after its implementation there is little evidence that the Patriot Act has been effective in making America more secure from terrorists. However, there are many unfortunate examples that the government abused these authorities in ways that both violate the rights of innocent people and squander precious security resources. Three Patriot Act-related surveillance provisions will expire in December 2009, which will give the 111th Congress an opportunity to review and thoroughly evaluate all Patriot Act authorities – as well as any other post-9/11 domestic intelligence programs – and rescind, repeal or modify provisions that are unused, ineffective or prone to abuse. The American Civil Liberties Union encourages Congress to exercise its oversight powers fully, to restore effective checks on executive branch surveillance powers and to prohibit unreasonable searches and seizures of private information without probable cause based on particularized suspicion.

REAL PATRIOTS DEMAND THEIR RIGHTS

The Fourth Amendment to the U. S. Constitution protects individuals against "unreasonable searches and seizures." In 1886, Supreme Court Justice Joseph P. Bradley suggested that the meaning of this phrase could not be understood without reference to the historic controversy over general warrants in England and her colonies.[2] General warrants were broad orders that allowed the search or seizure of unspecified places or persons, without probable cause or individualized suspicion. For centuries, English authorities had used these broad general warrants to enforce "seditious libel" laws designed to stifle the press and suppress political dissent. This history is particularly informative to an analysis of the Patriot Act because the purpose of the Fourth Amendment was not just to protect personal property, but "to curb the exercise of discretionary authority by [government] officers."[3]

To the American colonists, nothing demonstrated the British government's illegitimate use of authority more than "writs of assistance" – general warrants that granted revenue agents of the Crown blanket authority to search private property at their own discretion.[4] In 1761, in an event that John Adams later described as "the first act of opposition" to British rule, Boston lawyer James Otis condemned general warrants as "the worst instrument of arbitrary power, the most destructive of English liberty and the fundamental principles of law, that ever was found in an English law book."[5] Otis declared such discretionary warrants illegal, despite their official government sanction, because they "placed the liberty of every man in the hands of every petty officer."[6] The resistance to writs of assistance provided an ideological foundation for the American Revolution – the concept that the right of the people to be free from unwarranted government intrusion into their private affairs was the essence of liberty. American patriots carried a declaration of this foundational idea on their flag as they marched into battle: "Don't tread on me."

Proponents of the Patriot Act suggest that reducing individual liberties during a time of increased threat to our national security is both reasonable and necessary, and that allowing fear to drive the government's decisions in a time of emergency is "not a bad thing."[7] In effect, these modern-day patriots are willing to exchange our forbearers' "don't tread on me" banner for a less inspiring one reading "if you aren't doing anything wrong you have nothing to worry about."

Colonial-era patriots were cut from different cloth. They saw liberty not as something to trade for temporary comfort or security, but rather as a cause worth fighting for even when the odds of success, not to mention survival, were slight.

The framers of the Constitution recognized that giving the government unchecked authority to pry into our private lives risked more than just individual property rights, as the Supreme Court later recounted: "The Bill of Rights was fashioned against the background of knowledge that unrestricted power of search and seizure could also be an instrument for stifling liberty of expression."[8] These patriots understood from their own experience that political rights could not be secured without procedural protections. The Fourth Amendment requirements of prior judicial review and warrants issued only upon probable cause were determined to be the necessary remedies to the arbitrary and unreasonable assaults on free expression that were characterized by the government's use of general warrants. "The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another."[9] The Supreme Court has long acknowledged the important interplay between First Amendment and Fourth Amendment freedoms. As it reflected in 1965, "what this history indispensably teaches is that the constitutional requirement that warrants must

particularly describe the 'things to be seized' is to be accorded the most scrupulous exactitude when the 'things' are books, and the basis for their seizure is the ideas which they contain."[10]

The seizure of electronic communications and private records under the Patriot Act today is no less an assault on the ideas they contain than seizure of books during a less technologically advanced era. Indeed, even more fundamental liberty interests are at stake today because the Patriot Act expanded "material support" for terrorism statutes that effectively criminalize political association and punish wholly innocent assistance to arbitrarily blacklisted individuals and organizations. Patriot Act proponents suggest we should forfeit our rights in times of emergency, but the Supreme Court has made clear that the Constitution requires holding the government to more exacting standards when a seizure involve the expression of ideas even where compelling security interests are involved. As Justice Powell explained in *United States v United States District Court*,

> National security cases, moreover, often reflect a convergence of First and Fourth Amendment values not present in cases of "ordinary" crime. Though the investigative duty of the executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech.[11]

More exacting standards are necessary in national security cases because history has repeatedly shown that government leaders too easily mistake threats to their political security for threats to the national security. Enhanced executive powers justified on national security grounds were used against anti-war activists, political dissidents, labor organizers and immigrants during and after World War I. In the 1950s prominent intellectuals, artists and writers were blacklisted and denied employment for associating with suspected communists and socialists. Civil rights activists and anti-war protesters were targeted in the 1960s and 1970s in secret FBI and CIA operations.

Stifling dissent does not enhance security. The framers created our constitutional system of checks and balances to curb government abuse, and ultimately to make the government more responsive to the needs of the people – which is where all government power ultimately lies. The Patriot Act gave the executive branch broad and unprecendented discretion to monitor electronic communications and seize private records, placing individual liberty, as John Otis warned, "in the hands of every petty officer."[12] Limiting the government's power to intrude into private affairs, and checking that power with independent oversight, reduces the error and abuse that conspire to undermine public confidence. As the original patriots knew, adhering to the Constitution and the Bill of Rights makes our government stronger, not weaker.

EXCESSIVE SECRECY THWARTS CONGRESSIONAL OVERSIGHT

Just 45 days after the worst terrorist attack in history Congress passed the Patriot Act, a 342-page bill amending more than a dozen federal statutes, with virtually no debate. The Patriot Act was not crafted with careful deliberation, or narrowly tailored to address specific gaps in intelligence gathering authorities that were found to have harmed the government's ability to protect the nation from terrorism. In fact, the government hesitated for months before authorizing an official inquiry, and it took over a year before Congress published a report detailing the many significant pieces of intelligence the government lawfully collected before 9/11 but failed to properly analyze, disseminate or exploit to prevent the attacks.[14] Instead of first determining what led to the intelligence breakdowns and then legislating, Congress quickly cobbled together a bill in ignorance, and while under intense pressure, to give the president all the authorities he claimed he needed to protect the nation against future attacks.

The Patriot Act vastly – and unconstitutionally – expanded the government's authority to pry into people's private lives with little or no evidence of wrongdoing. This overbroad authority unnecessarily and improperly infringes on Fourth Amendment protections against unreasonable searches and seizures and First Amendment protections of free speech and association. Worse, it authorizes the government to engage in this expanded domestic spying in secret, with few, if any, protections built in to ensure these powers are not abused, and little opportunity for Congress to review whether the authorities it granted the government actually made Americans any safer.

The ACLU warned that these unchecked powers could be used improperly against wholly innocent American citizens, against immigrants living legally within our borders and against those whose First Amendment-protected activities were improperly deemed to be threats to national security by the attorney general.[14] Many members of Congress shared the ACLU's concerns and demanded the government include "sunsets," or expiration dates on certain provisions of the Patriot Act to give Congress an opportunity to review their effectiveness over time.

Unfortunately, when the expiring provisions came up for review in 2005 there was very little in the public record for Congress to evaluate. While the ACLU objected to the way the government exercised Patriot Act powers against individuals like Oregon attorney Brandon Mayfield, Idaho student Sami al-Hussayen and European scholar Tariq Ramadan, among others,[15] officials from the Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI) repeatedly claimed there had been no "substantiated" allegations of abuse.[16] Of course, the lack of substantiation was not due to a lack of abuse, but rather to the cloak of secrecy that surrounded the government's use of these authorities, which was duly enforced through unconstitutional gag orders. Excessive secrecy prevented any meaningful evaluation of the Patriot Act. Nevertheless, in March 2006 Congress passed the USA Patriot Act Improvement and Reauthorization Act (Patriot Act reauthorization), making fourteen of the sixteen expiring provisions permanent.[17]

Increasing Levels of Surveillance

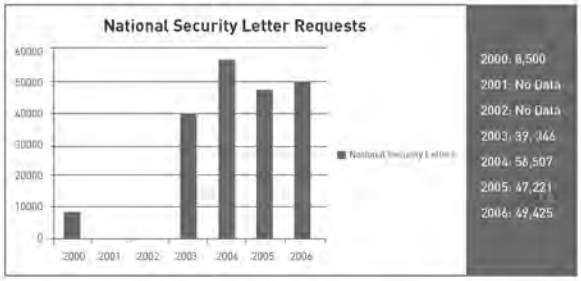
Little is known about how the government uses many of its authorities under the Patriot Act, but saw numbers available through government reports reflect a rapidly increasing level of surveillance.

Foreign Intelligence Surveillance Court Orders Approved
(Includes orders for electronic surveillance and physical searches)
Section 218 of the Patriot Act modified the legal standard necessary to obtain Foreign Intelligence Surveillance Court orders.

See Electronic Privacy Information Center, Foreign Intelligence Surveillance Act Orders 1979-2007, http://epic.org/privacy/wiretap/stats/fisa_stats.html#footnote12 (last visited Dec. 1, 2008).

National Security Letter Requests*

Section 505 of the Patriot Act reduced the legal standard for issuing National Security Letters.

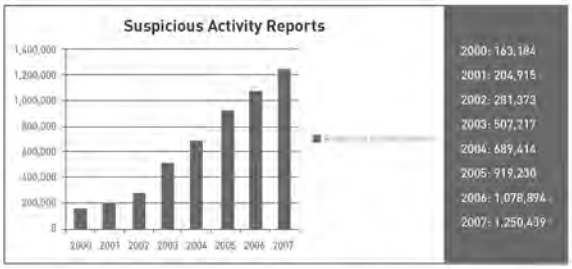


See Dep't Of Justice, Office Of Inspector General, A Review Of The Federal Bureau Of Investigation's Use Of National Security Letters 89 (Mar. 2007), *available at* http://www.usdoj.gov/oig/special/s0703b/final.pdf; Dep't Of Justice, Office Of Inspector General, A Review Of The Federal Bureau Of Investigation's Use Of Section 215 Orders for Business Records (Mar. 2007), *available at* http://www.usdoj.gov/oig/special/s0703a/final.pdf.

*These numbers understate the number of NSL requests the FBI actually made during these time periods. The inspector general determined that the FBI did not keep proper records regarding its use of NSLs and the audit revealed significant underreporting of NSL requests. No reliable data exists for the number of NSLs served in 2001 and 2002.

Suspicious Activity Reports filed by financial institutions

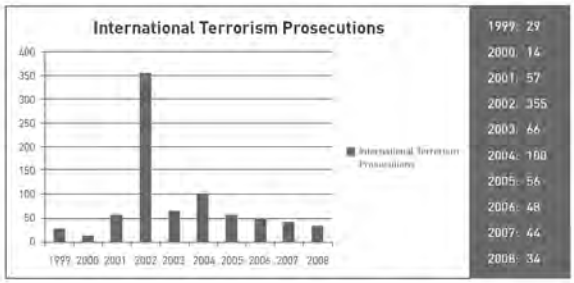
Sections 356 and 359 of the Patriot Act expanded the types of financial institutions required to file suspicious activity reports under the Bank Secrecy Act. These reports include detailed personal and account information and are turned over to the Treasury Department and the FBI.



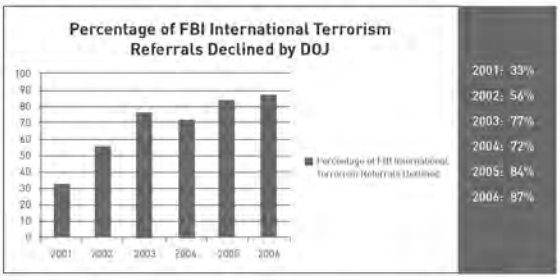
See Dep't of the Treasury, Financial Crimes Enforcement Network, The SAR Activity Review – By the Numbers, Issue 10 (May 2008), *available at* http://www.fincen.gov/news_room/rp/files/sar_by_numb_10.pdf.

More Collection Does Not Result in More Prosecutions

Data produced by the Executive Office for United States Attorneys and analyzed by the Transactional Records Access Clearinghouse (TRAC) shows that prosecutions in FBI international terrorism cases dropped steadily from 2002 to 2008.*



More critical to evaluating the effectiveness of post-Patriot Act surveillance, however, is DOJ's increasing tendency to refuse to prosecute FBI international terrorism investigations during that time period. In 2006, the DOJ declined to prosecute a shocking 87% of the international terrorism cases the FBI referred for prosecution. Only a tiny fraction of the many thousands of terrorism investigations the FBI opens each year are even referred for prosecution, thereby demonstrating that the vast majority of the FBI's terrorism-related investigative activity is completely for naught – yet the FBI keeps all of the information it collects through these dubious investigations, forever.



*See Transactional Records Access Clearinghouse, National Profile and Enforcement Trends over Time (2006), http://trac.syr.edu/tracfbi/newfindings/current/ (last visited Dec. 1, 2008); Todd Lochner, *Sound and Fury: Perpetual Prosecution and Department of Justice Counterterrorism Efforts*, 30 Law & Policy 168, 179 (2008), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1199250 ("In fiscal year 2003 alone the FBI opened over 25,000 terrorism investigations, a figure that dwarfs all declinations by federal prosecutors since that time").

NEW SUNSET DATES CREATE OVERSIGHT OPPORTUNITY

When Congress reauthorized the Patriot Act in 2006, it established new expiration dates for two Patriot Act provisions and for a related provision of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA).[9] Under the reauthorization, these three provisions, **section 206** and **section 215** of the Patriot Act and **section 6001** of the IRTPA, are all set to expire on December 31, 2009. The 111th Congress will revisit these provisions this year, which creates an opportunity for Congress to examine and evaluate the government's use and abuse of all Patriot Act authorities, as well as other post-9/11 surveillance or security programs.

Section 206 of the Patriot Act authorizes the government to obtain "roving wiretap" orders from the Foreign Intelligence Surveillance Court (FISC) whenever a subject of a wiretap request uses multiple communications devices. The FISC is a secret court established under the Foreign Intelligence Surveillance Act (FISA) that issues classified orders for the FBI to conduct electronic surveillance or physical searches in intelligence investigations against foreign agents and international terrorists. Unlike roving wiretaps authorized for criminal investigations, section 206 does not require the order to identify either the communications device to be tapped nor the individual against whom the surveillance is directed, which is what gives section 206 the Kafkaesque moniker, the "John Doe roving wiretap provision." The reauthorized provision requires the target to be described "with particularity," and the FBI to file an after-the-fact report to the FISC to explain why the government believed the target was using the phones it was tapping. However, it does not require the government to name the target, or to make sure its roving wiretaps are intercepting only the target's communications. The power to intercept a roving series of unidentified devices of an unidentified target provides government agents with an inappropriate level of discretion reminiscent of the general warrants that so angered the American colonists. There is virtually no public information available regarding how the government uses section 206.

Likewise, little is known about the way the government uses **section 6001** of the IRTPA, which is known as the "lone wolf" provision. Section 6001 authorizes government agencies to obtain secret FISA surveillance orders against individuals who are not connected to any international terrorist group or foreign nation. The government justified this provision by imagining a hypothetical "lone wolf," an international terrorist operating independently of any terrorist organization, but there is little evidence to suggest this imaginary construct had any basis in reality. Moreover, since terrorism is a crime, there is no reason to believe that the government could not obtain a Title III surveillance order from a criminal court if the government had probable cause to believe an individual was planning an act of terrorism.[10] Quite simply, this provision allows the government to avoid the more exacting standards for obtaining electronic surveillance orders from criminal courts. No public records are available to document whether, or how, the government has used this power.

Section 215 of the Patriot Act provides a sweeping grant of authority for the government to obtain secret FISC orders demanding "any tangible thing" it claims is relevant to an authorized investigation regarding international terrorism or espionage. Known as the "library provision," section 215 significantly expands the types of items the government can demand under FISA, and lowers the standard of proof necessary to obtain an order. Prior to the Patriot Act, FISA required probable cause to believe the target was an agent of a foreign power. Section 215 only requires the government to claim the items sought are relevant to an authorized investigation. Most significant in this change of standard, however, was the removal of the requirement for the FBI to show that the items sought pertain to a person the FBI is investigating. Under section 215, the government can obtain orders for private records

or items belonging to people who are not even under suspicion of involvement with terrorism or espionage, including U.S. citizens and lawful resident aliens, not just foreigners.

Section 215 orders come with compulsory non-disclosure orders, or "gags," which contributed to the secrecy surrounding how they were being used. To ensure that it would have at least some information upon which to evaluate Patriot Act powers before the next sunset period, Congress included a provision in the 2006 Patriot Act reauthorization that required the Department of Justice Inspector General (IG) to audit the FBI's use of National Security Letters (NSLs) and Section 215 orders.[20] These reports provided the first thorough examination of the implementation of the post-9/11 anti-terrorism powers. They also confirmed what our nation's founders already knew: unchecked authority is too easily abused.

EVIDENCE OF ABUSE: THE INSPECTOR GENERAL AUDITS

National Security Letters

NSLs are secret demand letters issued without judicial review to obtain sensitive personal information such as financial records, credit reports, telephone and e-mail communications data and Internet searches. The FBI had authority to issue NSLs through four separate statutes, but these authorities were significantly expanded by **section 505** of the Patriot Act.[21] **Section 505** increased the number of officials who could authorize NSLs and reduced the standard necessary to obtain information with them, requiring only an internal certification that the records sought are "relevant" to an authorized counterterrorism or counter-intelligence investigation. The Patriot Act reauthorization made the NSL provisions permanent.

The NSL statutes now allow the FBI and other executive branch agencies to obtain records about people who are not known – or even suspected – to have done anything wrong. The NSL statutes also allow the government to prohibit NSL recipients from disclosing that the government sought or obtained information from them. While Congress modified these "gag orders" in the Patriot Act reauthorization to allow NSL recipients to consult a lawyer, under the current state of the law NSLs are still not subject to any meaningful level of judicial review (ACLU challenges to the NSL gag orders are described below).[22]

The first two IG audits, covering NSLs and section 215 orders issued from 2003 through 2005, were released in March of 2007. They confirmed widespread FBI mismanagement, misuse and abuse of these Patriot Act authorities.[23] The NSL audit revealed that the FBI managed its use of NSLs so negligently that it literally did not know how many NSLs it had issued. As a result, the FBI seriously under-reported its use of NSLs in its previous reports to Congress. The IG also found that FBI agents repeatedly ignored or confused the requirements of the NSL authorizing statutes, and used NSLs to collect private information against individuals two or three times removed from the subjects of FBI investigations. Twenty-two percent of the audited files contained unreported legal violations.[24] Most troubling, FBI supervisors used hundreds of illegal "exigent letters" to obtain telephone records without NSLs by falsely claiming emergencies, apparently finding even the lax standards of NSLs too onerous.[25]

On March 13, 2008, the IG released a second pair of audit reports covering 2006 and evaluating the reforms implemented by the DOJ and the FBI after the first audits were released in 2007.[26] Not surprisingly, the new reports identified many of the same problems discovered in the earlier audits. The 2008 NSL report showed that the FBI issued 49,425 NSLs in 2006 (a 4.7 percent increase over 2005), and confirmed the FBI is increasingly using NSLs to gather information on U.S. persons (57 percent in 2006, up from 53 percent in 2005).[27]

The 2008 IG audit also revealed that high-ranking FBI officials, including an assistant director, a deputy assistant director, two acting deputy directors and a special agent in charge, improperly issued eleven "blanket NSLs" in 2006 seeking data on 3,860 telephone numbers.[28] None of these "blanket NSLs" complied with FBI policy and eight imposed unlawful non-disclosure requirements on recipients.[29] Moreover, the "blanket NSLs" were written to "cover information already acquired through exigent letters and other informal responses."[30] The IG expressed concern that such high-ranking officials would fail to comply with FBI policies requiring FBI lawyers to review all NSLs, but it seems clear enough that this step was intentionally avoided because the officials knew these NSL

requests were illegal.[33] It would be difficult to call this conduct anything but intentional.

The ACLU successfully challenged the constitutionality of the original Patriot Act's gag provisions, which imposed a categorical and blanket non-disclosure order on every NSL recipient.[34] Upon reauthorization, the Patriot Act limited these gag orders to situations when a special agent in charge certifies that disclosure of the NSL request might result in danger to the national security, interference with an FBI investigation or danger to any person. Despite this attempted reform, the IG's 2008 audit showed that 97 percent of NSLs issued by the FBI in 2006 included gag orders, and that five percent of these NSLs contained "insufficient explanation to justify imposition of these obligations."[35] While a five percent violation rate may seem small compared to the widespread abuse of NSL authorities documented elsewhere, these audit findings demonstrate that the FBI continues to gag NSL recipients in an overly broad, and therefore unconstitutional manner. Moreover, the IG found that gags were improperly included in eight of the 11 "blanket NSLs" that senior FBI counterterrorism officials issued to cover hundreds of illegal FBI requests for telephone records through exigent letters.[36]

The FBI's gross mismanagement of its NSL authorities risks security as much as it risks the privacy of innocent persons. The IG reported that the FBI could not locate return information for at least 532 NSL requests issued from the field, and 70 NSL requests issued from FBI headquarters (28 percent of the NSLs sampled).[38] Since the law only allows the FBI to issue NSLs in terrorism and espionage investigations, it cannot be assumed that the loss of these records is inconsequential to our security. Intelligence information continuing to fall through the cracks at the FBI through sheer incompetence is truly a worrisome revelation.

FACES *of* SURVEILLANCE

PETER CHASE is the Director of the Plainville Public Library and was formerly the Vice President of Library Connection Inc, a consortium of 26 Connecticut libraries. In 2005, the FBI used an NSL to demand library patron records from Library Connection and imposed a gag order on the librarians, prohibiting them from speaking to Congress during the debate about the reauthorization of the Patriot Act. Peter and his colleagues decided to challenge the NSL demand and gag. "The government was telling Congress that it didn't use the Patriot Act against libraries and that no one's rights had been violated. I felt that I just could not be part of this fraud being foisted on our nation." Bizarrely, the FBI continued to enforce the gag order even after *The New York Times* revealed Library Connection's identity. The librarians prevailed and the government ultimately withdrew the record demand and the gag order, permitting them to finally tell their story.

Section 215 Orders

The IG's **section 215** audits showed the number of FBI requests for section 215 orders was small by comparison to the number of NSLs issued. Only six section 215 applications were made in 2007.[36]

The disparity between the number of section 215 applications and the number of NSLs issued seems to suggest that FBI agents were bypassing judicial review in the section 215 process by using NSLs in a manner not authorized by law. An example of this abuse of the system was documented in the IG's 2008 section 215 report. The FBI applied to the FISC for a section 215 order, only to be denied on First Amendment grounds. The FBI instead used NSLs to obtain the information.

While this portion of the IG report is heavily redacted, it appears that sometime in 2006 the FBI twice asked the FISC for a section 215 order seeking "tangible things" as part of a counterterrorism case. The court denied the request, both times, because "the facts were too 'thin' and [the] request implicated the target's First Amendment rights."[37] Rather than re-evaluating the underlying investigation based on the court's First Amendment concerns, the FBI circumvented the court's oversight and pursued the investigation using three NSLs that were predicated on the same information contained in the section 215 application.[38] The IG questioned the legality of the FBI's use of NSLs based on the same factual predicate contained in the section 215 request rejected by the FISC on First Amendment grounds, because the authorizing statutes for NSLs and section 215 orders contain the same First Amendment caveat.[39]

The IG also discovered the FISC was not the first to raise First Amendment concerns over this investigation to FBI officials. Lawyers with the Department of Justice Office of Intelligence Policy Review(OIPR) raised the First Amendment issue when the FBI sent the section 215 application for its review.[40] The OIPR is supposed to oversee FBI intelligence investigations, but OIPR officials quoted in the IG report said the OIPR has "not been able to fully serve such an oversight role" and that they were often bullied by FBI agents:

> In addition, the former Acting Counsel for Intelligence Policy stated that there is a history of significant pushback from the FBI when OIPR questions agents about the assertions included in FISA applications. The OIPR attorney assigned to Section 215 requests also told us that she routinely accepts the FBI's assertions regarding the underlying investigations as fact and that the FBI would respond poorly if she questioned their assertions.[41]

SUGGESTED REFORM OF NSL STATUTES

- Repeal the expanded NSL authorities that allow the FBI to demand information about innocent people who are not the targets of any investigation. Reinstate prior standards limiting NSLs to information about terrorism suspects and other agents of foreign powers.
- Allow gag orders only upon the authority of a court, and only when necessary to protect national security. Limit scope and duration of such gag orders and ensure that their targets and recipients have a meaningful right to challenge them before a fair and neutral arbiter.
- Impose judicial oversight of all Patriot Act authorities. Allowing the FBI to self-certify that it has met the statutory requirements invites further abuse and overuse of NSLs. Contemporaneous and independent oversight of the issuance of NSLs is needed to ensure that they are no longer issued at the drop of a hat to collect information about innocent U.S. persons.

Two bills introduced in the 110th Congress would have reined in the FBI's use of NSLs: the National Security Letter Reform Act of 2007 (H.R. 3189) sponsored by Representative Jerrold Nadler (D-NY) and the NSL Reform Act of 2007 (S. 2088) sponsored by Senator Russ Feingold (D-WI). These were good bills that took great strides toward limiting the FBI's authority to issue NSLs. Assuming their reintroduction in similar form, they should be acted upon promptly. Further delay will simply mean that thousands more innocent people will have their private records collected by the FBI.

When the FISC raised First Amendment concerns about the FBI investigation, the FBI general counsel decided the FBI would continue the investigation anyway, using methods that had less oversight. When asked whether the court's concern caused her to review the underlying investigation for compliance with legal guidelines that prohibit investigations based solely on protected First Amendment activity, the general counsel said she did not because "she disagreed with the court's ruling and nothing in the court's ruling altered her belief that the investigation was appropriate."[42] Astonishingly, she put her own legal judgment above the decision of the court. She added that the FISC "does not have the authority to close an FBI investigation."[43]

A former OIPR counsel for intelligence policy argued that while investigations based solely on association with subjects of other national security investigations were "weak," they were "not necessarily illegitimate."[44] It is also important to note that this investigation, based on simple association with the subject of another FBI investigation, was apparently not an aberration. The FBI general counsel told the IG the FBI would have to close "numerous investigations" if they could not open cases against individuals who merely have contact with other subjects of FBI investigations.[45] Conducting "numerous investigations" based upon mere contact, and absent facts establishing a reasonable suspicion of wrongdoing, will only result in wasted effort, misspent security resources and unnecessary violations of the rights of innocent Americans.

The FBI's stubborn defiance of OIPR attorneys and the FISC demonstrates a dangerous interpretation of the legal limits of the FBI's authority at its highest levels, and lays bare the inherent weakness of any set of internal controls. The FBI's use of NSLs to circumvent more arduous section 215 procedures confirms the ACLU's previously articulated concerns that the lack of oversight of the FBI's use of its NSL authorities would lead to such inappropriate use.

Moreover, despite the FBI's infrequent use of section 215, the IG discovered serious deficiencies in the way it managed this authority. The IG found substantial bureaucratic delays at both FBI headquarters and OIPR in bringing section 215 applications to the FISC for approval. While neither the FBI's FISA Management System nor DOJ's OIPR tracking system kept reliable records regarding the length of time section 215 requests remained pending, the IG was able to determine that processing times for section 215 requests ranged from ten days to an incredible 608 days, with an average delay of 169 days for approved orders and 312 days for withdrawn requests.[46] The IG found these delays were the result of unfamiliarity with the proper process, simple mismanagement of the section 215 requests and an unnecessarily bureaucratic, self-imposed, multi-layered review process.[47] Most tellingly, the IG's 2008 report found that the process had not improved since the IG identified these problems had been identified in the 2007 audit.[48] DOJ has used long processing times

FACES *of* SURVEILLANCE

Photo Credit: Melissa Haynes, Internet Archive

BREWSTER KAHLE is the founder and digital librarian of the Internet Archive, a digital library. In November 2007, the FBI used an NSL to demand personal information about one of the Archive's users. The NSL also included a gag order, prohibiting the Archive from revealing the existence of the letter. In April 2008, the FBI withdrew the unconstitutional NSL as part of the settlement of a lawsuit brought by the ACLU and the Electronic Frontier Foundation. "The free flow of information is at the heart of every library's work. That's why Congress passed a law limiting the FBI's power to issue NSLs to America's libraries. While it's never easy standing up to the government - particularly when I was barred from discussing it with anyone - I knew I had to challenge something that was clearly wrong. I'm grateful that I am able now to talk about what happened to me, so that other libraries can learn how they can fight back from these overreaching demands."

for FISA applications as justification for expanding its surveillance powers and reducing FISC review; but this evidence shows clearly that ongoing mismanagement at the FBI and OIPR drives these delays, not a lack of authority.[10] Congress should instead compel efficiency at these agencies by increasing its oversight and reining in these expanded authorities.

SUGGESTED REFORMS

- Repeal the expanded section 215 authorities that allow the FBI to demand information about innocent people who are not the targets of any investigation. Return to previous standards limiting the use of 215 authorities to gather information only about terrorism suspects and other agents of foreign powers.

UNCONSTITUTIONAL: COURT CHALLENGES TO THE PATRIOT ACT

Court challenges offered another source of information about the government's misuse of Patriot Act powers.

National Security Letter Gag Orders

The ACLU challenged the non-disclosure and confidentiality requirements in NSLs in three cases. The first, *Doe v. Ashcroft*, involved an NSL served on an Internet Service Provider (ISP) in 2004 demanding customer records pursuant to the Electronic Communications Privacy Act (ECPA).[50] The letter prohibited the anonymous ISP and its employees and agents "from disclosing to any person that the FBI sought or obtained access to information or records under these provisions."[51] In the midst of a lawsuit over the constitutionality of the NSL provisions in ECPA, the Patriot Act reauthorization[51] was enacted amending the NSL provision but maintaining the government's authority to request sensitive customer information and issue gag orders – albeit in a slightly narrower set of circumstances. In September 2007, the District Court for the Southern District of New York found that even with the reauthorization amendments the gag provisions violated the Constitution. The court struck down the amended ECPA NSL statute in its entirety,[52] with Judge Victor Marrero writing that the statute's gag provisions violated the First Amendment and the principle of separation of powers.

In December 2008 the U.S. Court of Appeals for the Second Circuit upheld the decision in part. The appeals court invalidated parts of the statute that placed the burden on NSL recipients to initiate judicial review of gag orders, holding that the government has the burden to justify silencing NSL recipients. The appeals court also invalidated parts of the statute that narrowly limited judicial review of the gag orders – provisions that required the courts to treat the government's claims about the need for secrecy as conclusive and required the courts to defer entirely to the executive branch.[53] As this is written, the FBI still maintains its gag on the ISP even though it abandoned its demand for the records.

The second case, *Library Connection v. Gonzales*, involved an NSL served on a consortium of libraries in Connecticut.[54] In September 2006, a federal district court ruled that the gag on the librarians violated the First Amendment. The government ultimately withdrew both the gag and its demand for records.

FACES *of* SURVEILLANCE

TARIQ RAMADAN, a Swiss native and Visiting Fellow at the University of Oxford, is a leading scholar of the Muslim world. The U.S. government revoked Ramadan's visa in August 2004, preventing him from assuming a tenured teaching position at the University of Notre Dame and from attending speaking engagements with U.S. audiences. Although Professor Ramadan has been a consistent critic of terrorism and those who use it, the Department of Homeland Security cited a provision of the Patriot Act that allows the government to deny a visa to anyone whom the government believes has "endorse[d] or espouse[d] terrorist activity" as the basis for its decision. The government later withdrew that accusation but Professor Ramadan remains barred from the country.

The third case, *Internet Archive v. Mukasey*, involved an NSL served on a digital library.[58] In April 2008, the FBI withdrew the NSL and the gag as a part of the settlement of the legal challenge brought by the ACLU and the Electronic Frontier Foundation.[59] In every case in which an NSL recipient has challenged an NSL in court, the government has withdrawn its demand for records, creating doubt regarding the government's need for the records in the first place.

In addition, a 2007 ACLU Freedom of Information Act suit revealed that the FBI was not the only agency abusing its NSL authority. The Department of Defense (DOD) does not have the authority to investigate Americans, except in extremely limited circumstances. Recognizing this, Congress gave the DOD a narrow NSL authority, strictly limited to non-compulsory requests for information regarding DOD employees in counterterrorism and counter-intelligence investigations,[60] and to obtaining financial records[61] and consumer reports[62] when necessary to conduct such investigations. Only the FBI has the authority to issue compulsory NSLs for electronic communication records and for certain consumer information from consumer reporting agencies. This authority can only be used in furtherance of authorized FBI investigations. Records obtained by the ACLU show the DOD issued hundreds of NSLs to collect financial and credit information since September 2001, and at times asked the FBI to issue NSLs compelling the production of records the DOD wanted but did not have the authority to obtain. The documents suggest the DOD used the FBI to circumvent limits on the DOD's investigative authority and to obtain information it was not entitled to under the law. The FBI compliance with these DOD requests – even when it was not conducting its own authorized investigation – is an apparent violation of its own statutory authority.[63]

Material Support for Terrorism Provisions

Laws prohibiting material support for terrorism, which were expanded by the Patriot Act, are in desperate need of re-evaluation and reform. Intended as a mechanism to starve terrorist organizations of resources, these statutes instead undermine legitimate humanitarian efforts and perpetuate the perception that U.S. counterterrorism policies are unjust.

The Antiterrorism and Effective Death Penalty Act of 1996 (AEDPA), passed in the wake of the Oklahoma City bombing, criminalized providing material support to terrorists or terrorist organizations.[64] Title 18 U.S.C. § 2339A makes it a federal crime to knowingly provide material support or resources in preparation for or in carrying out specified crimes of terrorism, and 18 U.S.C. § 2339B outlaws the knowing provision of material support or resources to any group of individuals the secretary of state has designated a foreign terrorist organization (FTO).[65] AEDPA defined "material support or resources" as "currency or other financial securities, financial services, lodging, training, safe-houses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel, transportation, and other physical assets, except medicine or religious materials."[66] AEDPA also amended the Immigration & Nationality Act (INA) to give the secretary of state almost unfettered discretion to designate FTOs.[67]

The secretary of state may designate an organization as an FTO if she finds that the organization is foreign, that it engages in or retains the capacity and intent to engage in terrorist activities, and that its activities threaten the national defense, foreign relations or economic interests of the United States. An FTO may challenge its designation in federal court but the INA gives the government the ability to use classified information *in camera* and *ex parte*, so the designated organization never gets to see, much less dispute the allegations against it. Moreover, a judge must

determine that the government acted in an arbitrary and capricious manner – a very difficult legal standard for an FTO to prove – in order to overturn a designation.

Section 805 of the Patriot Act expanded the already overbroad definition of "material support and resources" to include "expert advice or assistance," and **section 810** increased penalties for violations of the statute.[60] Through IRTPA, Congress narrowed these provisions in 2004 to require that a person have knowledge that the organization is an FTO, or has engaged or engages in terrorism. However, the statute still does not require the government to prove that the person specifically intended for his or her support to advance the terrorist activities of the designated organization.[61] In fact, the government has argued that those who provide support to designated organizations can run afoul of the law even if they oppose the unlawful activities of the designated group, intend their support to be used only for humanitarian purposes and take precautions to ensure that their support is indeed used for these purposes.[62] This broad interpretation of the material support prohibition effectively prevents humanitarian organizations from providing needed relief in many parts of the world where designated groups control schools, orphanages, medical clinics, hospitals and refugee camps.[63]

In testimony before Congress in 2005, ACLU of Southern California staff attorney Ahilan T. Arulanantham gave a first-hand account of the difficulties he experienced while providing humanitarian aid to victims of the 2004 tsunami in Sri Lanka.[64] At the time of the tsunami approximately one-fifth of Sri Lanka was controlled by the Liberation Tigers of Tamil Eelam (LTTE), an armed group fighting against the Sri Lankan government. The U.S. government designated the LTTE as an FTO, but for the 500,000 people living within its territory, the LTTE operates as an authoritarian military government. As a result, providing humanitarian aid to needy people in this part of Sri Lanka almost inevitably requires dealing directly with institutions the LTTE controls. And because there is no humanitarian exemption from material support laws (only the provision of medicine and religious materials are exempted), aid workers in conflict zones like Sri Lanka are at risk of prosecution by the U.S. government. Arulanantham explained the chilling effect of these laws:

> I have spoken personally with doctors, teachers, and others who want to work with people desperately needing their help in Sri Lanka, but fear liability under the "expert advice," "training," and "personnel" provisions of the law. I also know people who feared to send funds for urgent humanitarian needs, including clothing, tents, and even books, because they thought that doing so might violate the material support laws. I have also consulted with organizations, in

FACES *of* SURVEILLANCE

WANDA GUTHRIE, a volunteer with the Thomas Merton Center for Peace & Justice, an organization founded in 1972 to bring people from diverse philosophies and faiths together to work, through nonviolent efforts, for a more just and peaceful world, was monitored by the FBI Joint Terrorism Task Force. "The government's surveillance of the TMC events and gatherings which may include those of Roots for Peace is just horrible. Spying invades peoples' privacy and sacred space when they are speaking out – and make no bones about it, when you're speaking out for peace it is sacred space. For the FBI to monitor us as if we were terrorists is unconscionable."

my capacity as an ACLU attorney, that seek to send money for humanitarian assistance to areas controlled by designated groups. I have heard those organizations express grave concerns about continuing their work for precisely these reasons. Unfortunately, the fears of these organizations are well-justified. Our Department of Justice has argued that doctors seeking to work in areas under LTTE control are not entitled to an injunction against prosecution under the material support laws, and it has even succeeded in winning deportation orders under the immigration law's definition of material support, for merely giving food and shelter to people who belong to a "terrorist organization" even if that group is not designated.[69]

Tragically, our counterterrorism laws make it more difficult for U.S. charities to operate in parts of the world where their good works could be most effective in winning the battle of hearts and minds. In 2006 Congress passed the Patriot Act reauthorization, making the material support provisions permanent.[70]

Such unjust and counter-productive consequences are a direct result of the overbroad and unconstitutionally vague definition of material support in the statute. The First Amendment protects an individual's right to join or support political organizations and to associate with others in order to pursue common goals. The framers understood that protecting speech and assembly were essential to the creation and functioning of a vibrant democracy. As a result, the government cannot punish mere membership in or political association with disfavored groups – even those that engage in both lawful and unlawful activity – without the strictest safeguards.

The material support provisions impermissibly criminalize a broad range of First Amendment-protected activity, both as a result of their sweeping, vague terms and because they do not require the government to show that a defendant *intends* to support the criminal activity of a designated FTO. Courts have held that vague statutes should be invalidated for three reasons: "(1) to avoid punishing people for behavior that they could not have known was illegal; (2) to avoid subjective enforcement of laws…; and (3) to avoid any chilling effect on the exercise of First Amendment freedoms."[71] Material support prohibitions against "training," "services" and "expert advice and assistance"[72] fail each of these three standards.

Any suggestion that the government would not use the material support statutes to prosecute purely First Amendment-protected speech is belied by the fact that it already has. In a most notorious example, the government brought charges against University of Idaho Ph.D. candidate Sami Omar Al-Hussayen, whose volunteer work managing websites for a Muslim charity led to a six-week criminal trial for materially supporting terrorism. The prosecution argued that by running a website that had links to other websites that carried speeches advocating violence, Al-Hussayen provided "expert assistance" to terrorists. A jury ultimately acquitted Al-Hussayen of all terrorism-related charges.[73]

SUGGESTED REFORM OF MATERIAL SUPPORT STATUTES

- Amend the material support statutes to require specific intent to further an organization's unlawful activities before imposing criminal liability.
- Remove overbroad and impermissibly vague language, such as "training," "service" and "expert advice and assistance," from the definition of material support.
- Establish an explicit duress exemption to remove obstacles for genuine refugees and asylum-seekers to enter and/or remain in the United States.
- Provide notice, due process and meaningful review requirements in the designation process, and permit defendants charged with material support to challenge the underlying designation in their criminal cases.

The material support provisions also impose guilt by association in violation of the Fifth Amendment. Due process requires the government to prove personal guilt – that an individual *specifically intended* to further the group's unlawful ends – before criminal sanctions may be imposed.[75] Even with the IRTPA amendments, the material support provisions do not require specific intent. Rather, the statutes impose criminal liability based on the mere knowledge that the group receiving support is an FTO or engages in terrorism. Indeed, a Florida district court judge in *United States v. Al-Arian* warned that under the government's reading of the material support statute, "a cab driver could be guilty for giving a ride to an FTO member to the UN."[76] And these constitutional deficiencies are only exacerbated by the unfettered discretion these laws give the secretary of state to designate groups, and the lack of due process afforded to groups that wish to appeal their designation.

A recent study of material support prosecutions from September 2001 to July 2007 reveals an unusually high acquittal rate for these cases.[77] The DOJ's trial conviction rate for all felonies is fairly steady over the years: 80% in 2001, 82% in 2002, 82% in 2003 and 80% in 2004.[78] But almost half (eight of 17) of the defendants charged with material support of terrorism under §2339B who chose to go to trial were acquitted, and three others successfully moved to have their charges dismissed before trial.[79] This disparity suggests that the government is overreaching in charging material support violations for behavior not reasonably linked to illegal or violent activity. The data is especially troubling given that the median sentence for a conviction at trial for material support under §2339B is 84 months longer than for a guilty plea to the same offense.[80] That those defendants who risk the additional 84 months in prison are acquitted in almost half of the cases raises a disturbing question of whether the government is using the draconian sentences provided in the Patriot Act-enhanced statute to compel plea bargains where the evidence might not support conviction at trial. Of the 61 defendants whose cases were resolved during the study period, 30 pled guilty to material support and another 11 pled guilty to other charges. Only nine of the remaining 20 were convicted.

In *Humanitarian Law Project v. Mukasey*, a group of organizations and individuals seeking to support the nonviolent and lawful activities of Kurdish and Tamil humanitarian organizations challenged the constitutionality of the material support provisions on First and Fifth Amendment grounds.[81] They contended that the law violated the Constitution by imposing a criminal penalty for association without requiring specific intent to further an FTO's unlawful goals, and that the terms included in the definition of "material support or resources" were impermissibly vague. In 2007, the U.S. Court of Appeals for the Ninth Circuit found the terms "training" and "service," and part of the definition of "expert advice and assistance" unconstitutionally vague under the Fifth Amendment.[82] The government is appealing this decision.

FACES *of* SURVEILLANCE

JOHN DOE, the President of an Internet Service Provider, is an NSL recipient who has been under an FBI gag order for more than four years. John Doe challenged the constitutionality of the NSL statute. Because of the gag order, the lawsuit was initially filed under seal, and even today the ACLU is prohibited from disclosing its client's identity. The FBI continues to maintain the gag order even though the underlying investigation is more than four years old (and may well have ended), and even though the FBI abandoned its demand for records two years ago. In December of 2008, the U.S. Court of Appeals for the Second Circuit ruled that the NSL statute's gag provisions, as amended by Congress in 2006, violated the First Amendment.

Ideological Exclusion

The Patriot Act revived the discredited practice of ideological exclusion: denying foreign citizens' entry into the U.S. based solely on their political views and associations, rather than their conduct.

Section 411 of the Patriot Act amended the INA to expand the grounds for denying foreign nationals admission into the United States, and for deporting those already here.[91] This section authorizes the exclusion not only of foreign nationals who support domestic or foreign groups the U.S. has designated as "terrorist organizations," but also those who support "a political, social or other similar group whose public endorsement of acts of terrorist activity the secretary of state has determined undermines United States efforts to reduce or eliminate terrorist activities." Moreover, Congress added a provision that authorizes the exclusion of those who have used a "position of prominence within any country to endorse or espouse terrorist activity, or to persuade others to support terrorist activity or a terrorist organization, in a way that the secretary of state has determined undermines United States efforts to reduce or eliminate terrorist activities."[92] Though ostensibly directed at terrorism, the provision focuses on words, not conduct, and its terms are broad and easily manipulated. The State Department's Foreign Affairs Manual takes the sweeping view that the provision applies to foreign nationals who have voiced "irresponsible expressions of opinion." Over the last six years, dozens of foreign scholars, artists and human rights activists have been denied entry to the United States not because of their actions – but because of their political views, their writings and their associations.

SUGGESTED REFORM OF IDEOLOGICAL EXCLUSION STATUTES

- Bar ideological exclusion based on speech that would be protected in the United States under the First Amendment.
- Repeal the "endorse or espouse" provision.

During the Cold War, the U.S. was notorious for excluding suspected communists. Among the many "dangerous" individuals excluded in the name of national security were Nobel Laureates Gabriel Garcia Márquez, Pablo Neruda and Doris Lessing, British novelist Graham Greene, Italian playwright Dario Fo and Pierre Trudeau, who later became prime minister of Canada. When Congress repealed the Cold War-era communist exclusion laws, it determined that "it is not in the interests of the United States to establish one standard of ideology for citizens and another for foreigners who wish to visit the United States." It found that ideological exclusion caused "the reputation of the United States as an open society, tolerant of divergent ideas" to suffer. When Congress enacted the "endorse or espouse" provision, it ignored this historical lesson.

The ACLU challenged the constitutionality of "ideological exclusion" in *American Academy of Religion v. Chertoff*. In July 2004, the Department of Homeland Security (DHS) used the provision to revoke the visa of Tariq Ramadan, a Swiss citizen, one of Europe's leading scholars of Islam and a vocal critic of U.S. policy. Ramadan had accepted a position to teach at the University of Notre Dame. After DHS and the State Department failed to act on a second visa application that would have permitted Ramadan to teach at Notre Dame, he applied for a B visa to attend and participate in conferences in the U.S. After the government failed to act on *that* application for many months, in January 2006, the American Academy of Religion (AAR), the American Association of University Professors and PEN American Center – organizations that had invited Professor Ramadan to speak in the United States – filed suit. They argued that the government's exclusion of Professor Ramadan, as well as the ideological exclusion provision, violated their First Amendment right to receive information and hear ideas, and compromised their ability to

engage in an intellectual exchange with foreign scholars. When challenged in court, the government abandoned its allegation that Professor Ramadan had endorsed terrorism.[43]

The district court held that the government could not exclude Ramadan without providing a legitimate reason and that it could not exclude Ramadan based solely on his speech. It ordered the government to adjudicate Ramadan's pending visa application within 90 days.[44] Thereafter, however, the government found an entirely new basis for barring Ramadan. Invoking the expanded material support provisions of the Real ID Act, the government determined that Professor Ramadan was inadmissible because of small donations he made from 1998 to 2002 to a lawful European charity that provides aid to Palestinians.[45] The plaintiffs continued to challenge the legality of Professor Ramadan's exclusion as well as the constitutionality of the ideological exclusion provision. In July 2007, the district court upheld Professor Ramadan's exclusion but did not rule on the constitutionality of the ideological exclusion provision, finding instead that the plaintiffs lacked standing. The ACLU appealed and the case remains pending before the the U.S. Court of Appeals for the Second Circuit.

The imposition of an ideological litmus test at the border is raw censorship and violates the First Amendment. It allows the government to decide which ideas Americans may or may not hear. Ideological exclusion skews political and academic debate in the U.S. and deprives Americans of information they have a constitutional right to hear. Particularly now, Americans should be engaged with the world, not isolated from it.

Relaxed FISA Standards

Section 218 of the Patriot Act amended FISA to eliminate the requirement that the *primary purpose* of a FISA search or surveillance must be to gather foreign intelligence.[46] Under the Patriot Act's amendment, the government needs to show only that a *significant purpose* of the search or surveillance is to gather foreign information in order to obtain authorization from the FISC.[47] This seemingly minor change allows the government to use FISA to circumvent the basic protections of the Fourth Amendment, even where criminal prosecution is the government's primary purpose for conducting the search or surveillance. This amendment allows the government to conduct intrusive investigations to gather evidence for use in criminal trials without establishing probable cause of illegal activity before a neutral and disinterested magistrate, and without providing notice required with ordinary warrants. Instead, the government can obtain authorization for secret searches from a secret and unaccountable court based on an assertion of probable cause that the target is an "agent of a foreign power," a representation the court must accept unless "clearly erroneous." An

FACES *of* SURVEILLANCE

Photo Credit: AP Images

BRANDON MAYFIELD, an American attorney practicing in Portland, Oregon, was subjected to secret FISA searches of his home and office after an FBI agent mistakenly identified his fingerprint on materials related to a terrorist bombing in Madrid, Spain. The FBI agents who conducted the searches of the Mayfield home left tell-tale signs of their presence, leading the Mayfield family to fear their home was being burglarized. Mayfield challenged the constitutionality of the Patriot Act provision that allows FBI agents to use FISA orders to gather evidence in a criminal investigation. "In the debate over the scope of the government's authority to wiretap Americans we often hear people say, 'If you're not doing something wrong you have nothing to worry about.' I am here to tell you that even the innocent can have their lives turned upside-down when laws designed to protect against unrestrained government actions are weakened."

improperly targeted person has no way of knowing his or her rights have been violated, so the government can never be held accountable.

Lowering evidentiary standards does not make it easier for the government to spy on the guilty. Rather, it makes it more likely that the innocent will be unfairly ensnared in overzealous investigations. A most disturbing example of the way this provision enables the government to spy on innocent Americans is the case of Brandon Mayfield, an American citizen and former U.S. Army officer who lives with his wife and three children in Oregon where he practices law.

In March 2004, the FBI began to suspect Mayfield of involvement in a series of terrorist bombings in Madrid, Spain, based on an inaccurate fingerprint identification. Although Mayfield had no criminal record and had not left the U.S. in over 10 years, he and his family became subject to months of secret physical searches and electronic surveillance approved by the FISC. In May 2004, Mayfield was arrested and imprisoned for weeks until news reports revealed that the fingerprints had been matched to an Algerian national, Ouhane Daoud. Mayfield was released the following day. In a subsequent lawsuit, *Mayfield v. United States*, a federal district court held that the Patriot Act amendment violated the Fourth Amendment by allowing the government to avoid traditional judicial oversight to obtain a surveillance order, retain and use information collected in criminal prosecutions without allowing the targeted individuals a meaningful opportunity to challenge the legality of the surveillance, intercept communications and search a person's home without ever informing the targeted individual and circumvent the Fourth Amendment's particularity requirement.[28]

SUGGESTED REFORM OF FISA STATUTES

- Restore the primary purpose requirement to FISA.

ONLY ONE PIECE OF THE PUZZLE

The Patriot Act may have been the first overt expansion of domestic spying powers after September 11, 2001 – but it certainly wasn't the last, and arguably wasn't even the most egregious. There have been many significant changes to our national security laws over the past seven years, and addressing the excesses of the Patriot Act without examining the larger surveillance picture may not be enough to rein in an out-of-control intelligence-gathering regime. Congress must not only conduct vigorous oversight of the government's use of Patriot Act powers, it must also review the other laws, regulations and guidelines that now permit surveillance of Americans without suspicion of wrongdoing. Congress should scrutinize the expanded surveillance authorities found in the Attorney General Guidelines for Domestic FBI Operations, Executive Order 12333, IRTPA, the amended FISA, and the ECPA. Ultimately, Congress must examine the full panoply of intelligence activities, especially domestic intelligence gathering programs, and encourage a public debate about the proper nature and reach of government surveillance programs on American soil and abroad.

Fundamentally, Congress must recognize that overbroad, ineffective or abusive surveillance programs are counterproductive to long-term government interests because they undermine public confidence and support of U.S. anti-terrorism programs. An effort by Congress to account fully for abuses of government surveillance authorities in the recent past is absolutely necessary for several reasons. First, only by holding accountable those who engaged in intentional violations of law can we re-establish the primacy of the law and deter future abuses. Second, only by creating an accurate historical record of the failure of these abusive programs can government officials learn from these mistakes and properly reform our national security laws and policies. Finally, only by vigorously exercising its oversight responsibility in matters of national security can Congress reassert its critical role as an effective check against abuse of executive authority.

The Constitution gives Congress the responsibility to conduct oversight, and Congress must fulfill this obligation to ensure the effective operation of our government. Congress should begin vigorous and comprehensive oversight hearings to examine all post-9/11 national security programs to evaluate their effectiveness and their impact on Americans' privacy and civil liberties, and it should hold these hearings in public to the greatest extent possible.

FACES *of* SURVEILLANCE

Photo Credit: Rick Rosenthal

KONSTANTY HORDYNSKI, a student at the University of California at Santa Cruz, was quite surprised to learn that he was in a Pentagon domestic threat database. "I didn't protest with Students Against War to be threatening, or to be un-American, or to waste anyone's time. I protested because it was a way I could stand up for what I believed was right. I knew that my actions were protected by the Constitution. Yet the government believes that the peaceful protest in which I took part is a "credible threat." When lawfully standing up for my beliefs—standing up for what I think is right and just—is a "threat" to the government, something is wrong..."

CONCLUSION – IT IS TIME TO RECLAIM PATRIOTISM

In 2009, Congress must once again revisit the Patriot Act, as three temporary provisions from the 2006 reauthorization are set to expire by the end of the year. This time, however, Congress is not completely in the dark. The IG audits ordered in the Patriot Act reauthorization proved the government lied when it claimed that no Patriot Act powers had been abused. Critics former Attorney General John Ashcroft once derided as hysterical librarians were proven prescient in their warnings that these arbitrary and unchecked authorities would be misused.[30] Just like the colonists who fought against writs of assistance, these individuals recognized that true patriotism meant standing up for their rights, even in the face of an oppressive government and an unknowable future. Certainly there are threats to our security, as there always have been, but our nation can and must address those threats without sacrificing our essential values or we will have lost the very freedoms we strive to protect.

Courts all around the country have spoken, striking down several Patriot Act provisions that infringed on the constitutional rights of ordinary Americans. Yet the government has successfully hidden the true impact of the Patriot Act under a cloak of secrecy that even the courts couldn't – or wouldn't – penetrate.

It is time for Congress to act. Lawmakers should take this opportunity to examine thoroughly all Patriot Act powers, and indeed all national security and intelligence programs, and bring an end to any government activities that are illegal, ineffective or prone to abuse. This oversight is essential to the proper functioning of our constitutional system of government and becomes more necessary during times of crisis, not less. Serving as an effective check against the abuse of executive power is more than just Congress' responsibility; it is its patriotic duty.

APPENDIX – THE PATRIOT ACT AT A GLANCE

Many provisions in the amended Patriot Act have been abused – or have the potential to be – because of their broad and sweeping nature. The sections detailed on these pages need congressional oversight. Despite numerous hearings during the 2005 reauthorization process, there is a dearth of meaningful information about their use. Congress and the public need real answers, and the forthcoming expiration date is the perfect opportunity to revisit the provisions that have worried civil libertarians since 2001:

- Section 203: Information Sharing. The Patriot Act and subsequent statutes encourage or require information sharing. While it is important for critical details to reach the right people, little is known about the breadth of use and the scope of distribution of our personal information.

- Section 206: Roving "John Doe" Wiretaps. Typical judicial orders authorizing wiretaps, including Foreign Intelligence Surveillance Act (FISA) wiretap orders, identify the person or place to be monitored. This requirement has its roots firmly planted in the original Bill of Rights – the giants of our history having insisted on such a concept, now memorialized in the Fourth Amendment, where it calls for warrants "particularly describing the place to be searched, and the persons or things to be seized." However, these roving warrants are required to specify neither person nor place, amounting to the "general warrants" that our nation's founders had abhorred. This section will expire on December 31, 2009.

- Section 209: Access to Stored Communications. The Patriot Act amended criminal statutes so that the government can obtain opened emails and emails older than 180 days with only a subpoena instead of a warrant.

- Section 212: Voluntary Disclosures and Exigent Letters. Current law permits telecommunications companies to release consumer records and content to the government when they have a good faith belief it relates to a threat. However, the Patriot Act and subsequent legislation lowered that trigger from a "reasonable" to "good faith" belief that the information reflects an emergency. The act also took away the requirement that the threat be "imminent." The Department of Justice Inspector General has confirmed that the government is using this loophole to request information in the absence of true emergencies.

- Section 213: Sneak and Peek Searches. These are delayed notice search warrants. Before the Patriot Act, criminal search warrants required prior notification except in exigent circumstances or for stored communications when notice would "seriously jeopardize an investigation." The Patriot Act expanded this once narrow loophole – used solely for stored communications – to all searches. Agents might now use this vague catch-all to circumvent longstanding Fourth Amendment protections. These sneak and peek warrants are not limited to terrorism cases – thereby undermining one of the core justifications for the original Patriot Act. In fact, for the 2007 fiscal year, the government reports that out of 690 sneak and peak applications, only seven, or about one percent, were used for terrorism cases.

- Section 214: Pen Register/Trap and Trace Orders Under FISA. Pen register/trap and trace devices pick up communication records in real time and provide the government with a streaming list of phone calls or emails made by a person or account. Before the Patriot Act, this section was limited to tracking the

communications of suspected terrorists. Now, it can be used against people who are generally relevant to an investigation, even if they have done nothing wrong.

- Section 215: FISA Orders for Any Tangible Thing. These are FISA Court orders for any tangible thing – library records, a computer hard drive, a car – the government claims is relevant to an investigation to protect against terrorism. Since passage of the Patriot Act, the person whose things are being seized need not be a suspected terrorist or even be in contact with one. This section is scheduled to expire on Dec. 31, 2009.

- Section 216: Criminal Pen Register/ Trap and Trace Orders. The Patriot Act amended the criminal code to clarify that the pen register/trap and trace authority permits the government to collect Internet records in real time. However, the statute does not define 'Internet record' clearly. Congress needs to make sure that the government is not abusing this provision to collect lists of everything an innocent person reads on the Internet.

- Section 218: "Significant Purpose" to Begin an Intelligence Wiretap or Conduct Physical Searches. Before the Patriot Act, the extensive and secretive powers under FISA could only be used when the collection of foreign intelligence – as opposed to prosecution – was the primary purpose of the surveillance. Now, collecting foreign intelligence need only be a "significant" purpose, permitting the government to use this lower FISA warrant standard in place of a traditional criminal warrant. Congress must find out whether the government has conducted surveillance under the relaxed FISA standards for criminal prosecutions.

- Section 219: Single Jurisdiction Search Warrants. The Patriot Act allows judges sitting in districts where terrorism-related activities may have occurred to issue warrants outside of their district, possibly causing hardship on a recipient who may want to challenge the warrant.

- Section 220: Nationwide Search Warrants for Electronic Evidence. This provision permits a judge to issue an order for electronic evidence outside of the district in which he or she sits. This provision may cause a hardship for a remote Internet or phone service provider who wants to challenge the legality of the order.

- Section 411: Ideological Exclusion. The Patriot Act amended the Immigration and Nationality Act to expand the terrorism-related grounds for denying foreign nationals admission into the United States, and for deporting aliens already here. This revived the discredited practice of ideological exclusion: excluding foreign citizens based solely on their political views and associations, rather than their conduct.

- Section 505: National Security Letters. NSLs are demands for customer records from financial institutions, credit bureaus and communications service providers. They have existed for decades, but prior to passage of the Patriot Act and its subsequent amendments, they were limited to collecting information on suspected terrorists or foreign actors. Recipients are gagged from telling anyone besides their lawyers and those necessary to respond to the request that they either received or complied with a NSL. The gag has been struck down as unconstitutional but remains on the books. In 2007 and 2008, the Justice Department's inspector general reported that upwards of 50,000 NSLs are now issued each year, many of which obtain information on people two and three times removed from a suspected terrorist.

- Section 802: Definition of Domestic Terrorism. The Patriot Act broadened the definition of domestic terrorist acts to include any state or federal crime as a predicate offense, including peaceful civil disobedience.

- Section 805: Material Support. This provision bars individuals from providing material support to terrorists, defined as providing any tangible or intangible good, service or advice to a terrorist or designated group. As amended by the Patriot Act and other laws since September 11, this section criminalizes a wide array of activities, regardless of whether they actually or intentionally further terrorist goals or organizations. Federal courts have struck portions of the statute as unconstitutional and a number of cases have been dismissed or ended in mistrial.

- Section 6001 of intelligence reform bill: "Lone Wolf" Surveillance and Search Orders. Since its inception, FISA has regulated searches and surveillance on US soil for intelligence purposes. Under FISA, a person would have to belong to a group suspected of terrorism before he or she could be surveilled. The Intelligence Reform and Terrorism Prevention Act of 2004 added a new category, allowing someone wholly unaffiliated with a terrorist organization to be targeted for surveillance. This section is scheduled to expire on December 31, 2009.

ENDNOTES

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

2 *Boyd v. United States*, 116 U.S. 616, 624 (1886).

3 Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 Mich. L. Rev. 547, 556 (1999).

4 *See Boyd v. United States*, 116 U.S. 616 (1886).

5 *Id.* at 625.

6 *Id.* at 625.

7 John Yoo and Eric Posner, *Patriot Act Under Fire*, AMERICAN ENTERPRISE INSTITUTE ONLINE, Dec. 1, 2003, *available at* http://www.aei.org/publications/pubID.19661,filter./pub_detail.asp.

8 *Mapp v. Search Warrant*, 367 U.S. 717, 729 (1961).

9 *Marron v. United States*, 275 U.S. 192, 196 (1927).

10 *Stanford v. Texas*, 379 U.S. 476, 485 (1965).

11 *United States v. United States District Court (Keith)*, 407 U.S. 297, 313 (1972).

12 *Boyd v. United States*, 116 U.S. 616, 625 (1886).

13 S. REP. NO. 107-351 (Dec. 2002); H.R. REP. NO. 107-792 (Dec. 2002).

14 Letter from the American Civil Liberties Union to the U.S. House of Representatives (Oct. 23, 2001) (on file with author), *available at* http://www.aclu.org/natsec/emergpowers/14402leg20011023.html; Letter from the American Civil Liberties Union to the U.S. Senate (Oct. 23, 2001) (on file with author), *available at* http://www.aclu.org/natsec/emergpowers/14401leg20011023.html.

15 Letter from the American Civil Liberties Union to Senator Dianne Feinstein (April 4, 2005) (on file with author), *available at* http://www.aclu.org/safefree/general/17563leg20050404.html.

16 *USA PATRIOT Act of 2001: Hearing Before the S. Select Comm. on Intelligence*, 109th Cong. 97, 100 (2005) (statement of Alberto R. Gonzales, Attorney General of the United States and Robert S. Mueller, III, Director, Federal Bureau of Investigation). A later report by the Department of Justice Inspector General would reveal that between 2003 and 2005 the FBI had self-reported 19 possible legal violations regarding its use of National Security Letters to the President's Intelligence Oversight Board. Attorney General Gonzales received at least six reports detailing FBI intelligence violations, including misuse of NSLs, three months prior to his Senate testimony. To a certain degree AG Gonzales and FBI Director Mueller were truthful in their testimony because as they well knew, President Bush's Intelligence Oversight Board did not meet to "substantiate" any of the violations reported until the Spring of 2007. *See* DEP'T. OF JUSTICE, OFFICE OF INSPECTOR GENERAL, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF NATIONAL SECURITY LETTERS 69 (Mar. 2007), *available at* http://www.usdoj.gov/oig/special/s0703b/final.pdf; John Solomon, *Gonzales was told of FBI violations*, WASH. POST, Jul. 10, 2007, at A1, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2007/07/09/AR2007070902065.html; John Solomon, *In Intelligence World, a Mute Watchdog*, WASH. POST, Jul. 15, 2007, at A3, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2007/07/14/AR2007071400862.html.

17 USA PATRIOT Improvement and Reauthorization Act of 2005 (PIRA), Pub. L. No. 109-177, 120 Stat. 192 (2006).

18 Pub. L. No. 108-458, 118 Stat. 3638 (2004).

19 Electronic surveillance orders in criminal investigations are governed by the Omnibus Crime Control and Safe Streets Act of 1968. *See* 18 U.S.C.A. §§2510-2520 (2006).

20 PIRA, *supra* note 17, at § 119(a).

21 The four NSL authorizing statutes include the Electronic Communications Privacy Act, 18 U.S.C. § 2709 (2000), the Right

to Financial Privacy Act, 12 U.S.C. § 3401 (2000), the Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq. (2000), and the National Security Act of 1947, 50 U.S.C. § 436(a)(1)(2000).

22 As amended, the NSL statute authorizes the Director of the FBI or his designee (including a Special Agent in Charge of a Bureau field office) to impose a gag order on any person or entity served with an NSL. *See* 18 U.S.C. § 2709(c). To impose such an order, the Director or his designee must "certify" that, absent the non-disclosure obligation, "there may result a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person." *Id.* at § 2709(c)(1). If the Director of the FBI or his designee so certifies, the recipient of the NSL is prohibited from "disclos[ing] to any person (other than those to whom such disclosure is necessary to comply with the request or an attorney to obtain legal advice or legal assistance with respect to the request) that the [FBI] has sought or obtained access to information or records under [the NSL statute]." *Id.* Gag orders imposed under the NSL statute are imposed by the FBI unilaterally, without prior judicial review. While the statute requires a "certification" that the gag is necessary, the certification is not examined by anyone outside the executive branch. The gag provisions permit the recipient of an NSL to petition a court "for an order modifying or setting aside a nondisclosure requirement." *Id.* at § 3511(b)(1). However, in the case of a petition filed "within one year of the request for records," the reviewing court may modify or set aside the nondisclosure requirement only if it finds that there is "no reason to believe that disclosure may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person." *Id.* at § 3511(b)(2). Moreover, if a designated senior government official "certifies that disclosure may endanger the national security of the United States or interfere with diplomatic relations," the certification must be "treated as conclusive unless the court finds that the certification was made in bad faith." *Id.*

23 Dep't Of Justice, Office Of Inspector General, A Review Of The Federal Bureau Of Investigation's Use Of National Security Letters (Mar. 2007), *available at* http://www.usdoj.gov/oig/special/s0703b/final.pdf [hereinafter 2007 NSL Report]; Dep't Of Justice, Office Of Inspector General, A Review Of The Federal Bureau Of Investigation's Use Of Section 215 Orders for Business Records (Mar. 2007), *available at* http://www.usdoj.gov/oig/special/s0703a/final.pdf [hereinafter 2007 Section 215 Report].

24 2007 NSL Report, *supra* note 23, at 84.

25 2007 NSL Report, *supra* note 23, at 86-99.

26 Dep't Of Justice, Office Of Inspector General, A Review Of The FBI's Use Of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006 (Mar. 2008), *available at* http://www.usdoj.gov/oig/special/s0803b/final.pdf [hereinafter 2008 NSL Report]; Dep't Of Justice, Office Of Inspector General, A Review Of The FBI's Use Of Section 215 Orders for Business Records in 2006 (Mar. 2008), *available at* http://www.usdoj.gov/oig/special/s0803a/final.pdf [hereinafter 2008 Section 215 Report].

27 2008 NSL Report, *supra* note 26, at 9.

28 2008 NSL Report, *supra* note 26, at 127, 129 n.116.

29 2008 NSL Report, *supra* note 26, at 127.

30 2008 NSL Report, *supra* note 26, at 127.

31 2008 NSL Report, *supra* note 26, at 130.

32 *See Doe v. Ashcroft*, 334 F.Supp. 2d 471 (S.D.N.Y 2004); *Doe v. Gonzales*, 500 F.Supp. 2d 379 (S.D.N.Y. 2007); *Doe v. Gonzales*, 386 F.Supp. 2d 66 (D.Conn. 2005); PIRA, Pub. L. No. 109-177, 120 Stat. 195 (2006); USA Patriot Act Additional Reauthorizing Amendments Act of 2006 (ARAA) Pub. L. No.109-178, 120 Stat. 278 (2006). The ACLU is still litigating the constitutionality of the gag order provisions in the USA PATRIOT Improvement and Reauthorization Act of 2005. *See* Press Release, American Civil Liberties Union, ACLU Asks Appeals Court to Affirm Striking Down Patriot Act 'National Security Letter' Provision (Mar. 14, 2008) (on file with author), *available at* http://www.aclu.org/safefree/nationalsecurityletters/34480prs20080314.html.

33 2008 NSL Report, *supra* note 26, at 11, 124.

34 2008 NSL Report, *supra* note 26, at 127.

35 2008 NSL Report, *supra* note 26, at 81, 88.

36 Letter from Brian Benczkowski, Principal Deputy Assistant Attorney General, United States Department of Justice, to Nancy

Pelosi, Speaker, United States House of Representatives (Apr. 30, 2008) (on file with author), *available at* http://www.fas.org/irp/agency/doj/fisa/2007rept.pdf.

37 2008 Section 215 Report, *supra* note 26, at 68.

38 2008 Section 215 Report, *supra* note 26, at 72.

39 2008 Section 215 Report, *supra* note 26, at 73.

40 2008 Section 215 Report, *supra* note 26, at 67.

41 2008 Section 215 Report, *supra* note 26, at 72.

42 2008 Section 215 Report, *supra* note 26, at 72.

43 2008 Section 215 Report, *supra* note 26, at 71 n.63.

44 2008 Section 215 Report, *supra* note 26, at 73.

45 2008 Section 215 Report, *supra* note 26, at 72-73.

46 2008 Section 215 Report, *supra* note 26, at 43.

47 2008 Section 215 Report, *supra* note 26, at 45-47.

48 2008 Section 215 Report, *supra* note 26, at 47.

49 *See, Foreign Intelligence Surveillance Act: Closed Hearing Before the H. Permanent Select Comm. on Intelligence*, 110th Cong. (Sept. 6, 2007) (Statement of Kenneth Wainstein, Assistant Attorney General, National Security Division, U.S. Dep't of Justice), *available at* http://www.fas.org/irp/congress/2007_hr/090607wainstein.pdf.

50 *See Doe v. Ashcroft*, 334 F.Supp. 2d 471 (S.D.N.Y 2004); *Doe v. Gonzales*, 500 F.Supp. 2d 379 (S.D.N.Y. 2007); *Doe v. Gonzales*, 386 F. Supp. 2d 66 (D.Conn. 2005). The ACLU is still litigating the constitutionality of the gag order provisions in the USA PATRIOT Improvement and Reauthorization Act of 2005. *See*, Press Release, American Civil Liberties Union, ACLU Asks Appeals Court to Affirm Striking Down Patriot Act 'National Security Letter' Provision (Mar. 14, 2008) (on file with author), *available at* http://www.aclu.org/safefree/nationalsecurityletters/34480prs20080314.html.

51 PIRA, *supra* note 17.

52 *Doe v. Gonzales*, 500 F.Supp.2d 379, 25 A.L.R. Fed. 2d 775 (S.D.N.Y. 2007).

53 *Doe v. Mukasey*, No. 07-4943-cv (2nd Cir. Dec. 15, 2008), *available at* http://www.aclu.org/pdfs/safefree/doevmukasey_decision.pdf.

54 *Library Connection v. Gonzales*, 386 F.Supp.2d 66, 75 (D.Conn. 2005).

55 *See* Joint Administrative Motion to Unseal Case, Internet Archive v. Mukasey, No. 07-6346-CW (N.D. Cal May 1, 2008), *available at* https://www.aclu.org/pdfs/safefree/internetarchive_motiontounseal_20080501.pdf.

56 *Id.* at 3.

57 National Security Act of 1947, 50 U.S.C. §436.

58 Right to Financial Privacy Act, 12 U.S.C. §4314.

59 Fair Credit Reporting Act, 15 U.S.C. §1681v.

60 *See* National Security Act of 1947, 50 U.S.C. §436; Right to Financial Privacy Act, 12 U.S.C. §4314; Fair Credit Reporting Act, 15 U.S.C. §1681v; and PIRA, Pub. L. No. 109-177, §116, 120 Stat. 192 (2006), codified at 18 U.S.C. §2709.

61 Pub. L. No. 104-132, 110 Stat. 1214 (1996).

62 § 2339A. Providing material support to terrorists

(a) Offense. – Whoever provides material support or resources or conceals or disguises the nature, location, source, or ownership of material support or resources, knowing or intending that they are to be used in preparation for, or in carrying out, a violation of section 32, 37, 81, 175, 229, 351, 831, 842(m) or (n), 844(f) or (i), 930(c), 956, 1114, 1116, 1203, 1361, 1362, 1363, 1366, 1751, 1992, 1993, 2155, 2156, 2280, 2281, 2332, 2332a, 2332b, 2332f, or 2340A of this title, section 236 of the Atomic Energy Act of 1954 (42 U.S.C. 2284), or section 46502 or 60123(b) of title 49, or in preparation for, or in

carrying out, the concealment of an escape from the commission of any such violation, or attempts or conspires to do such an act, shall be fined under this title, imprisoned not more than 15 years, or both, and, if the death of any person results, shall be imprisoned for any term of years or for life.

(b) Definition. – In this section, the term "material support or resources" means currency or monetary instruments or financial securities, financial services, lodging, training, expert advice or assistance, safehouses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel, transportation, and other physical assets, except medicine or religious materials.

§ 2339B. Providing material support or resources to designated foreign terrorist organizations

(a) Prohibited activities. –

(1) Unlawful conduct. – Whoever, within the United States or subject to the jurisdiction of the United States, knowingly provides material support or resources to a foreign terrorist organization, or attempts or conspires to do so, shall be fined under this title or imprisoned not more than 15 years, or both, and, if the death of any person results, shall be imprisoned for any term of years or for life. . . .

(g) Definitions. – As used in this section . . .

(4) the term "material support or resources" has the same meaning as in section 2339A; . . .

(6) the term "terrorist organization" means an organization designated as a terrorist organization under section 219 of the Immigration and Nationality Act.

63 66 Stat. 163, § 219, as amended, 8 U.S.C.A. §§ 1101 et seq. As noted, 18 U.S.C. §§ 2339A and 2339B are not the only statutes pertaining to material support. In addition, the criminal liability provisions of the International Emergency Economic Powers Act (IEEPA), permit the designation of "specially designated terrorists" and "specially designated global terrorists" and give the President authority to regulate, prohibit or prevent any form of economic transaction that provides services to benefit terrorists. 50 U.S.C.A. § 1705 (2007).

64 PATRIOT Act, *supra* note 1, at §805(a)(2); 18 U.S.C. §§ 2339A(b) and 2339B(g)(4).

65 IRTPA, Pub. L. No. 108-458, 118 Stat. 3638 (2004).

66 *See Humanitarian Law Project v. Gonzales*, 380 FSupp.2d. 1134, 1142-48, (C.D.Cal 2005).

67 *See* Brief for American Civil Liberties Union as Amicus Curiae Supporting Plaintiffs-Appellees, HLP v. Gonzales, No. 05-56753, 05-56846 (9th Cir. filed May 19, 2006), *available at* http://www.aclu.org/images/general/asset_upload_file394_25628.pdf.

68 *Implementation of the USA Patriot Act: Prohibition of Material Support Under Sections 805 of the USA Patriot Act and 6603 of the Intelligence Reform and Terrorism Prevention Act of 2004: Hearing Before the H. Subcomm. on Crime, Terrorism and Homeland Security of the H. Comm. on the Judiciary*, 109th Cong. 23-28 (2005) (Written statement of Ahilan T. Arulanantham, Staff Attorney, ACLU of Southern California), *available at* http://www.aclu.org/safefree/general/17536leg20050510.html; *See also*, Ahilan T. Arulanantham, A Hungry Child Knows No Politics: A Proposal for Reform of the Laws Governing Humanitarian Relief and 'Material Support' of Terrorism, American Constitution Society (June 2008), *available at* http://www.acslaw.org/files/Arulanantham%20Issue%20Brief.pdf.

69 *Implementation of the USA Patriot Act: Prohibition of Material Support Under Sections 805 of the USA Patriot Act and 6603 of the Intelligence Reform and Terrorism Prevention Act of 2004: Hearing Before the H. Subcomm. on Crime, Terrorism and Homeland Security of the H. Comm. on the Judiciary*, 109th Cong. 26 (2005) (Written statement of Ahilan T. Arulanantham, Staff Attorney, ACLU of Southern California).

70 PIRA, *supra* note 17, at §104.

71 *Fox v. City of Menlo Park*, 146 F.3d 629, 638 (9th Cir. 1998).

72 Maureen O'Hagan, *A Terrorism Case that went Awry*, SEATTLE TIMES, Nov. 22, 2004, *available at* http://seattletimes.nwsource.com/html/localnews/2002097570_sam22m.html.

73 *See Scales v. United States*, 367 U.S. 203, 224-25 (1961).

74 *United States v. Al-Arian*, 308 F.Supp. 2d 1322, 1337 (M.D.Fl 2004).

75 Robert M. Chesney, *Federal Prosecution of Terrorism-Related Offenses: Conviction and Sentencing Data of the "Soft-Sentence" and "Data-Reliability" Critiques*, 11 LEWIS & CLARK L. REV. 837 (2007).

76 BUREAU OF JUSTICE STATISTICS, COMPENDIUM OF FEDERAL JUSTICE STATISTICS, 2001, U.S. DEPARTMENT OF JUSTICE OFFICE OF JUSTICE PROGRAMS (Nov. 2003), BUREAU OF JUSTICE STATISTICS, COMPENDIUM OF FEDERAL JUSTICE STATISTICS, 2002, U.S. DEPARTMENT OF JUSTICE OFFICE OF JUSTICE PROGRAMS (Sept. 2004), BUREAU OF JUSTICE STATISTICS, COMPENDIUM OF FEDERAL JUSTICE STATISTICS, 2003, U.S. DEPARTMENT OF JUSTICE OFFICE OF JUSTICE PROGRAMS (undated), BUREAU OF JUSTICE STATISTICS, COMPENDIUM OF FEDERAL JUSTICE STATISTICS, 2004, U.S. DEPARTMENT OF JUSTICE OFFICE OF JUSTICE PROGRAMS (Dec. 2006), http://fjsrc.urban.org/fjs.cfm?p=pubs_ann_rpt&t=h&a=compendium.

77 Chesney, *supra* note 75, at 885.

78 Chesney, *supra* note 75, at 886.

79 The ACLU filed an *amicus curiae* brief on behalf of Plaintiffs. *See* Brief for American Civil Liberties Union as Amicus Curiae Supporting Plaintiffs-Appellees, Humanitarian Law Project v. Gonzales, No. 05-56753, 05-56846 (9th Cir. filed May 19, 2006), *available at* http://www.aclu.org/images/general/asset_upload_file394_25628.pdf.

80 *Humanitarian Law Project v. Mukasey*, 509 F.3d 1122 (9th Cir. 2007).

81 PATRIOT Act, *supra* note 1, at §411, codified at 8 U.S.C. §1182(a)(3)(B)(i)(VI).

82 PATRIOT Act, *supra* note 1, at §411, codified at 8 U.S.C. §1182(a)(3)(B)(i)(VI).

83 *American Academy of Religion v. Chertoff*, No. 06 CV 588(PAC), 2007 WL 4527504 (S.D.N.Y.).

84 *See American Academy of Religion v. Chertoff*, 463 F.Supp.2d 400 (S.D.N.Y. Jun. 23, 2006); *American Academy of Religion v. Chertoff*, No. 06 CV 588(PAC), 2007 WL 4527504 (S.D.N.Y.).

85 *See* REAL ID Act, Pub. L. No. 109-13, Div. B, 119 Stat. 231 (May 11, 2005).

86 PATRIOT Act, *supra* note 1, at §218.

87 PATRIOT Act, *supra* note 1, at §218.

88 *Mayfield v. U.S.*, 504 F.Supp.2d 1023 (D.Or. Sep 26, 2007). The ACLU filed an *amicus curiae* brief on behalf of Plaintiffs. *See* brief for American Civil Liberties Union as Amicus Curiae Supporting Plaintiffs, Mayfield v. U.S., No. 07-35865 (9th Cir. filed March 14, 2008), *available at* http://www.aclu.org/images/asset_upload_file16_34495.pdf.

89 Eric Lichtblau, *Ashcroft Mocks Librarians and Others Who Oppose Parts of Counterterrorism Law*, N.Y. TIMES, Sept. 16, 2003, available at http://query.nytimes.com/gst/fullpage.html?res=9D00E4D8163AF935A2575AC0A9659C8B63.

Mr. SENSENBRENNER. Also without objection, all Members will have 5 legislative days to submit any additional materials for inclusion in the record, and without objection, the hearing is adjourned.

[Whereupon, at 3:54 p.m., the Subcommittee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Prepared Statement of the Honorable Henry C. "Hank" Johnson, Jr., a Representative in Congress from the State of Georgia, and Member, Subcommittee on Crime, Terrorism, and Homeland Security

Mr. Chairman, on October 26, 2001, in a time of fear and uncertainty that followed the terrorist attacks of September 11, 2001, President George W. Bush signed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, commonly referred to as the PATRIOT Act, into law.

The PATRIOT Act is one of the most controversial laws to date. It was more than 300 pages long and was passed a little over a month after the September 11th attacks.

I am not down-playing the significance of the September 11th attacks; it was the worst terrorist attack in American history.

While the threat of terrorism is real, and law enforcement must have the right tools to protect Americans, any counterterrorism measures must have a solid Constitutional footing and respect the privacy and civil liberties of the American people.

The framers of the Constitution recognized the inherent danger of giving the government unbridled authority to look into our private lives and put checks and balances in place to curb government abuses.

As we started off the 112th Session, my colleagues on the other side of the aisle demonstrated their commitment to the Constitution by reading it on the House floor.

Surely, they are familiar with the Fourth Amendment which states "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

The provisions of the PATRIOT Act that will sunset on May 27, 2011 are disconcerting and expand the government's authority to meddle in our lives with little or no evidence of illegal conduct.

Section 215 of the PATRIOT Act allows the government to seize "any tangible thing," from an American who has not been suspected of terrorism, including library records and diaries, relevant to a terrorism investigation, even if there was no showing that the "thing" pertains to suspected terrorists or terrorist activities.

Section 206 of the PATRIOT Act, commonly referred to as the "roving wiretap" provision, is less controversial. Roving wiretaps are commonly used by law enforcement and it is reasonable to make it available to intelligence officers. Under the Foreign Intelligence Surveillance Act ("FISA"), "John Doe" wiretaps that do not specify the person's identity are allowed. This standard could be tightened to decrease the likelihood that the wrong person will be targeted.

Finally, Section 6001 of the Intelligence Reform and Terrorism Prevention Act of 2004 ("IRTPA"), also known as the "lone wolf" provision, permits secret service intelligence surveillance of non-U.S. persons suspected of being involved in terrorist activities even if they are not connected to any overseas terrorist group. Because the "lone wolf" provision operates in secret, it could be subject to government abuses. To date, this provision has never been used.

There is bipartisan consensus, evidenced by the 26 Republican Members who voted against reauthorization of the expiring provisions of the PATRIOT Act on February 17th, that they need improvement to preserve the rights of the American people.

If Congress reauthorizes these provisions again with no changes, Americans merely visiting a website, mentioning a matter under investigation on social networks,

or checking out a "controversial" book from a library is enough not only to invade the privacy of law-abiding Americans, but to also do so without any of them knowing that the Feds are watching.

One of the most difficult tasks for Congress is balancing the nation's need for security against Americans' rights to privacy, but this is a duty that should not be ignored.

I look forward to hearing from the witnesses about how we can achieve this goal.

Thank you, Mr. Chairman, and I yield back the balance of my time.

Letter from Debra Burlingame, Co-Founder, and Timothy Killeen, Executive Director, Keep America Safe

KEEP AMERICA SAFE.COM

April 1, 2011

The Honorable Lamar Smith
2409 Rayburn HOB
United States House Of Representatives
Washington, DC 20515

Dear Rep. Smith:

The PATRIOT Act has been an essential tool for law enforcement in defending America and keeping us safe since its passage in 2001. Thanks to the PATRIOT Act, numerous terror plots have been stymied and untold numbers of American lives have been saved. Continued success, however, can only be ensured if the PATRIOT Act is renewed in its entirety. The PATRIOT Act is both constitutional and effective.

America remains a primary target for Al Qaeda and its allies. While the War on Terror rages on, we face the very real danger of another devastating attack. The threat of Al Qaeda-inspired, home-grown terrorism plots are on the rise as the terrorist organization increases its presence on the internet--using videos, internet forums and an on-line magazine--to reach adherents and recruit new followers within the United States. In February, Secretary of Homeland Security Janet Napolitano testified before Congress that the threat level today is as high as it has been since September 11. In March, Denis McDonough, the Deputy National Security Advisor to President Obama, addressed the issue of radicalization within the U.S. in a major speech, bluntly observing, "For a long time, many in the U.S. thought that we were immune from this threat... That was false hope, and false comfort. This threat is real, and it is serious." Last December, Attorney General Eric Holder said the growing number of Americans being radicalized and willing to take up arms against our country "keeps him awake at night."

If the PATRIOT Act had been in effect prior to 9/11, law enforcement agencies would have stood a far greater chance of disrupting the terror attack. The PATRIOT Act has been credited with helping to erode the bureaucratic "wall," which many believe allowed the 9/11 terrorists to succeed undetected, between the law enforcement and intelligence communities. It is imperative that we never again allow ourselves to regress into the pre-9/11 mindset, which is exactly what will happen without a permanent extension of all provisions of the PATRIOT Act.

On behalf of over 75,000 members of Keep America Safe, we urge Congress to permanently extend all provisions of the PATRIOT Act in a timely manner. Failure to do so jeopardizes our national security and the lives of Americans in the future.

Respectfully,

Debra Burlingame
Co-Founder, Keep America Safe

Timothy Killeen
Executive Director, Keep America Safe

1718 M Street, NW, #351 • Washington, DC 20036

Letter from J. Adler, National President,
the Federal Law Enforcement Officers Association (FLEOA)

FEDERAL LAW ENFORCEMENT OFFICERS ASSOCIATION
P.O. Box 326 Lewisberry, PA 17339
www.fleoa.org
(717) 938-2300

Representing Members of:
AGENCY FOR INTERNATIONAL DEVELOPMENT
AGRICULTURE (OIG and FOREST SERVICE)
COMMERCE
Export Enforcement, OLE
& NOAA Fisheries Law Enforcement
DEFENSE
Air Force – OSI
Army – CID
Defense Criminal Investigative Service
Naval Criminal Investigative Service
OSD
EDUCATION – OIG
ENERGY – OIG
ENVIRONMENTAL PROTECTION AGENCY – OIG & OEI
FEDERAL DEPOSIT INSURANCE CORPORATION – OIG
GENERAL SERVICES ADMIN – OIG
HEALTH & HUMAN SERVICES
Food & Drug Administration & OIG
HOMELAND SECURITY
Border Patrol
Coast Guard Investigative Service
Immigration & Customs Enforcement
FORMER AIS Marshal
Federal Emergency Management Agency
Federal Protective Service
US Secret Service
Transportation Security Administration
HOUSING & URBAN DEVELOPMENT – OIG
INTERIOR
Bureau of Indian Affairs
Bureau of Land Management
Fish & Wildlife Service
National Park Service
OIG
U.S. Park Police
JUSTICE
Bureau of Alcohol, Tobacco, Firearms & Explosives
Drug Enforcement Administration
Federal Bureau of Investigation
US Marshals Service
OIG
U.S. Attorney's Offices
LABOR – OIG & Bankruptcy
NATIONAL AERONAUTICS & SPACE ADMIN – OIG
NUCLEAR REGULATORY COMMISSION – OIG
POSTAL SERVICE OIG & Inspector
RAILROAD RETIREMENT BOARD – OIG
SECURITIES & EXCHANGE COMMISSION – OIG
SMALL BUSINESS ADMINISTRATION – OIG
SOCIAL SECURITY ADMINISTRATION – OIG
STATE DEPARTMENT
Bureau of Diplomatic Security & OIG
TRANSPORTATION – OIG
TREASURY
FINCEN & OIG
Internal Revenue Service – CI
TIGTA
U.S. CONFIDENTIAL
Probation, Pretrial & Postal Services
VETERANS AFFAIRS – OIG

NATIONAL OFFICERS
President
JOE ADLER
Executive Vice President
NATHAN CATURA
Vice President – Operations
LARRY CORNE
Vice President – Agency Affairs
CHRIS SCHOFFSTOLL
Vice President – Membership Outreach
JOHN BAMBEY
Vice President – Legislative Affairs
DUNCAN TEMPLETON
Secretary
MARIA TORTA
Treasurer
JAMES OTTINGER
General Counsel Emeritus
RANDOLPH TAHIR
Scholarship Awards Director
SHANNON LAMAY-KEPPERMAN
Public Affairs
Donald Mangolo
Legislative Counsel
Jeff A. Anderson, PLLC

March 8, 2011

The Honorable Lamar Smith
House Committee on the Judiciary
United States House of Representatives
Washington, DC 20515

The Honorable John Conyers, Jr.
Ranking Member
House Committee on the Judiciary
United States House of Representatives
Washington, DC 20515

Dear Chairman Smith and Ranking Member Conyers:

On behalf of the 26,000 members of the Federal Law Enforcement Officers Association (FLEOA), I am prepared to support legislation that seeks to incorporate a long-term solution to the USA PATRIOT Act's problematic reoccurring expiration date. It is of paramount importance to federal law enforcement officers that the online surveillance provisions of the USA PATRIOT Improvement and Reauthorization Act of 2005 continue, are protected from expiring and are not degraded or impeded by any further restrictions of the currently existing authorities. FLEOA is the largest non-partisan, non-profit law enforcement association representing over 26,000 federal law enforcement officers from 65 federal agencies.

FLEOA has the distinct honor of representing the interests of law enforcement officers from the Department of Justice, Department of Homeland Security, Department of State, Department of Defense, Department of Treasury, and a host of other agencies. These officers are the front-line guardians that protect our nation from terrorist and criminal threats. They are the ones that have used the provisions in the USA PATRIOT Act to keep Americans safe under the microscope of strict Agency and judicial oversight that has yet to be cited as "excessive."

The USA PATRIOT Act gave law enforcement 21st Century tools to combat 21st Century crimes. In today's world, terrorist and criminals use the internet, cellular and satellite phones, phishing schemes, social networking and wire transfers to affect their crimes. Prior to the USA PATRIOT Act, law enforcement found itself playing catch up to terrorists' schemes. Today, as has been evidenced by many recently thwarted terrorist plots, federal law enforcement officers can be ahead of violent criminals and better protect the American citizenry. FLEOA sees this act as a crucial tool for law enforcement, and not something that should periodically expire.

Currently, there are a few legislative proposals that have been introduced to extend the provisions of the USA PATRIOT Act. Each would continue to allow roving wiretaps of suspects who change computers or phone numbers to avoid monitoring; tracking of individuals of interest with no known links to terrorist groups; and retrieval of records and other tangible evidence from organizations with a court order. Unfortunately, they only allow for a short-term fix, and do not provide any long-term support for federal law enforcement officers.

Crime and terrorism will not "sunset" and terrorists don't need any "extension" to continue their heinous activities. Just like handcuff's, this tool should be a permanent part of the law enforcement arsenal. Arguments to the contrary are flawed and don't recognize the reality that the Act has been judiciously used and has kept American's safe. The Department of Justice's, Office of Inspector General and the Inspectors General within the Intelligence community, are staffed by dedicated Special Agents who are capable of investigating any allegations of abuse. With their professional oversight, there is no need for a short-term expiration date.

As you move forward to a reauthorization of the act, we strongly encourage you to pay close attention to any amendments to law that might impede or degrade the ability of law enforcement officers to act as swiftly as possible. It is imperative to the effectiveness of law enforcement's ability to protect our communities that they have timely and broad access to information and the ability to put that information to use as they deploy.

Those of us in law enforcement are well aware of the crucial importance of the first three hours after a kidnapping. Whether or not the victim survives often depends on the actions of responding and investigating officers during these crucial first three hours. Our society has seen fit, based on the nature of that crime and the exigent circumstances involved, to granting special authorities and allowances to investigating officers when responding to a kidnapping. We urge you to view the investigation of terrorist acts in the same light and not to place any further burdens on our Federal Law Enforcement Officers while they conduct these extremely important, dangerous, and time sensitive investigations.

We thank you for your continued efforts to resolve issues surrounding this important reauthorization and we stand ready to offer any support you should need.

Respectfully yours,

Jon Adler

J. Adler
National President

Letter from Konrad Motyka, President,
the Federal Bureau of Investigation Agents Association

Federal Bureau of Investigation
Agents Association

March 16, 2011

The Honorable Lamar Smith
House Committee on the Judiciary
United States House of Representatives
Washington, DC 20515

The Honorable John Conyers, Jr.
House Committee on the Judiciary
United States House of Representatives
Washington, DC 20515

Dear Chairman Smith and Ranking Member Conyers:

The FBI Agents Association ("FBIAA") appreciates this opportunity to submit our views on the importance of reauthorizing the expiring provisions of the USA PATRIOT Act ("PATRIOT Act"). The FBIAA is comprised of over 12,000 active duty and retired Agents nationwide and is the only professional association dedicated to advancing the goals of FBI Agents. On behalf of the Special Agents of the FBI, we urge you to permanently reauthorize the provisions of the PATRIOT Act and related laws that will expire on May 27, 2011.

Business Records

The "business records" provision, § 215 of the PATRIOT Act, allows criminal investigators to apply to the U.S. Foreign Intelligence Surveillance Act Court ("FISA Court") for an order requiring the production of business records related to foreign intelligence operations or an investigation of international terrorism. However, no such order can be issued if it concerns an investigation of a U.S. person based solely on that person's exercise of his or her First Amendment rights.

This provision is used in specific and rare circumstances. As described by the Congressional Research Service, the business records tool has been used "sparingly and never to acquire library, bookstores, medical or gun sale records."[1] Despite infrequent use, the ability to access important bank and telephone records early in investigations is critical for criminal investigators, and leaders in the Department of Justice and FBI have called the business records provision a "vital tool in the war on terror."[2]

---

[1] Charles Doyle, Congressional Research Service, USA PATRIOT Act Sunset: A Sketch (June 29, 2005), http://www.fas.org/sgp/crs/intel/RS21704.pdf . *See Also* Edward C. Liu, Congressional Research Service, Amendments to the Foreign Intelligence Surveillance Act (FISA) Set to Expire February 28, 2011 (Feb. 28, 2011).

[2] Letter from James B. Comey, Deputy Attorney General, to The Honorable J. Dennis Hastert, Speaker of the U.S. House of Representatives (July 6, 2004) available at: http://www.justice.gov/dag/readingroom/dag-memo-07062004.pdf

Post Office Box 12650 • Arlington, Virginia 22219
A Non-Governmental Association
(703) 247-2173 Fax (703) 247-2175
E-mail: fbiaa@fbiaa.org www.fbiaa.org

Given that the provision has been used carefully and effectively in investigations of terrorist threats, the FBIAA recommends that Congress reauthorize the provision on a permanent basis without new limitations on its use.

Roving Wiretaps

The "roving wiretap" provision, § 206 of the PATRIOT Act, allows the FISA Court to issue wiretap orders that are not linked to specific phones or computers if the target of the surveillance has demonstrated an intent to evade surveillance.

The ability to obtain orders for roving wiretaps is absolutely essential to contemporary criminal and counterterrorism investigations because criminal networks have become technologically advanced and will often purchase and use many different mobile phones and computers in order to evade wiretap efforts. Law enforcement experts have described the roving wiretap provision as a "very critical measure"[3] that has likely helped detect and prevent numerous terrorist plots, including the plots to bomb multiple synagogues in New York City.

The FBIAA urges Congress to permanently reauthorize the roving wiretap authority and not subject it to further restrictions. The roving wiretap provision is already constrained by the requirements that the FISA Court must find probable cause that the target intends to evade surveillance to issue a wiretap and that minimization procedures are followed regarding the collection, retention, and dissemination of information about U.S. persons. A failure to reauthorize the roving wiretap provision, or encumbering the provision with unnecessary restrictions, would jeopardize the utility of an important investigative tool and could, as Director Mueller has warned, open up a "gap in the law that…sophisticated terrorists or spies could easily exploit."[4]

Lone Wolf Surveillance

The "lone wolf" provision, found in Section 6001 of the Intelligence Reform and Terrorism Prevention Act of 2004, allows the FISA Court to issue surveillance orders targeted at non-U.S. persons who engage in international terrorism or activities in preparation of terrorism. Prior to enactment of the lone wolf provision, the FISA Court could only issue surveillance orders if specific evidence linked the targeted person to a foreign power or entity. This meant that non-U.S. individuals acting alone could not be effectively investigated, even if evidence indicated that they were preparing to engage in international terrorism.

The FBIAA recommends that Congress permanently reauthorize the lone wolf provision because it is a necessary part of combating contemporary terrorist threats. Communication between individual terrorists and foreign governments and/or entities is often very scarce,

---

[3] Cristina Corbin, *Patriot Act Likely Helped Thwart NYC Terror Plot, Experts Say*, May 21, 2009, http://www.foxnews.com/politics/2009/05/21/patriot-act-likely-helped-thwart-nyc-terror-plot-security-experts-say/.

[4] *USA Patriot Act of 2001: Hearing Before the Senate Select Comm. On Intelligence*, 110th Congress (July 9, 2007) (statement of FBI Director Robert Mueller).

precisely because these groups are seeking to evade detection by law enforcement. The lone wolf provision gives law enforcement an important tool to obtain the information necessary to ensure that threats are thwarted before terrorists can act on their plans. Congress should not allow this provision to expire, or place additional restrictions on the provision, as such actions could make it more difficult to investigate and prevent dangerous terrorist threats.

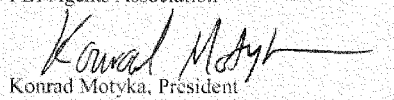
Conclusion

FBI Agents work diligently to detect, investigate, and apprehend individuals and groups that are engaged in a constant and evolving effort to craft and execute plots against the United States and its citizens. These expiring provisions of the PATRIOT Act and similar laws are an important part of the fight against terrorism.

The FBIAA appreciates your consideration of these comments and urges Congress to permanently reauthorize the expiring provisions of the PATRIOT Act without imposing new and unnecessary restrictions on their use.

Very truly yours,

FBI Agents Association



Konrad Motyka, President

○