USA PATRIOT ACT: DISPELLING THE MYTHS

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

MAY 11, 2011

Serial No. 112–32

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

66–314 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
TIM GRIFFIN, Arkansas
TOM MARINO, Pennsylvania
TREY GOWDY, South Carolina
DENNIS ROSS, Florida
SANDY ADAMS, Florida
BEN QUAYLE, Arizona
[Vacant]

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 R. PIERLUISI, Puerto Rico
MIKE QUIGLEY, Illinois
JUDY CHU, California
TED DEUTCH, Florida
LINDA T. SÁNCHEZ, California
[Vacant]

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
SHEILA JACKSON LEE, Texas
MIKE QUIGLEY, Illinois
[Vacant]

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

CONTENTS

MAY 11, 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 3
The Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan, and Ranking Member, Committee on the Judiciary 3

WITNESSES

J. Patrick Rowan, Partner, McGuire Woods LLP
Oral Testimony 11
Prepared Statement 14
The Honorable Bob Barr, a former Representative in Congress from the State of Georgia
Oral Testimony 21
Prepared Statement 23
Bruce Fein, Campaign for Liberty
Oral Testimony 68
Prepared Statement 71
Ed Mullins, President, Sergeants Benevolent Association of New York
Oral Testimony 83
Prepared Statement 86

LETTERS, STATEMENTS, ETC., SUBMITTED FOR THE HEARING

Prepared Statement of the Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan, and Ranking Member, Committee on the Judiciary 7
Article from The New York Times submitted by the Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan, and Ranking Member, Committee on the Judiciary 98
Article from The Washington Post submitted by the Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan, and Ranking Member, Committee on the Judiciary 100

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Prepared Statement of the Honorable Sheila Jackson Lee, a Representative in Congress from the State of Texas, and Member, Subcommittee on Crime, Terrorism, and Homeland Security 117
Article written by Julian Sanchez, Research Fellow, the Cato Institute 126
Letter from John Quinn, President, the Association of State Criminal Investigative Agencies (ASCIA), Director of Criminal Investigation, State of Iowa 158

Page

Letter from Jon Adler, National President, Federal Law Enforcement Officers Association 160
Letter from Ed Mullins, President, Sergeants Benevolent Association of New York City 163
Letter from Lester A. Davis, President, Society of Former Special Agents of the Federal Bureau of Investigation, Inc. 166
Letter from Konrad Motyka, President, Federal Bureau of Investigation Agents Association 168
Letter from Debra Burlingame, Co-Founder, and Timothy Killeen, Executive Director, Keep America Safe 171
Letter from Chuck Canterbury, National President, National Fraternal Order of Police 172
Letter from Doug Gillespie, Sheriff, and President, Major County Sheriffs' Association (MCSA) 173
Letter from James Reams, President, National District Attorneys Association 175
Letter from Steven H. Cook, President, National Association of Assistant United States Attorneys 176

USA PATRIOT ACT: DISPELLING THE MYTHS

WEDNESDAY, MAY 11, 2011

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

The Subcommittee met, pursuant to call, at 10:05 a.m., in room 2141, Rayburn Office Building, the Honorable F. James Sensenbrenner, Jr. (Chairman of the Subcommittee) presiding.

Present: Representatives Sensenbrenner, Gohmert, Goodlatte, Lungren, Chaffetz, Marino, Gowdy, Adams, Quayle, Conyers, Scott, Johnson, Chu, Jackson Lee, and Quigley

Staff present: (Majority) Caroline Lynch, Subcommittee Chief Counsel; Lindsay Hamilton, Clerk; (Minority) Bobby Vassar, Subcommittee Chief Counsel; Sam Sokol, Counsel; Joe Graupensberger, Counsel; and Veronica Eligan, Professional Staff Member.

Mr. SENSENBRENNER. The Subcommittee will come to order, and the Chair recognizes himself for 5 minutes.

Today's hearing is the third the Subcommittee has held in the last 2 months on the USA PATRIOT Act. The first two hearings examined what the expiring provisions and the permanent provisions of the Act authorized the government to do and why they are critical to our national security.

Today's hearing will examine what the government is not authorized to do under these provisions, dispelling the myths and misinformation that has swirled around this law for 10 years.

Let's begin with the "Lone-Wolf" provision. First proposed by Senator Schumer and Kyle in 2002, the provision was added to the FISA definition of agent of a foreign power in the Intelligence Reform and Terrorism Prevention Act of 2004.

Let's be clear. "Lone-Wolf" is simply a definition intended to close a gap in our intelligent laws that allows rogue terrorists to slip through the cracks. It is not a free-standing provision. It does not create a set of surveillance tools different from FISA. It does not allow the government to engage in warrantless surveillance or gather any intelligence without the approval of a FISA court. Only those tools currently laid out in FISA—business records, roving wire taps, and the like—can be used to target a "Lone-Wolf". And the "Lone-Wolf" definition can only be applied to non-U.S. persons, meaning it cannot be applied to citizens or permanent resident aliens.

Similar to the "Lone-Wolf" provision, the roving wire tape authority is not a free-standing provision. It does not authorize warrantless surveillance, nor can roving authority be used to target an entire neighborhood or city block of people. Since 1978, FISA has authorized court-approved surveillance for intelligence gathering purposes.

But gone are the days of landlines and rotary phones. Today's terrorists and spies use disposable cell phones and free e-mail accounts to hide their tracks and to thwart detection. So, in 2001, Congress amended FISA to allow the FISA court to approve roving authority in certain circumstances similar to criminal roving authority that has been in place since 1986.

In order to use a roving wiretap, intelligence agents must first establish, and a FISA court must approve, all of the criteria for a traditional wiretap. These include probable cause that the target of the surveillance is a foreign power or an agent of a foreign power, and probable cause that the devices being used are about to be used by a foreign power or an agent of foreign power. Then the agents must make an additional showing, which the FISA court must also approve, that the actions of the target may have the effect of thwarting their identification. With this authority, agents can monitor modern day terrorists and spies. Without it, agents would have to obtain a new surveillance order from the FISA court every time a target switches cell phones or e-mail accounts and risk losing track of him.

Despite claims to the contrary, roving authority does not create a John Doe warrant. We know that drug dealers and gang members often use nicknames or aliases. It should come as no surprise that terrorists and spies do as well. It should not surprise anyone that it may be difficult or impossible to provide the true identity of those who engage in clandestine underground activities in circumstances in which the identity of a target is unknown and the government may provide a description of the specific target. But it must provide it description specific enough to establish probable cause that the target of the surveillance is a foreign power or an agent of a foreign power.

That leaves us with the business records provision. To begin with, business records orders are not—and I repeat—are not national security letters. PATRIOT Act critics often join the two together in an effort to transfer NSL concerns to business records. National security records are administrative subpoenas; business records are FISA court orders. These orders cannot be used to search a person's home or obtain their personal records. They can only be used to obtain third party records, such as hotel or car rental records.

Perhaps the biggest myth that we just dispel here today is with the death of Osama bin Laden, we no longer need the PATRIOT Act. Nothing could be further from the truth. Just last week, Al-Qaeda released a statement saying it will continue to plan and plot "without any fatigue, boredom, despair, surrender, or indifference." It is clear that Al-Qaeda has not backed down, and neither should we as the United States of America. That's why last week I introduced legislation to permanently reauthorize the "Lone-Wolf" defi-

nition and extend for 6 years the sunsets for roving and business records authority.

It is now my pleasure to recognize for his opening statement the Ranking Member of the Subcommittee, the distinguished gentleman from Virginia, Bobby Scott?

Mr. SCOTT. Thank you, Mr. Chairman.

Today's Subcommittee meets again to discuss the provisions of the USA PATRIOT Act, and I believe it is appropriate that we thoroughly examine these controversial provisions. And I thank you for holding a series of hearings that you have been holding so that we can fully understand exactly what these provisions are.

Each time we allow law enforcement greater power to access private communications or look at records regarding private activities, we give up something important. Piece by piece we may not notice it, but we may wake up one day and ask, where did our freedoms go?

There is no doubt that we entrust our law enforcement officers at all levels with awesome responsibility to protect us from harm. We respect them and thank them for that, and we work on a bipartisan basis to give them the resources and authorities they need. However in protecting us, we must also protect our freedoms and civil liberties, the basic principles of our Bill of Rights underlying what it means to live in a free country, and to define that relationship between citizens and government.

And when we talk about government, it is not government in the abstract. In Northern Virginia, we are talking about people who may be our neighborhoods, lots of other people who may be involved in these activities. So, when we say government, we may be talking about dozens of people, or hundreds of people, who may have access to our private conversations.

For years we've discussed roving wire taps, the "Lone-Wolf" provision, and the relaxed standards for access to business records. These provisions have expanded the government's power to listen to personal conversations, read confidential records, and track private movements. We may establish procedures on how these authorities may be executed and require a secret court to authorize some of these actions, but those subject to the surveillance or those whose records have been examined may never get a chance to know just how much the government, their neighbors, and friends, or other people who may be government employees have intruded into their lives. It is difficult for us to conduct meaningful oversight over provisions which are implemented in such secret conditions.

So, I welcome our witnesses, including one of our former colleagues, a Member of the Subcommittee, the gentleman from Georgia, Mr. Barr, and the other witnesses. I look forward to their testimony.

Mr. SENSENBRENNER. I thank the gentleman from Virginia.

I now recognize the junior Chairman emeritus of the Committee, the distinguished gentleman from Michigan, Mr. Conyers?

Mr. CONYERS. Thank you, Chairman Sensenbrenner. It is a pleasure to be here today and to join Bobby Scott in welcoming Bob Barr, our former colleague from Georgia, for many years here to the Committee room. He also served on the Judiciary Committee, and we know we are all pleased to see him again.

Now, instead of this hearing, which is another oversight hearing, I begin by making the point that we have not had a legislative bill on the PATRIOT Act before the Committee for hearing. We have had a number of oversight hearings, and what we want to do is try to get ready with 16 days left to determine what we are going to do on this bill.

Now, we have been having a hearing on "The USA PATRIOT Act: Dispelling the Myths." Well, that is great, but I think that it shortchanges the real problems with a bill that we have so little time to work on. We ought to be, in my judgment, be working on what compromises we have to make to the PATRIOT Act to get it through the Committee and the House and the conference that is sure to follow. And it is in that spirit that I make this opening statement.

We have got some work to do here. Now, there are a lot of people that are troubled about these expiring provisions. So, to introduce a bill that makes some of them permanent is exactly the wrong way to go. Now, this is the Committee that unanimously passed the first PATRIOT Act because we worked it out on both sides. And I do not think we are following that procedure again the way that we are going now.

And so, I have introduced a compromise measure—H.R. 18-5—that is intended to cover this. And that compromise is a bill to extend the sunset of certain provisions of the USA PATRIOT Act, and that is what I would like all of my colleagues, especially the Chairman of our Judiciary Committee and the Members of this Subcommittee, to examine critically so that we can work out some position that we can reach some accord on.

So, what we are dealing with now is legislation that makes "Lone-Wolf" authority permanent. Well, no hearings, but let us just make it permanent because it is not that bad, all you critics of the PATRIOT Act. If you understood it and listened and read it, you would not feel so bad about it.

It extends the business records and roving wiretaps for 6 years. The majority's bill would make no further improvements to the PATRIOT Act period. It includes no new protections for privacy. It requires no reporting to Congress to the inspector general audits or to any other oversight. And so, I do not feel very supportive of that kind of approach.

And so, thank goodness we will be hearing from some of our witnesses today about the serious issues raised by the 21st century government surveillance plan.

Mr. SENSENBRENNER. Will the gentleman yield?

Mr. CONYERS. Of course I will yield.

Mr. SENSENBRENNER. First of all, I ask that the gentleman be given two additional minutes.

Mr. CONYERS. Thank you.

Mr. SENSENBRENNER. I look back at what happened in 2009, and there was only one oversight hearing that was conducted then. And there was a bill that was introduced, and following that there was a classified hearing that was closed to the public, and the Committee marked it up and sent the bill, you know, off to the floor. I have had a very open process, both when I was the full Committee Chairman in 2001 and 2005, and I believe this year as well

You know, we have heard testimony on the three expiring provisions and what they do, and this was a request for a third open hearing on what the PATRIOT Act does not do. So, I think we certainly have been able to hear all viewpoints on this. And, you know, I will continue to hear all viewpoints on this, but the time for a decision is at hand.

And if the gentleman wants to respond to that, I will be happy, and then we can go on to the witnesses' testimony.

Mr. CONYERS. Well, thank you, Mr. Chairman. What I would like to do is finish my opening statement, and I do not choose to respond to it.

So, what I hope—and I am sorry I did not see my Subcommittee Chairman or my Judiciary Committee Chairman—on the floor yesterday. I was not able to get there because I wanted to alert you to what this discussion was going to be like from my chair today.

So, it is unfortunate, from my point of view, that we have not had more negotiations or discussions that may more quickly lead to a bipartisan compromise. Many Members on both sides of the aisle have serious concerns about the PATRIOT Act, including these three provisions that are about to expire.

While some Members will judge that they cannot support any reauthorization, others may be open to compromise. Indeed, two inform these negotiations, I have introduced, by the bipartisan compromise measure that has been reported out by the Senate Judiciary Committee, and which has the full support of the intelligence community.

Now, at an earlier hearing of this Subcommittee, the Assistant Attorney for National Security and the General Counsel for the Director of National Intelligence, both stated their support for this compromise. Both. General Counsel Bob Lipp said that this was the kind of measure that, "...would provide enhanced protection for civil liberties without affecting operational utility."

Can I have some additional time, Mr. Chairman? I yielded to you.

Mr. SENSENBRENNER. But I did not use the whole 2 minutes. How much additional time does the——

Mr. CONYERS. Well, if you do not want to grant it——

Mr. SENSENBRENNER. How much do you want?

Mr. CONYERS. I want to finish my opening statement.

Mr. SENSENBRENNER. I ask unanimous consent the gentleman be given two additional minutes.

Mr. CONYERS. Well, thank you for your generosity.

What we are doing is trying to make meaningful improvements in important legislation, and what I am proposing in the bill, Chairman Sensenbrenner, is to remove the over broad "presumption of relevance" in Section 215 cases. Instead, require a detailed written statement of the facts and circumstances supporting the request for a Section 215 order in every case.

We also have a provision to offer greater protection to library and book seller records. In addition, we tighten up the use of NSLs and reform the gag orders that were struck down as unconstitutional by the 2nd Circuit Court of Appeals. And finally, it puts in new reporting and audit requirements.

For many, or for some, this bill will not go far enough, but for others it may go too far. For me, the bill represents a reasonable compromise. And with the short time that we all know that we have, and with the need to find a measure that can win the support of the other body and the Administration, I think this bipartisan compromise measure is the proper vehicle for moving this issue forward.

In any event, I appreciate that we are not here today for a legislative hearing. Instead, we are holding another general oversight hearing, this one called "Dispelling the Myths" about the PATRIOT Act. This title, of course, raises a question. If the majority has already concluded the concerns about the PATRIOT Act are myths, then why is the hearing necessary? It seems like they have already made up their mind.

And I will submit the rest of my statement, and thank you, Chairman Sensenbrenner.

[The prepared statement of Mr. Conyers follows:]

Statement of the Honorable John Conyers, Jr,
at a hearing on

"The USA PATRIOT Act: Dispelling the Myths"

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

Room 2141 Rayburn House Office Building
May 11, 2011
10:00 am

In sixteen days, three provisions of the Foreign Intelligence Surveillance Act expire. Under the majority leader's current schedule, the House will be open for legislative business on only six of those days.

The majority has now introduced legislation that would make the Lone Wolf authority permanent, and that extends the business records and roving wiretaps for six years. The majority's bill would make no further improvements to the Patriot Act. It includes no new protections for privacy. It requires no reporting to Congress, Inspector General audits, or any other oversight. I do not support that approach.

We will hear from our witnesses today about the serious issues raised by 21st century government surveillance. Conservative civil libertarians like Bruce Fein and Bob Barr will remind us of the vision of our founders – a free and brave nation that elevates the individual over government.

So I hope that when we consider Chairman Sensenbrenner's bill at markup tomorrow, there will be bipartisan openness to improvements and changes.

Indeed, it is unfortunate in my opinion that we have not had more negotiations or discussions that might have led to a bipartisan compromise. Many members on both sides of the aisle have serious concerns about the Patriot Act, including these three provisions that are set to expire. While some members will judge that they cannot support any re-authorization, others may be open to compromise.

Indeed, to inform these negotiations I have introduced the bipartisan compromise measure that has been reported out by the Senate Judiciary Committee, and which has the full support of the intelligence community.

At an earlier hearing of this Subcommittee, the Assistant Attorney General for National Security and the General Counsel for the Director of National Intelligence both stated their support for this compromise.

ODNI General Counsel Bob Litt said this was the kind of measure that "would provide enhanced protection for civil liberties without affecting operational utility."

The bill is not perfect, but it makes meaningful improvements to the law. For example:

- It removes the overbroad "presumption of relevance" in Section 215 cases. Instead, it requires a detailed written statement of the facts and circumstances supporting the request for a Section 215 order in every case.
- It offers greater protection to library and bookseller records.
- It tightens up the use of NSLs, and reforms the NSL gag orders that were struck down as unconstitutional by the Second Circuit Court of Appeals
- It puts in new reporting and audit requirements.

For many this bill will not go far enough; for others it may go too far. For me, the bill represents a reasonable compromise. With the short time we have – and with the need to find a measure that can win the support of the Senate and the Administration -- I think this bipartisan compromise measure is the proper vehicle for moving this issue forward.

In any event, I appreciate that we are not here today for a legislative hearing. Instead we are holding another general oversight hearing, this one titled "Dispelling the Myths" about the PATRIOT Act. This title of course raises a question – if the majority has already concluded that concerns about the PATRIOT Act are – quote -- "myths," then why is the hearing necessary? It seems like they have already made up their mind.

In any event, I for one do not think that concerns about the PATRIOT Act are fanciful. For one thing, these powers are used in secret and the people whose

phones are tapped or records are seized often never find out. And if they do find out they are often barred by court order from telling anyone. So I question whether it will ever be possible to fully document the impact of these powers on our privacy and civil liberties.

Furthermore, what does it mean to say that these powers have not been abused? The 215 power, for example, is so broad that the issue is not whether it has been misused - the question is whether the permitted uses of it are too broad. The critical question is not whether the rules are being broken, but whether we have the right rules in the first place. As a witness at one of our earlier hearings put it:

> "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."

Now, I expect we will hear today many reasons why these powers are useful to the government.

And no doubt they are. But that is not the question. The Judiciary Committee does not exist to simply rubber stamp the executive's demands for more and more power.

Of course more and more government surveillance can be helpful in fighting terrorism. But as a nation we have chosen a different course. We value freedom and privacy, as well as our physical safety.

So the question is not whether these authorities are helpful. The question is whether they are worth it. Is a nation that gives its government this type of power truly free? That is the question I hope our witnesses will address today.

And with that I thank the Chairman and yield back.

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

And 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.

Patrick Rowan is a partner in McGuire Woods in Washington, D.C., where he practices in the Government, Regulatory, and Criminal Investigations group. Before joining McGuire Woods, he spent 18 years in the Department of Justice serving as an assistant U.S. attorney in Washington, then as acting deputy general counsel for the FBI's national security law branch. And in 2004, he became senior counsel to the assistant attorney general in charge of the criminal division, where he assisted in the management of all counterterrorism investigations.

Excuse me. In 2006, DoJ established the national security division, which consolidated its law enforcement and intelligence activities on counterterrorism and counterintelligence matters. Mr. Rowan served first as the division's principal deputy assistant attorney general, and then as its assistant attorney general.

He received his law degree from the University of Virginia in 1989 and his undergraduate degree from Dartmouth College in 1986.

The Honorable Bob Barr represented the 7th District of Georgia in the U.S. House of Representatives from 1995 to 2003, and was the 2008 Libertarian Party nominee for President of the United States.

He practices law in Atlanta, Georgia, and he is of counsel with the Law Offices of Edwin Marger. He runs a consulting firm, Liberty Strategies, Inc., which is also headquartered in Atlanta, and is a registered mediator and arbitrator.

Mr. Barr was appointed by President Reagan as the United States attorney for the Northern District of Georgia in 1986, and served as president of the Southeastern Legal Foundation from 1990 to 1991. He was an official with the CIA from 1971 to '78, and additionally, he served as an official member of the U.S. delegation at several major United Nations conferences.

He received his law degree from Georgetown University, his master's degree from the George Washington University, and his bachelor's degree from the University of Southern California.

Mr. Bruce Fein is a constitutional lawyer, scholar, and writer. He has served as a visiting scholar for constitutional studies at the Heritage Foundation and adjunct scholar at the American Enterprise Institution, a guest lecturer at the Brooking Institution, and an adjunct professor at the George Washington University in Washington.

He was appointed as research director for the House Republicans on the Joint Congressional Committee on Covert Arms Sales to Iran from 1986 to 1987, and was general counsel of the Federal Communications Commission from 1983 to 1984. From 1981 to 1982, he served as the associate deputy attorney general in the Department of Justice and supervised the Department's litigation and vetting of candidates for the Federal judiciary. From 1975 to '76, he served as the assistant director in the Office of Legal Policy at DoJ, where his primary duties concerned legislative initiatives, aimed at upgrading the administration of Federal justice. Prior to his work in the Office of Legal Policy, he served as special assistant to the assistant attorney general for the Office of Legal Counsel

from 1973 to 1975, then he graduated with honors from Harvard Law School in 1972.

Sergeant Edward D. Mullins has been a member of the New York City Police Department since January 1982. On July 1, 2002, he was elected president of the Sergeant's Benevolent Association of New York City, one of the largest police unions in the Nation with more than 11,000 members.

Early in his career, he was assigned to the 13th Precinct on Manhattan's East Side. After nearly 10 years, he was promoted to detective and assigned to the 10th precinct in Manhattan's Chelsea area. Promoted to sergeant in 1993, he was assigned to the 19th precinct on Manhattan's Upper East Side, and subsequently transferred to the detective bureau in Brooklyn South, where he served as the violent crime supervisor in the 67th Precinct Detective Squad, Special Victim's Squad, and the King's County District Attorney's Office.

He has a bachelor's degree from Concordia College and a master's degree in organizational leadership from Mercy College.

Each witness will be recognized for 5 minutes to summarize their written statement.

And the Chair now recognizes Mr. Rowan for 5 minutes.

Could you turn the PA on and bring the mic a little bit closer to you, and we will reset the clock?

TESTIMONY OF J. PATRICK ROWAN, PARTNER, McGUIRE WOODS LLP

Mr. ROWAN. Thank you. Chairman Sensenbrenner, Ranking Member Scott, and Members of the Subcommittee, thank you for inviting me to testify today.

My name is Patrick Rowan, and I am currently a partner in the law firm of McGuire Woods, but prior to joining the firm in 2009 I worked at the Department of Justice for 18 years, including at the FBI's office of General Counsel, the Criminal Division, and the National Security Division.

During this period I had the opportunity to work with FBI agents and DoJ lawyers who dedicated their days and nights to countering the national security threats that face our country. In this work, the investigative tools drawn from the PATRIOT Act were regularly deployed in the service of our national security.

Even though the provisions of the PATRIOT Act have been repeatedly and successfully used in national security investigations over the last nine and a half years, the Act remains somewhat controversial. While there is great value in the ongoing national dialogue about the balance between national security and liberty, I believe that at least some of the continuing concern about the PATRIOT Act stems from misconceptions that have grown up around the Act. Accordingly, I appreciate the opportunity to appear before this Committee to address some of those misconceptions.

I want to talk specifically about the three provisions that are scheduled to sunset this month—the roving surveillance provision, the business records provision, and the "Lone-Wolf" definition. Each requires the government to make a showing to an independent court—the FISA court. Each provision comes with rule governing how the government handles information regarding

United States persons, and each is subject to extensive executive branch oversight, as well as congressional reporting requirements, all of which is to suggest that they are not particularly susceptible to misuse in any way.

The government's most recent statements indicate that the "Lone-Wolf" definition has never been used, let alone abused. The two other tools which have been used hardly represent radical incursions on civil liberties as these tools were recognized as available for ordinary criminal investigations long before 9/11.

Some apparently believe that the government uses these national security tools to make an end run around the judiciary and the protections that surround our criminal justice system. I think that notion overstates the protections on the criminal side and understate the protections on the national security intelligence gathering side. For example, a FISA business records order is used to obtain the same records that can be acquired with a grand jury subpoena. As a Federal prosecutor, I issued grand jury subpoenas to specific individuals and organizations with virtually no oversight and no meaningful judicial review. Because those records were acquired in the course of a grand jury investigation, the person to whom those records pertained was ordinarily not aware that the government had obtained them. Those records did not necessarily relate directly to the target of the investigation. For example, in a fraud or bribery investigation, it would certainly not be unusual to seek records relating to the target's girlfriend to determine if her activities had some relation to the target's crimes. If the grand jury did not return an indictment or the charged offenses were not connected to the girlfriend's activities, the girlfriend would likely never learn that her records had been subpoenaed.

To employ the FISA business records provision, the government must apply to an independent court and demonstrate relevance in order to obtain a court order under the provision. There are heightened protections when investigators seek materials that are considered especially sensitive, such as medical records and records from libraries.

If the target of the investigation is a U.S. person, the government must show that the investigation is not based solely on activities protected by the First Amendment. Moreover, the government must adhere to minimization procedures that limit the retention and dissemination of the information that is obtained concerning U.S. persons. And the government must also report to Congress on the use of this tool.

To the extent that one assumes that criminal investigative tools are used with greater care because investigators understand that they will eventually have to defend their actions in court, one must keep in mind that national security investigations, intelligence investigations, often result in prosecutions as well. Agents know that even the most sensitive national security investigation may ultimately end up in a U.S. court where the investigative techniques will be scrutinized. This is particularly true when the investigations target a U.S. person. Agents understand that the most obvious and effective tools for neutralizing a U.S. person who threatens our security is a Federal criminal prosecution, and they make deci-

sions about the use of investigative tools with that principle in mind.

Let me talk for a minute about the "Lone-Wolf" definition. The government recently indicated that it has never had occasion to use the "Lone-Wolf" definition, which was contained in the Intelligence Perform Terrorism Prevention Act of 2004. And there are some that argue that the non-use of the definition demonstrates this provision is unnecessary and that it should be allowed to expire. I do not subscribe to this logic. The mere fact that I have never had occasion to use my spare tire does not mean that I would prefer not to have one in my car. The availability of radicalizing material on the Internet seems to be producing more and more individuals who form the intention to carry out violence on their own without the aid and support of a terrorist organization.

These are circumstances for which the "Lone-Wolf" definition was created. If and when the need for the "Lone-Wolf" definition arises, it should be available to the FBI and their partners at NSD. Valuable time and resources might be wasted in trying to engineer our work around for the lapsed definition.

Many of those who are concerned about the PATRIOT Act seems to think that the judges of the FISA court are rubber stamps from the government, that these judges approve everything that there is to approve and impose no meaningful check on the government. From personal experience, I can tell you that simply is not true. And I will be happy to answer further questions about the court and the other provisions that we are here to discuss today later on in the hearing.

Thank you, Chairman.

[The prepared statement of Mr. Rowan follows:]

STATEMENT OF

J. PATRICK ROWAN
PARTNER, MCGUIREWOODS LLP

BEFORE THE

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

HEARING ON: "THE USA PATRIOT ACT: DISPELLING THE MYTHS"

PRESENTED ON

MAY 11, 2011

Chairman Sensenbrenner, Ranking Member Scott, and members of the Subcommittee, thank you for inviting me to testify today. My name is Patrick Rowan, and I am currently a partner in the law firm of McGuireWoods LLP. Prior to joining the firm in 2009, I worked at the Department of Justice (DOJ) for eighteen years. Many of those years were spent as a federal prosecutor, but the last portion of my time at DOJ was spent in positions with national security responsibilities, including at the FBI Office of General Counsel, the Criminal Division and then the National Security Division (NSD).

During this period, I had the opportunity to work with FBI agents and DOJ lawyers who dedicated their days and nights to countering the national security threats that face our country. In this work, the investigative tools drawn from the USA PATRIOT Act (PATRIOT Act) were regularly and responsibly deployed in the service of our national security. Even though the provisions of the PATRIOT Act have been repeatedly and successfully used in national security investigations over the last nine and a half years, the Act remains somewhat controversial. While there is great value in the ongoing national dialogue about the balance between liberty and security, I believe that at least some of the continuing concern about the PATRIOT Act stems from misconceptions that have grown up around the Act.

Accordingly, I appreciate the opportunity to appear before this Committee to address some of these misconceptions. In my remarks I will try to focus most specifically on misconceptions relating to the three provisions of the Foreign Intelligence Surveillance Act ("FISA") that are scheduled to sunset this month: the "roving" surveillance provision, the "business records" provision and the "lone wolf" definition.

There is nothing about these three provisions, Sections 206 (roving) and 215 (business records) of the PATRIOT Act and Section 6001(a) (lone wolf) of the Intelligence Reform and Terrorism Prevention Act, to suggest that they are particularly susceptible to misuse. On the contrary, each of the provisions is subject to substantial protections against civil rights abuses. Each requires the Government to make a showing to an independent court, the FISA court. Each provision comes with rules governing how the Government handles information regarding United States persons. And each is subject to extensive executive branch oversight, as well as congressional reporting requirements.

The Government's most recent statements indicate that the lone wolf definition has never been used, let alone abused. The two other tools, which have been used, hardly represent radical incursions on civil liberties. These tools were recognized as available for ordinary criminal investigations long before 9/11. Law enforcement agencies have had similar roving authority for Title III wiretaps since 1986, and the authority has repeatedly been upheld in the courts. *See, e.g.*, *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). The business records that the government seeks to obtain through a Section 215 order can be

obtained with a garden variety grand jury subpoena in a conventional criminal investigation.

Criminal Investigations Compared With National Security Investigatons

Some apparently believe that the Government uses these national security tools to make an end-run around the judiciary and other forms of oversight that exist on the criminal law enforcement side. I think that notion overstates the protections on the criminal side and understates the protections on the national security side.

For example, as I already noted, a FISA business records order is used to obtain the same records that can be acquired with a grand jury subpoena. As a federal prosecutor, I issued grand jury subpoenas to specific individuals and organizations with virtually no oversight and no meaningful judicial review. The recipient of such a subpoena was required to comply with its demands whenever there was 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." *United States v. R. Enterprises, Inc.*, 498 U.S. 292, 301 (1991).

Because those records were acquired in the course of a grand jury investigation, the person to whom those records pertained was ordinarily not aware that the government had obtained them. Those records did not necessarily relate directly to the target of the investigation. For example, in a fraud or bribery investigation, it would certainly not be unusual to seek records relating to the target's girlfriend to determine if her activities had some relation to the target's crimes. If the grand jury did not return an indictment or the charged offenses were not connected to the girlfriend's activities, the girlfriend would likely never learn that her records had been subpoenaed.

To employ the FISA business records provision, the Government must apply to an independent court and demonstrate relevance in order to obtain a court order under the provision. There are heightened protections when investigators seek materials that are considered especially sensitive, such as medical records and records from libraries or bookstores. If the target of the investigation 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). Moreover, 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 Government must also report to Congress on the use of this tool.

To the extent that one assumes that criminal investigative tools are used with greater care because investigators understand that they will eventually have to defend their actions in a court, one must keep in mind that national security investigations often result in prosecutions as well. Agents know that even the most sensitive national security investigation may ultimately end up in court, where the investigative techniques will be scrutinized. This is particularly true when the investigation targets a U.S. person. Agents understand that the most obvious and effective tool for neutralizing a U.S. person who

threatens our security is a federal criminal prosecution, and they make decisions about the use of investigative tools with that principle in mind.

While there are thousands and thousands of grand jury subpoenas issued every year, the National Security Division recently disclosed that the business records provision is used about forty times per year on average. There is nothing about these numbers that suggests the business records provision is being abused.

The business records provision is not as fast or convenient as a grand jury subpoena. As a result, agents do not ordinarily elect to seek them except in those circumstances in which the secrecy of the investigation is paramount. The business records provision bars the recipient from disclosing it, although the recipient may challenge the non-disclosure requirement in court (as well as the validity of the order).

The secrecy provisions surrounding these authorities are a critical element of their utility. Given the high stakes in national security investigations, it is essential that the investigations be conducted in secret, so that the targets do not adopt countermeasures to avoid detection.

In this regard, the criminal law analogues to our FISA tools – Title III wiretaps, grand jury subpoenas and criminal search warrants – are simply not an acceptable substitute. The procedural requirements imposed by the criminal law, which for Title III wiretaps include mandatory disclosure to the target at the conclusion of the wiretap, make it impossible to conduct long-running intelligence-gathering investigations and increase the likelihood that an investigation will be compromised in the short term.

The Lone Wolf Definition Remains Necessary

The Government recently indicated that it has never had occasion to use the "lone wolf" definition, contained in Section 1801(b)(1)(C) of Title 50 and added in 2004. This provision, which applies only to non-U.S. persons, allows the Government to conduct surveillance and physical search of individuals engaged in international terrorism without demonstrating that they are affiliated with a particular international terrorist group.

There are some who argue that the non-use of the lone wolf definition demonstrates that this provision is unnecessary and that it should be allowed to expire. I don't subscribe to this logic. The mere fact that I have never had occasion to use my spare tire does not mean that I would prefer not to have one in my car. The availability of radicalizing material on the Internet seems to be producing more and more individuals who form the intention to carry out violence on their own, without the aid and support of a terrorist organization. These are the circumstances for which the lone wolf definition was created. If and when the need for the lone wolf definition arises, it should be available to the FBI and their partners at NSD; valuable time and resources might be wasted in trying to engineer a work-around for the lapsed definition.

The FISA Judges Conduct Meaningful Review

Many of those who are concerned about the PATRIOT Act seem to think that the judges of the FISA Court are rubber-stamps for the government, that these judges approve everything that they are asked to approve and impose no meaningful check on the government. From personal experience, I can tell you that this simply is not true.

The judges who sit on the FISA Court are well aware that they only hear the government's side of the story. This is not an unfamiliar posture for any federal judge, because they are regularly called upon to review ex parte requests for search warrants, arrest warrants, and Title III electronic surveillance. They understand that a one-sided recitation of allegations requires extra scrutiny, and the FISA judges bring that understanding with them to the Court.

The judges of the FISA Court conduct a meaningful review of each application that is submitted to them. The judges often require additional information and changes and modifications to the proposed orders. Moreover, the judges regularly require reporting as to whether their orders are being followed. The Government's lawyers and agents understand that the FISA Court expects to hear if its orders have been violated, even if the violation was inadvertent.

The Value of Oversight

Over and above the requirements of the FISA Court, the Executive Branch conducts its own oversight of FISA-related intelligence-gathering activities. Each FISA application is subject to close scrutiny by the FBI and the NSD and must be approved by one of a small number of officials before it is submitted to the FISA Court. The FBI's use of FISA authorities is also subject to oversight by the NSD, the DOJ's Office of Inspector General (OIG) and the Office of the Director of National Intelligence. In addition, Congress receives regular reports and copies of significant FISA Court opinions. Thus, there are a number of entities that seek to ensure that these authorities are used in compliance with the law and in a manner that protects privacy and civil liberties.

These oversight mechanisms have real value, as was demonstrated in connection with the FBI's use of National Security Letters (NSLs). As you know, the PATRIOT Act changed the standard of proof required to use NSLs, permitting their use when the material sought by the NSL is relevant to a national security investigation. This change and others, combined with the changing threat environment, resulted in dramatically expanded use of NSLs by the FBI.

In reauthorizing the PATRIOT Act in 2006, the Congress revised the NSL provisions to permit recipients to challenge the NSLs and their nondisclosure provisions and to require the DOJ's OIG to review the FBI's use of NSLs for potential misuse.

Thereafter, the DOJ's OIG issued a report that was critical of the FBI's use of NSL authorities. A 2007 report exposed a number of problems, including that NSLs were issued out of "control files," rather than from "investigative files," in violation of FBI policy. In his report, the Inspector General explained that "in most – but not all of the cases we examined in this review, the FBI was seeking information that it could have obtained properly through national security letters if it had followed applicable statutes, guidelines, and internal policies. *See* Statement of Glenn A. Fine, Inspector General, U.S. Department of Justice, before the House Judiciary Committee concerning the FBI's Use of National Security Letters and Section 215 Requests for Business Records," (March 20, 2007) at 4. The Inspector General also found that FBI agents had not intentionally sought to misuse NSLs but that the misuses were the product of mistakes, carelessness, confusion, sloppiness, lack of training, lack of guidance, and lack of adequate oversight." *Id.*

In response to this report, the FBI developed an automated process for the issuance of NSLs, to ensure that all applicable legal and administrative requirements are met before the NSL goes out. One of these requirements is review and approval by an FBI attorney. The processing system has also improved the FBI's ability to accurately report NSL use to Congress.

The FBI also tightened its policies regarding the use of NSLs and published comprehensive guidance for agents on their use. Extensive training on the use of NSLs has been conducted at FBI Headquarters and in field offices. The FBI's Inspections Division began conducting NSL audits, and the Bureau established an Office of Integrity and Compliance that aids in assessing compliance with NSL policies and procedures. Finally, lawyers from NSD and the FBI conduct oversight of FBI field offices each year through National Security Reviews ("NSRs"). The NSR teams ordinarily visit 15-20 field offices each year and perform comprehensive reviews of the field office's use of NSLs, among other things.

In a follow-on report before all these improvements were in place, the Inspector General found that the FBI and DOJ had made "significant progress" in implementing recommendations from the 2007 report. Department of Justice Office of Inspector General Report, "A Review of the FBI's Use of National Security Letters: Assessment of NSL Usage in 2006" (March 2008). With the full implementation of the mechanisms outlined above, I have little doubt that compliance has further improved.

I cite this history of NSL flaws and fixes to demonstrate that oversight is meaningful, and problems do get identified and fixed, even when they arise in a secret environment. The Congress, the DOJ and the FBI recognize the value of our national security investigative tools and they take care to police their use of the tools.

Conclusion

In conclusion, I want to thank you for the opportunity to appear before you to discuss the USA PATRIOT Act. The three provisions that are set to expire constitute

important tools for use in a narrow class of national security investigations. I appreciate your desire to identify and strip away any misconceptions that serve to complicate the important task of reviewing their utility. I would be happy to answer any questions that you might have.

Mr. SENSENBRENNER. Thank you very much. The gentleman's time has expired.

Mr. Barr?

TESTIMONY OF THE HONORABLE BOB BARR, A FORMER REPRESENTATIVE IN CONGRESS FROM THE STATE OF GEORGIA

Mr. BARR. Thank you very much, Mr. Chairman and Ranking Member Scott, Chairman Conyers, and Members of the Subcommittee and the Judiciary Committee. It is an honor to be here to discuss an Act that was passed with my vote back in 2001, but, as with many Members on both sides of the aisle who voted for it, not without very serious reservations, which is one of the reasons why we placed in the USA PATRIOT Act at the time a number of sunset provisions. Those were placed in there not simply to provide an opportunity to re-up the provisions regardless of whether they were ever used, whether they were necessary, whether they had been abused, but in order to provide a meaningful mechanism for the Congress of the United States to properly and regularly re-evaluate whether or not these provisions, like any provisions of law, are necessary, need to be limited, need to be expanded perhaps, or are no longer necessary because they have been abused by the executive branch. This is both a very conservative view of government as a well as a very liberal view. It does not apply to one side of the aisle as opposed to the other. In other words, Members on both sides of the aisle should never be afraid to go back and re-evaluate a law that was voted for that they might have voted for in earlier times based on exigent circumstances, so to speak, and the needs of the time, but which, with the passage of time and with evidence that the provisions either have been abused or require additional limitations and restrictions, need to be amended. And if that is indeed the purpose of this hearing, then I commend the Chairman for that and hope that all Members will approach it in that light.

It is very difficult, as this Committee knows, to really get at the issues contained in the PATRIOT Act. There is a feeling or a presumption on the part of the American people that whatever is necessary to protect the national security is okay with them and should be done. Of course, we on the—you on the Judiciary Committee and we as officers of the court and the private arena or sworn law enforcement officers—know that the job of the President is not to do whatever is necessary to protect national security. The job of the President is in his oath, is to protect and defend the Constitution of the United States of America. And that includes what Justice Brandeis said many years ago, and which is as true today as it was back in the 1920's when he penned the words that the right to privacy, which is essentially embodied in the Fourth Amendment, as the basic privacy protection for the people of this country, those who are here lawfully as well as citizens, of this country, is the most basic of right. It is the most important thing to be protected in our Nation. It is, as Ayn Rand said a number of years later in The Fountainhead, the right to privacy is what defines civilization. It defines freedom. And where we have provisions, such as some of these provisions in the PATRIOT Act, as well intended as they are, infringe those rights with no necessary

countervailing requirement in the government that the right to privacy be so suspended.

It is important to go back and place limitations. For example, simply require in these provisions that you all are looking at—Section 215, for example, the business records—provision simply require what the Constitution requires, and that is a reasonable link between the person, be it citizen or other person, lawfully in this country against who the government is seeking information, whether it is tangible things, tangible items, or business records, whatever it is, at least give that person the benefit of requiring the government to show a reasonable connection—some connection to illegal activity, to terrorist activity, to a known or suspected terrorist, or even a known or suspected associate of a terrorist—something that gives that person, whether they ever know about it or not. That is a red herring. It does not matter whether a person knows that their rights have been violated that is the gauge by which we determine whether a provision should be continued in law is constitutional. And it ignores it, a requirement that the citizenry of this country come before the courts or the Congress or the President and document abuses, nor is that the criteria for determining the constitutionality of a particular law. It is whether or not it comports with the intent and the spirit of the Constitution and provision of the law, such as those you are looking at here today and tomorrow and on which the House will shortly vote, violate those basic provisions because they have broken the link between a citizen of this country or a person in this country's right to privacy, and a reasonable suspicion that they may have done something wrong.

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

Mr. BARR. That needs to be restored. Thank you, Mr. Chairman.

[The prepared statement of Mr. Barr follows:]

OFFICE OF BOB BARR
Member of Congress, 1995-2003

TESTIMONY IN OPPOSITION TO SUNSETTED PROVISIONS OF THE USA PATRIOT ACT

BEFORE THE U.S. HOUSE JUDICIARY SUBCOMMITTEE ON CRIME, TERRORISM AND HOMELAND SECURITY

BY

BOB BARR

MAY 11, 2011

OFFICE OF BOB BARR
Member of Congress, 1995-2003

TESTIMONY IN OPPOSITION TO SUNSETTED PROVISIONS OF THE USA PATRIOT ACT

BEFORE THE U.S. HOUSE JUDICIARY SUBCOMMITTEE ON CRIME, TERRORISM AND HOMELAND SECURITY

BY
BOB BARR
MAY 11, 2011

Chairman Sensenbrenner, Ranking Member Scott and members of the Subcommittee, thank you for inviting me to testify on the USA PATRIOT Act, and in particular those provisions set to expire later this month.

From 1995 to 2003, I had the honor to represent Georgia's Seventh District in the United States House of Representatives, serving that entire, eight-year period with many of you on the House Judiciary Committee.

From 1986 to 1990, I served as the United States Attorney for the Northern District of Georgia after being nominated by President Ronald Reagan. Following my tenure as U.S. Attorney, I served as president of the Southeastern Legal Foundation. Earlier, and for much of the 1970s, I served with the Central Intelligence Agency.

I currently serve as CEO and President of Liberty Strategies, Inc. and practice law in Atlanta, Georgia. I am also a member of The Constitution Project's Initiative on Liberty and Security, and an adjunct professor at Atlanta's John Marshall Law School.

I understand the Chairman introduced legislation last week that would make the so-called "lone-wolf" authority in the USA PATRIOT Act permanent; and would extend the Section 215 and roving "John Doe" wiretap authorities in the Act for another six years, until 2017. I urge

this committee to reject this approach tomorrow during its markup, and either amend these sections in order to bring them into full compliance with the letter and the intent of our Constitution, or else allow them to expire.

In the aftermath of 9/11, the government itself has become one of the major threats to the very thing it was designed to protect – our liberty. We have sacrificed our liberty for, at best, perceived security. We have allowed the government to largely render the Fourth Amendment a nullity by way of the PATRIOT Act and warrantless wiretapping programs that empower the government to snoop on its own citizens.

There is a reason why the Founding Fathers – men well-studied in the history of governments – set up our Republic with a system of checks and balances, due process, and federalism. These procedural safeguards are absolutely crucial to securing and defending our rights. Without them, we have a government unaccountable to the people; and one which perceives itself as being above the law. As Michael German, Senior Policy Counsel for the American Civil Liberties Union and himself a former FBI Special Agent, pointed out, "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 is] doing."

Supporting repeal, or at the very least reform, of those provisions of the USA PATRIOT Act set to expire at the end of this month — provisions far too broad and not essential to investigating and thwarting terrorist plots or acts — would be an important signal to this President, that those civil liberties put on hold the past 9-1/2 years, must not be considered permanently frozen. Such a move by this committee will help him hold true to his promises of an open and transparent government.

This reform is absolutely crucial if we do not want to live in a society in which there are essentially no limits on the powers of the government. In a January 2011 report, the Electronic Frontier Foundation (EFF) details possible 40,000 violations of law, Executive Order, or other regulations governing intelligence investigations by the FBI from 2001 to 2008. Though nobody knows the full extent of the abuse, due to the shroud of secrecy surrounding intelligence investigations, this estimate is based on review of nearly 2,500 pages of documents released by the FBI as a result of a Freedom of Information Act suit. I have attached a copy of this EFF report to my written statement.

Many urge that the provisions of the USA PATRIOT Act under consideration for sunset be continued in law unless repeated and serious abuses of these provisions can be conclusively established. With all due respect, this is a red herring. In our system of government, and as clearly reflected in both the body of our Constitution and with even greater clarity in our Bill of Rights, a law is not to be *presumed* constitutional so long as the government does not abuse it (or does not abuse it too seriously). It is *not* up to the citizenry to prove government is abusing a law before that law might be determined to be improper. This is, of course, true *a fortiori* where a law empowers the government to retain a veil of secrecy over its exercise of that law. If a law is contrary to the Fourth Amendment, for example, the law *itself* is the abuse; and the Congress in its oversight role, should not be loathe to step in and correct it; regardless of whether citizens can chronicle abuses of it.

However, as detailed, for example, in the EFF report, there have been abuses of this law.

Today I would like to draw your attention to two sections of the PATRIOT Act in particular. The first is Section 215, also known as the "business records" provision, which is scheduled to expire at the end of this month. This very powerful tool permits the government to obtain any tangible thing, to collect information, on persons not suspected of any wrongdoing.

Section 215 amended what was special authority under FISA (the Foreign Intelligence Surveillance Act) to seize rental car, self-storage and airline records for national security investigations. Prior to the USA PATRIOT Act, the underlying statutes -- 50 U.S.C. §§ 1861, 1862 -- applied only to a limited subset of businesses, and it required a showing of "specific and articulable facts" that *the individual target* was in fact an agent of a foreign power.

Section 215 of the PATRIOT Act removed both of these limitations, thereby greatly expanding the power of the government to reach all "tangible things." This includes books, records, papers, documents and other items; even membership lists of political organizations, gun purchase records, medical records, and genetic information – basically any document, item or record that the government contends is a "tangible thing." It lowers the evidentiary standard below even that of

standard grand jury subpoenas, which are pegged to at least some showing of relevance to criminal activities. Under Section 215, the government is not even required to show that items sought relate to a person under suspicion or investigation. The link between the government invading a person's privacy and a reasonable suspicion of wrongdoing by that person – the foundation of the Fourth Amendment to our Constitution – has been completely severed by this provision.

Congress should amend this section to require a showing to a judge of specific and articulable facts demonstrating that the material sought pertains to a suspected agent of foreign powers. The provision also should include minimization procedures to ensure that the scope of the order is no greater than necessary to accomplish the investigative purpose.

Another section of the PATRIOT Act this sub-committee should address is that relating to National Security Letters (NSLs). NSLs are administrative subpoenas requiring businesses to produce personal communication, financial and credit records, but with no prior judicial approval and with no required nexus to a suspected terrorist. Before the PATRIOT Act, NSLs could only obtain information on suspected agents of foreign powers such as terrorists or spies; but now can be issued to collect information on anyone and to obtain any records the executive branch on its own determines to be "relevant" to an investigation.

Audits conducted by the Justice Department's Inspector General released in 2007 and 2008 have confirmed fears of critics of these provisions: unchecked powers are being used to collect information on innocent U.S. persons, which ultimately is stockpiled in government databases indefinitely, and is accessible by virtually unlimited numbers of law enforcement and intelligence personnel. More than 143,000 NSL requests were issued between 2003 and 2005, and the latest numbers plumbed by the Inspector General (IG) confirm that a majority of NSLs are now being issued about U.S. persons. That data is being stored in government databases, including one containing over 560 million separate records, and another having over 30,000 authorized users.

The reports also document that FBI agents are issuing NSLs for people two or three times removed from a suspected terrorist, even when there is no indication that those people are anything other than innocent links

or share some common element with a known or suspected terrorist or a known associate of a known or suspected terrorist.

The IG also found over 700 instances in which Federal Bureau of Investigation (FBI) agents issued so-called "exigent letters," claiming emergency circumstances and the immediate need for records. According to the reports, agents often lied about the existence of an "emergency," and never followed up with an actual legal request as promised. The NSLs or grand jury subpoenas that could have legally obtained the information never materialized. These exigent letters and sham processes continued even in the face of legal advice from the FBI General Counsel's office to cease.

While the FBI has taken important steps to create more accountability for, and internal checks and balances on NSLs, those changes do not address the fundamental question of whether the FBI should have access to information about people who are not suspected of any criminal wrongdoing or who are not or cannot be linked to terrorists or terrorist organizations. The FBI should not have easy or unfettered access to such information; and only an amendment to the statute can create that meaningful limitation. In fact, the Justice Department and the FBI have testified before this very committee that collecting innocent information is their goal. They claim that they must collect the information first, and sift through it looking for evidence of wrongdoing later; a process that in essence turns the Fourth Amendment on its head.

Congress should exercise its oversight responsibility by requiring that NSLs be used only to obtain information pertaining to suspected terrorists or spies, and by re-establishing the previous, probable cause requirement.

I have concerns also about the other two sections of the PATRIOT Act that you will be voting on tomorrow. The first is the so-called "roving John Doe wiretap," that permits the Foreign Intelligence Surveillance Court to issue wiretap orders to monitor multiple phones or email addresses that specify neither the person to be monitored nor the place to be tapped. This violates the Fourth Amendment's requirement that a warrant state with particularity the things to be searched or seized. This provision should be corrected to require that if the wiretap order does not specify the location of the surveillance, then it must identify the

target, or vice versa, in order to meet constitutional muster. Otherwise, the power should be allowed to sunset.

The other section is the so-called "lone wolf authority" that permits Foreign Intelligence Surveillance Act (FISA) surveillance of non-US persons even if they are not suspected to be connected to a foreign organization, terrorist group or government. This provision eliminated the FISA requirement that surveillance properly be conducted against persons actually suspected of being agents of foreign powers or terrorist organizations. As the Constitution Project has pointed out, "Under FISA, the government can obtain a warrant without a showing of probable cause that a crime is being committed or is about to be committed. FISA's authorization of secret wiretaps and secret home searches in the United States is an exception to traditional Fourth Amendment standards, which has been justified on the basis that these extraordinary surveillance powers are limited to investigations of foreign powers and their agents. By eliminating the requirement to show a connection to any foreign group, the 'lone wolf" provision undermines this justification for the lower FISA standards and raises serious constitutional concerns under the Fourth Amendment."

Considering that the Justice Department told Congress in March that the government has never once relied upon this authority in conjunction with the constitutional issues this provision raises, reauthorization is impossible to justify with a straight face. Persons suspected of terrorist activities would still be reachable and subject to traditional and established criminal law and foreign intelligence gathering standards.

In sum, I urge this subcommittee and the full Judiciary Committee as well, to allow the provisions of the USA PATRIOT Act that are set to sunset at the end of this month to expire; or, at the very least, to reform these provisions and bring them in line with the Constitution lest we allow the exigencies of the day to undermine our liberties.

Though our Constitution and Bill of Rights have taken some hits in the years since 9/11, it is not too late to reset the constitutional clock and roll back excessive, post-9/11 powers. History has shown, as recently as the Waco tragedy in 1993, for example, that government agents and agencies do fall prey to abusing government powers. Another subcommittee of this Judiciary Committee took the lead in 1995 to conduct extensive hearings on those abuses; and the full House refused

in 1996 to grant federal law enforcement many of the expanded powers it asked for, partially in recognition of such abuses.

In many other countries, it is neither acceptable nor lawful to reflect openly on and refine past action. In America, however, it is not only allowable, it is our *obligation* to regularly reexamine decisions made by the federal government; especially perhaps, those enacted during the panic of an event like the terrorist attacks of September 11th 2001. It is an essential responsibility of the Congress to review and reconsider powers previously granted to the Executive branch; to determine whether such authorities remain essential and necessary or whether they have been abused and should be reined in.

Certainly, our (or any) country suffering through the immediate fallout from the worst terrorist attack on American soil ever is liable to make some mistakes in responding legislatively thereto. To err isn't just human; it's a direct result of representative democracy. But also human, is the ability to learn from and *correct* our mistakes.

Case in point: myself. I voted for the USA PATRIOT Act. I did so only after I and a broad coalition of other Members and outside organizations had secured a number of limiting amendments, and only after receiving assurances the Justice Department would use the Act's extensive powers as a limited, if extraordinary measure to meet a specific, extraordinary threat. Little did I or many of my colleagues, know it would shortly be used in contexts other than terrorism, and in conjunction with a wide array of other, privacy-invasive programs and activities.

That I can stand before you and urge the Act's correction should serve as a lesson to other lawmakers who might have voted for the USA PATRIOT Act, and supported similar initiatives. We all should be unafraid to revisit past decisions. Indeed, it is an obligation – not only as members of Congress with delegated oversight responsibilities, but as American citizens with a duty to ourselves and our children to preserve our liberties as the generations before us fought and died to do.

Thank you again for allowing me to testify today.

Attachment

Patterns of Misconduct: FBI Intelligence Violations from 2001 - 2008
A Report Prepared by the Electronic Frontier Foundation
January 2011

Patterns of Misconduct:

FBI Intelligence Violations from 2001 – 2008

A Report Prepared by the Electronic Frontier Foundation

January 2011

ELECTRONIC FRONTIER FOUNDATION

EXECUTIVE SUMMARY

In a review of nearly 2,500 pages of documents released by the Federal Bureau of Investigation as a result of litigation under the Freedom of Information Act, EFF uncovered alarming trends in the Bureau's intelligence investigation practices. The documents consist of reports made by the FBI to the Intelligence Oversight Board of violations committed during intelligence investigations from 2001 to 2008. The documents suggest that FBI intelligence investigations have compromised the civil liberties of American citizens far more frequently, and to a greater extent, than was previously assumed. In particular, EFF's analysis provides new insight into:

Number of Violations Committed by the FBI

- From 2001 to 2008, the FBI reported to the IOB approximately 800 violations of laws, Executive Orders, or other regulations governing intelligence investigations, although this number likely significantly under-represents the number of violations that actually occurred.
- From 2001 to 2008, the FBI investigated, at minimum, 7000 potential violations of laws, Executive Orders, or other regulations governing intelligence investigations.
- Based on the proportion of violations reported to the IOB and the FBI's own statements regarding the number of NSL violations that occurred, the actual number of possible violations that may have occurred in the nine years since 9/11 could approach 40,000 violations of law, Executive Order, or other regulations governing intelligence investigations.[1]

[1] This figure is an estimate based, first, on the fact that a significant number of FBI violations went unreported, both internally and to the IOB; second, this estimate assumes the sample of violations reported to the IOB and released to EFF is representative of all violations that occurred, including those that went unreported; third, the estimate assumes violations occurred at the same rate over time. In the reports released to EFF, roughly 33% were violations of the NSIG, 33% were NSL violations, and 20% were other violations (the remaining violations were too heavily redacted to categorize). The estimate is based on an extrapolation from the OIG's estimate that 6,400 NSL violations occurred from 2003-2006. In the absence

Substantial Delays in the Intelligence Oversight Process

- From 2001 to 2008, both FBI and IOB oversight of intelligence activities was delayed and likely ineffectual; on average, 2.5 years elapsed between a violation's occurrence and its eventual reporting to the IOB.

Type and Frequency of FBI Intelligence Violations

- From 2001 to 2008, of the nearly 800 violations reported to the IOB:
  - over one-third involved FBI violation of rules governing internal oversight of intelligence investigations.
  - nearly one-third involved FBI abuse, misuse, or careless use of the Bureau's National Security Letter authority.
  - almost one-fifth involved an FBI violation of the Constitution, the Foreign Intelligence Surveillance Act, or other laws governing criminal investigations or intelligence gathering activities.

- From 2001 to 2008, in nearly half of all NSL violations, third-parties to whom NSLs were issued — phone companies, internet service providers, financial institutions, and credit agencies —contributed in some way to the FBI's unauthorized receipt of personal information.

- From 2001 to 2008, the FBI engaged in a number of flagrant legal violations, including:
  - submitting false or inaccurate declarations to courts.
  - using improper evidence to obtain federal grand jury subpoenas.
  - accessing password protected documents without a warrant.

For further information on this report, contact Mark Rumold, mark@eff.org, or Jennifer Lynch, jen@eff.org.

---

of robust FBI auditing and thorough oversight, estimates such as these are the only reasonable method to approximate the scope of the FBI's investigatory misconduct.

TABLE OF CONTENTS

INTRODUCTION 1
THE INTELLIGENCE OVERSIGHT BOARD 2
FBI INTELLIGENCE VIOLATIONS REPORTED TO THE IOB 4
Violations of Internal Oversight Guidelines 5
Abuse of National Security Letters 7
Violations of the Constitution, FISA, and Other Legal Authorities 10
TOTAL NUMBER OF VIOLATIONS FROM 2001 TO 2008 11
CONCLUSION 12
Appendix 1—IOB Report 2007-1402 15
Appendix 2—IOB Report 2001-46 17
Appendix 3—IOB Report 2003-25 18
Appendix 4—IOB Report 2006-246 19
Appendix 5—IOB Report 2007-718 20
Appendix 6—IOB Report 2004-80 21
Appendix 7—IOB Report 2007-1209 22
Appendix 8—IOB Report 2002-72 23
Appendix 9—IOB Report 2002-74 24
Appendix 10—IOB Report 2005-03 25
Appendix 11—IOB Report 2007-1693 26
Appendix 12—IOB Report 2006-224 27
Appendix 13—IOB Report 2008-255 28
Appendix 13—IOB Report 2008-255 32

INTRODUCTION

EFF's analysis of recently disclosed documents provides new insights into the Federal Bureau of Investigation's unlawful surveillance of Americans during intelligence investigations conducted between 2001 and 2008.

In response to EFF FOIA requests issued in 2008 and 2009, the FBI released reports of violations made to the Intelligence Oversight Board (IOB) — an independent, civilian intelligence-monitoring board that reports to the President on the legality of foreign and domestic intelligence operations. The nearly 2,500 pages of documents EFF received include FBI reports to the IOB from 2001 to 2008. The reports catalog 768 specific violations arising from FBI monitoring of U.S. citizens, resident aliens, and non-residents.

Following a series of government investigations into FBI intelligence abuses, EFF submitted FOIA requests in an effort to obtain the FBI's IOB reports. In 2007, the Department of Justice, Office of Inspector General released a report documenting the FBI's abuse of its National Security Letter (NSL) authority:[2] the report found, in an audit of only 10% of national security investigations, that the FBI may have committed as many as 3000 NSL violations and had failed to report many of those violations to the IOB.[3] A 2008 OIG report confirmed and expanded the earlier report's findings and critically assessed the steps taken by the FBI to address the abuse of NSLs.[4]

Following the second OIG report in 2008, EFF submitted FOIA requests to eleven federal agencies and agency components requesting all reports of intelligence violations made to the IOB from 2001 to 2008. EFF submitted subsequent requests the following year for violations reported to the IOB from 2008 to 2009. In July 2009, after many agencies failed to respond to the request, EFF filed suit against eight defendants — including the CIA, NSA, Department of Defense, Department of Homeland Security, Department of

[2] DEPARTMENT OF JUSTICE, OFFICE OF THE INSPECTOR GENERAL, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF NATIONAL SECURITY LETTERS (March 2007), *available at* http://www.justice.gov/oig/special/s0703b/final.pdf.

[3] *See* R. Jeffrey Smith, *FBI Violations May Number 3,000, Official Says*, WASH. POST., March 21, 2007, *available at* https://www.washingtonpost.com/wp-dyn/content/article/2007/03/20/AR2007032000921.html.

[4] DEPARTMENT OF JUSTICE, OFFICE OF THE INSPECTOR GENERAL, A REVIEW OF THE FBI'S USE OF NATIONAL SECURITY LETTERS: ASSESSMENT OF CORRECTIVE ACTIONS AND EXAMINATION OF NSL USAGE IN 2006 (March 2008), *available at* http://www.justice.gov/oig/special/s0803b/final.pdf. Even before the OIG's official acknowledgement of FBI investigative abuses, EFF, other civil liberties organizations, and members of the media had documented numerous instances of improper government intelligence activities in the years following 9/11. For example, in 2005, a FOIA request seeking information about violations related to 13 national security investigations revealed numerous instances of FBI misconduct stemming from the Bureau's newly expanded powers under the USA PATRIOT Act.

Justice, Office of the Director of National Intelligence, Department of Energy, and Department of State — demanding the agencies comply with the law and produce the requested documents. In December 2009, the Court ordered the agencies to begin processing EFF's request. In July 2010, two years after EFF's initial FOIA request, the FBI began its release of documents. Over three separate installments in July, August, and October 2010, the FBI released nearly 2,500 pages of documents related to reports of intelligence violations to the IOB.

The documents released to EFF constitute the most complete picture of post-9/11 FBI intelligence abuses available to the public. Among other findings, EFF's analysis of the documents shows that, from 2001 to 2008, significant delays occurred in the reporting of FBI violations to the IOB. The analysis also provides new insights into the type and frequency of violations committed by the Bureau. Most violations fell into one of three broad categories: first, FBI failure to comply with oversight guidelines; second, abuse of the FBI's authority to issue National Security Letters; and, third, the FBI's failure to carry out investigations within the bounds of the Constitution or other federal statutes governing intelligence-gathering. Finally, EFF's analysis concludes that the FBI may have committed as many as 40,000 violations in the 10 years since the attacks of 9/11.

THE INTELLIGENCE OVERSIGHT BOARD

The Intelligence Oversight Board "was created in 1976 by President Ford in response to recommendations made by the Rockefeller Commission calling for a Presidential-level body with specific oversight responsibilities for the legality and propriety of US intelligence activities."[5] The Commission's recommendations came in the wake of a series of congressional reports that revealed illegal and abusive intelligence activities targeting American and foreign citizens. These reports found that intelligence agencies had intercepted and read Americans' mail, performed surveillance on civil rights leaders and other dissidents, and had orchestrated assassination attempts on foreign leaders.

In light of the Commission's recommendation, President Ford established the IOB to provide an independent review of intelligence activities to better safeguard citizens' civil liberties against these types of abusive practices. The IOB consists of five civilian members, all with top-level security clearances, selected by the President to serve on the IOB from the larger intelligence-monitoring body, the President's Intelligence Advisory

[5] President's Intelligence Advisory Board and Intelligence Oversight Board, *PIAB History*, http://www.whitehouse.gov/administration/eop/piab/history.

Board (PIAB).[6] The IOB's mission is to "oversee the Intelligence Community's compliance with the Constitution and all applicable laws, Executive Orders, and Presidential Directives."[7] The IOB must then report to the President those violations the Board believes "may be unlawful or contrary to an Executive Order or presidential directive."[8] Since its creation, the vast majority of the IOB's reports and investigations have remained secret.

Intelligence Oversight Board

- Established in 1976 to oversee US Intelligence Activities
- Created in wake of Congressional reports of abusive practices such as reading Americans' mail, unwarranted surveillance on civil rights leaders, and assassination attempts on foreign leaders
- Role of IOB diminished in wake of 9/11 and many intelligence abuses went unchecked and unreported

Slight modifications to the IOB's authority and structure have occurred since its creation in 1976, but the IOB's oversight capacity remained largely unchanged for nearly 30 years. In the years following the attacks of 9/11, however, the Board's role within the intelligence community was diminished in several ways. First, from 2001 to 2003, President Bush failed to appoint advisers to serve on the IOB.[9] Even when advisers were appointed, however, the IOB continued to provide little real oversight: the IOB did not forward a single instance of intelligence misconduct to the Attorney General until 2006, despite having received notice of several hundred violations.[10] Further, in 2008, President Bush significantly weakened the IOB's oversight capacity by removing its ability to refer violations to the Attorney General for criminal investigation.[11] President Bush also removed the IOB's authority to oversee intelligence agency general counsel and eliminated the requirement for quarterly agency reporting to the IOB.[12]

EFF's analysis of FBI reports to the IOB confirms the perceived inefficacy of the IOB's oversight from 2001 to 2008. Significant delays between violations occurring and their eventual reporting rendered the IOB's oversight capacity entirely impotent. On average, nearly two-and-a-half years passed between the occurrence of an FBI intelligence

---

[6] *Id.*
[7] President's Intelligence Advisory Board and Intelligence Oversight Board, *About the PIAB*, http://www.whitehouse.gov/administration/eop/piab/about.
[8] *See, e.g.*, Exec. Order No. 13462 (Feb. 29, 2008), *available at* http://www.fas.org/irp/offdocs/eo/eo-13462.htm.
[9] John Solomon, *In Intelligence World, a Mute Watchdog*, WASH. POST, Jul. 15, 2007, *available at* https://www.washingtonpost.com/wp-dyn/content/article/2007/07/14/AR2007071400862.html.
[10] *Id.*
[11] Charlie Savage, *President Weakens Espionage Oversight*, BOS. GLOBE, Mar. 14, 2008, *available at* http://www.boston.com/news/nation/washington/articles/2008/03/14/president_weakens_espionage_oversight/?page=full.
[12] *Id.*

violation and its eventual reporting to the IOB. When a violation was reported within the FBI internally, on average, six months still passed before the Bureau reported the violation to the IOB, despite the Bureau's requirement to report IOB violations on a quarterly basis. In light of these significant gaps between the occurrence of a violation and its eventual reporting to the IOB, it seems unlikely that the IOB diligently fulfilled its intelligence oversight responsibilities for most of the past decade.

After taking office, President Obama rolled back some of the Bush Administration's changes to the IOB's authority, but the function and effectiveness of the Board still remains in question. In an October 2009 executive order, President Obama largely reversed the changes made to the IOB's oversight authority, and nine appointments have been made to the larger President's Intelligence Advisory Board.[13] Nevertheless, the White House has not disclosed the composition or membership, if any, of the IOB, which continues to call into question the legitimacy of current intelligence oversight efforts.

FBI INTELLIGENCE VIOLATIONS REPORTED TO THE IOB

As noted above, in EFF's review of nearly 2,500 pages of documents released by the FBI, EFF uncovered alarming trends in the Bureau's intelligence investigation practices from 2001 to 2008. The documents suggest the FBI's intelligence investigations have compromised the civil liberties of American citizens far more frequently, and to a greater extent, than was previously assumed. Broadly, these documents show that the FBI most frequently committed three types of intelligence violations — violations of internal oversight guidelines for conducting investigations; violations stemming from the abuse of National Security Letters; and violations of the Fourth Amendment, Foreign Intelligence

Four Categories of FBI Intelligence Violations

1. Violations of internal oversight guidelines—*over 1/3 of all violations reported*
2. Violations of National Security Letter powers—*almost 1/3 of all violations reported*
3. Violations of the Constitution, FISA and other laws—*1/5 of all violations reported*
4. Remainder—Unclear from redactions

[13] Charlie Savage, *Obama Order Strengthens Spy Oversight*, N.Y. TIMES, Oct. 29, 2009, at A16, *available at* https://www.nytimes.com/2009/10/30/us/politics/30intel.html.

Surveillance Act (FISA), and other laws governing intelligence investigations. Also, based on statements made by government officials and the proportion of violations occurring in the released reports, EFF estimates the FBI may have committed as many as 40,000 intelligence investigation violations over the past ten years.

Violations of Internal Oversight Guidelines

The first category of violation occurring with the most frequency involved the FBI's failure to comply with internal oversight guidelines for conducting investigations. This type of violation ultimately resulted in investigations occurring without any meaningful oversight from either FBI Headquarters or the IOB. Of the reports filed with the IOB, violations of oversight guidelines accounted for over a third of all FBI violations.

When the FBI fails to comply with its own internal guidelines there can be no meaningful oversight.

The Attorney General Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSIG)[14] set forth various reporting rules, investigative requirements, and classification regulations for FBI agents to follow when conducting intelligence investigations.[15] Originally issued in 1976 in the wake of the Church Committee's revelations of frequent and serious FBI violations of citizens' rights, the Guidelines task the Attorney General with ensuring that all government intelligence operations occur with sufficient oversight and within the bounds of the Constitution and other federal laws.[16] For example, the NSIG requires that, upon initiating a new intelligence investigation, an agent report the investigation to FBI Headquarters within a specified period. Other guidelines set requirements for annual reporting of investigations, for information sharing practices between agencies, and — depending on the stage of the investigation and the level of internal authorization — for the investigative techniques FBI agents may use. Broadly, the Guidelines are intended to protect American citizens' constitutional rights from intrusive and overreaching intelligence investigations.

In 2006, Department of Justice Inspector General Glenn Fine reported to Congress on FBI compliance with the Attorney General's Guidelines for Domestic Investigations, a

[14] A previous version of the NSIG, the Attorney General's Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Collection ("FCIG") is referenced in some of the earlier released documents. The NSIG replaced the FCIG in October 2003.
[15] A partially declassified version of the guidelines is available at http://www.fas.org/irp/agency/doj/fbi/nsiguidelines.pdf.
[16] *See* ELECTRONIC PRIVACY INFORMATION CENTER, THE ATTORNEY GENERAL'S GUIDELINES, *available at* http://epic.org/privacy/fbi/.

distinct set of guidelines from the NSIG governing FBI domestic investigations.[17] The OIG investigation revealed "significant non-compliance with the Guidelines."[18] EFF's analysis demonstrates that the FBI's non-compliance extends to the NSIG, as well: the FBI frequently violated its own internal oversight protocols for national security and intelligence investigations. These violations ranged from a failure to submit notification of the investigation of a US person to FBI Headquarters for three years,[19] to a failure to report a violation within 14 days of its discovery,[20] to continuing to investigate a US person when the authority to do so had expired.[21] In all cases involving violations of the NSIG, though, the FBI only reported to the IOB when it determined the agency's ability to supervise the investigation had been "*substantially* impaired."

FBI IOB Report 2007-1402

(b) [redacted] was further required to provide annual summaries of the [redacted] under both the AGG and the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSIG), effective October 31, 2003. This did not occur until March 26, 2007, more than three years after the case was converted to a [redacted]. As such, OGC determined that DIPR's oversight ability was impaired, and reported the matter to the IOB.

(b) Next, in IOB matter 2007-1733, on April 11, 2005,

In a 2005 *Washington Post* article, a senior FBI official dismissed the severity of this type of violation, noting that the "vast majority of the potential [violations] reported have to do with administrative timelines and time frames for renewing orders."[22] But these guidelines are much more than mere "administrative timelines:" the NSIG exists in order to prevent intelligence agencies from invoking "national security" to monitor citizens engaging in constitutionally protected activities — *exactly* the type of monitoring the FBI was engaging in at the time.[23]

Taken together, the FBI's disregard for its own internal oversight requirements and the Bureau's failure to timely report violations to the IOB undermined the safeguards

---

[17] The FBI operates under two separate sets of guidelines issued by the Attorney General: one for domestic investigations, one for national security and intelligence investigations. For a thorough treatment of the gradual expansion of the Attorney General's Domestic Guidelines, *see* EMILY BERMAN, BRENNAN CENTER FOR JUSTICE, DOMESTIC INTELLIGENCE: NEW POWERS, NEW RISKS (Jan. 2011), *available at* http://www.brennancenter.org/content/resource/domestic_intelligence_new_powers_new_risks/.

[18] *Oversight of the Federal Bureau of Investigation: Hearing Before the Sen. Comm. on the Judiciary* (May 2, 2006) (statement of Glenn A. Fine, Inspector General, U.S. Department of Justice), *available at* http://www.justice.gov/oig/testimony/0605.htm.

[19] FBI IOB Report 2007-1402, Appendix 1.

[20] FBI IOB Report 2001-46, Appendix 2.

[21] FBI IOB Report 2003-25, Appendix 3.

[22] Dan Eggen, *FBI Papers Indicate Intelligence Violations*, WASH. POST., Oct. 24, 2005, *available at* https://www.washingtonpost.com/wp-dyn/content/article/2005/10/23/AR2005102301352.html.

[23] *See, e.g.*, DEPARTMENT OF JUSTICE, OFFICE OF THE INSPECTOR GENERAL, A REVIEW OF THE FBI'S INVESTIGATIONS OF CERTAIN DOMESTIC ADVOCACY GROUPS (September 2010), *available at* http://www.justice.gov/oig/special/s1009r.pdf (describing FBI surveillance of various American advocacy groups from 2001 to 2006).

established to protect civil liberties violations from occurring—the precise object of both the NSIG and the IOB.

Abuse of National Security Letters

In the reports disclosed to EFF, the second type of violation occurring with the most frequency involved FBI abuse of National Security Letters. These violations accounted for almost one-third of all reported violations. National Security Letters, or NSLs, are secret administrative subpoenas used by the FBI to obtain records from third-parties without any judicial review.[24] While NSLs have existed since the late-1970s, the USA PATRIOT Act greatly expanded the intelligence community's authority to issue NSLs. During the course of a terrorism or counterintelligence investigation, NSLs can be used to obtain just three types of records: (1) subscriber and "toll billing information" from telephone companies and "electronic communications services;"[25] (2) financial records from banks and other financial institutions;[26] and (3) consumer identifying information and the identity of financial institutions from credit bureaus.[27]

The FBI issued nearly 200,000 NSL requests between 2003-2006.

The FBI's systemic abuse of NSLs has been well-documented — both by Justice Department investigations and through litigation and scrutiny of FBI practices by EFF. As noted above, in reports from 2007 and 2008, the Inspector General found that, between 2003 to 2006, the FBI may have committed as many as 6,400 violations of the FBI's NSL authority.[28] According to the 2008 Report, from 2003 to 2006, the FBI issued nearly 200,000 NSL requests; almost 60% of the 49,425 requests issued in 2006 were for investigations of U.S. citizens or legal aliens.[29]

---

[24] *See* Electronic Frontier Foundation, *National Security Letters*, https://www.eff.org/issues/national-security-letters.

[25] 18 U.S.C. § 2709.

[26] 12 U.S.C. § 3414.

[27] FBI has the authority to issue three different, but related, NSLs to credit agencies — an NSL pursuant to 15U.S.C. § 1681(u)(a) for the names of financial institutions with which the subject has an account; an NSL pursuant to 15 U.S.C. 1681(u)(b) for consumer identifying information; and an NSL pursuant to 15 U.S.C. § 1681(v) for a full credit report. The FBI may only request a full credit report while investigating international terrorism cases.

[28] *See* Jason Ryan, *FBI Search Abuses Could Number Thousands*, ABC NEWS, Apr. 16, 2008, *available at* http://abcnews.go.com/TheLaw/DOJ/story?id=4661216&page=1.

[29] DEPARTMENT OF JUSTICE, OFFICE OF THE INSPECTOR GENERAL, A REVIEW OF THE FBI'S USE OF NATIONAL SECURITY LETTERS: ASSESSMENT OF CORRECTIVE ACTIONS AND EXAMINATION OF NSL USAGE IN 2006 (March 2008), *available at* http://www.justice.gov/oig/special/s0803b/final.pdf.

Earlier scrutiny of FBI practices by EFF also revealed abuses of the Bureau's NSL authority. Documents obtained in a response to a 2007 EFF FOIA request showed that the FBI issued an NSL to North Carolina State University to obtain educational records, in clear violation of the FBI's statutory authority.[30] EFF also filed a lawsuit challenging the legality of an NSL issued by the FBI to the Internet Archive. The government formally withdrew the NSL request in 2008.[31]

Analysis of the FBI's IOB reports released to EFF show that the Bureau committed violations involving NSLs for telephone and electronic communications records twice as often as it did for financial and credit records. While the FBI has publicly disclosed the *total* number of NSLs issued annually,[32] the Bureau has refused to release the frequency with which the three individual types of NSLs issued. However, if the rate at which the FBI's NSL violations occurred is an indicator of the frequency with which the three types of requests were issued, then, on average, the FBI likely issued approximately 25,000 NSL requests for telephone and electronic communications records, 12,500 requests for financial records, and 12,500 requests for credit information annually from 2003 to 2006.

Perhaps most startling, however, was the frequency with which companies receiving NSLs — phone companies, internet providers, banks, or credit bureaus — contributed to the FBI's NSL abuse. In over half of all NSL violations reviewed by EFF, the private entity receiving the NSL either provided more information than requested or turned over information without receiving a valid legal justification from the FBI. Companies were all too willing to comply with the FBI's requests, and — in many cases — the Bureau readily incorporated the over-produced information into its investigatory databases.

> [redacted] [redacted] [redacted] resided at [redacted], who was and remains a "United States person" as that term is used in Section 101(i) of the Foreign Intelligence Surveillance Act of 1978 (FISA). During the course of the investigation, [redacted] issued two NSLs, [redacted] pursuant to the Electronic Communications Privacy Act, 18 U.S.C. § 2709. The subject NSL requested [redacted]
>
> [redacted] in [redacted] responded to the two NSLs by transmitting information responsive to both on a single compact disk (CD). Subsequently [redacted] determined that the CD contained full email content for both accounts. Pursuant to the direction of NSLB, SA [redacted] sealed and sequestered in A1 envelopes the CD, along with all paper copies of its contents.

For example, in a violation reported in 2006, the FBI requested email header information for two email addresses used by a U.S. person.[33] In response, the email service provider

[30] *See* Electronic Frontier Foundation, *Report on the Improper Use of an NSL to NC State University*, https://www.eff.org/issues/foia/report-nsl-ncstate.
[31] *See* Electronic Frontier Foundation, *Internet Archive v. Mukasey*, https://www.eff.org/cases/archive-v-mukasey.
[32] DEPARTMENT OF JUSTICE, OFFICE OF THE INSPECTOR GENERAL, A REVIEW OF THE FBI'S USE OF NATIONAL SECURITY LETTERS: ASSESSMENT OF CORRECTIVE ACTIONS AND EXAMINATION OF NSL USAGE IN 2006 (March 2008), *available at* http://www.justice.gov/oig/special/s0803b/final.pdf.
[33] FBI IOB Report 2006-246, Appendix 4.

returned two CDs containing the full content of all emails in the accounts. The FBI eventually (and properly) sequestered the CDs, notified the email provider of the overproduction, and re-issued an NSL for the originally requested header information; but, in response to the second NSL, the email provider *again* provided the FBI with the full content of all emails in the accounts.

Compounding the service providers' problematic over-disclosure, the scope of the FBI's authority to issue NSLs for electronic transactional records rests on unsettled and unclear legal grounds. The FBI's NSL authority under the Electronic Communications Privacy Act (ECPA) allows the government to issue NSLs to traditional telephone service providers for non-content subscriber information and toll billing records — essentially, the name, address, length of service, and local and long distance call records.[34] ECPA also provides the authority to issue NSLs for "electronic communications transactional records."[35] However, the exact scope of this remains unclear: according to the DOJ, "electronic communications transactional records" include "those categories of information parallel to . . . toll billing records for ordinary telephone service."[36] What, exactly, "those categories of information" constitute — possibly including, for example, email "header" information, IP addresses, URLs, or other information — remains unclear.

Third parties, such as financial institutions or ISPs, responded to NSLs that lacked any legal justification.

Third-parties not only willingly cooperated with FBI NSLs when the legal justification was unclear, however: they responded to NSLs without any legal justification at all. In one instance, when requesting financial records from a bank under the Right to Financial Privacy Act, the FBI used language and statutory citations from ECPA — a statute entirely unrelated to financial records — for its legal authority; nevertheless, the financial institution complied with the FBI's legally deficient request.[37] In another series of violations, the FBI improperly requested and received full credit reports on subjects of counterintelligence investigations.[38] The Fair Credit Reporting Act, the statute providing FBI authority to request credit information using an NSL, however, only provides that authority in terrorism investigations.[39] In other violations, the FBI failed to certify, as

[34] *See* 18 U.S.C. § 2709(a).
[35] *Id.*
[36] *See* Department of Justice, Office of Legal Counsel, Requests for Information under the Electronic Communications Privacy Act (November 2008) at 3 n. 3, *available at* http://www.fas.org/irp/agency/doj/olc/ecpa.pdf.
[37] FBI IOB Report 2007-718, Appendix 5.
[38] FBI IOB Report 2004-80, Appendix 6.
[39] *See* 15 U.S.C. § 1681(v).

required by statute, that the NSL was relevant to a terrorism investigation and not being used to investigate constitutionally protected activities.[40] Again, despite the deficiency of the request, the third-party complied with the FBI's NSL.

The FBI's abuse of its NSL power has garnered much of the attention in the debate over the FBI's abusive intelligence practices. What has *not* received as much attention, however, is the unwillingness of companies and organizations to guard their clients' and users' sensitive, personal information in the face of these NSL requests — whether the request was legally justifiable or not. Undeniably, if the FBI had complied with the law, the vast majority of NSL violations would never have occurred. Nevertheless, many of the businesses and organizations with which Americans trust their most private information are not applying any scrutiny to unjustifiable requests from the FBI and are not responding to valid requests in a responsible manner.

Violations of the Constitution, FISA, and Other Legal Authorities

The third category of FBI intelligence violations reported to the IOB, accounting for almost 20% of all reports, are violations of the Constitution, the Foreign Intelligence Surveillance Act (FISA), and other federal laws governing criminal investigations and intelligence-gathering activities. The first two types of intelligence violations committed by the FBI — violations of the NSIG and NSL abuse — were readily susceptible to categorization: these violations occurred with great frequency, and the violations were often repetitive and largely similar. On the other hand, violations falling into the third category were, in general, unique, and often flagrant, violations of a variety of legal authorities.

Violations falling into this third category were consistently the most brazen and egregious violations. For example, in two separate incidents, the FBI reported to the IOB that its agents had made false statements in written declarations to courts.[41] Another reported violation involved the FBI's use of improper evidence to

FBI IOB Report 2002-74

[redacted] who was a "United States person" as that term is used in Foreign Intelligence Surveillance Act of 1978 (FISA).[1] The declaration provided by the FBI [redacted] for [redacted] of the target provided incorrect information. The declaration referred to a previously installed audio [redacted] of other subjects at the same location and specifically described how the surveillance is being conducted. However, the technology to implement this surveillance was never installed.[2] The inaccurate representations in the declaration submitted [redacted] were material misstatements of fact, contrary to the Executive Order 12333 and [redacted] thus requiring an IOB reporting. [redacted]

[40] FBI IOB Report 2007-1209, Appendix 7.

obtain grand jury subpoenas.[42] Other violations involved FBI's use of a target's username and password to access and download account information[43] and a warrantless search of password-protected files.[44]

Of the reports reviewed by EFF, however, this type of violation was also generally the most redacted. One four-page report (on average, most reports are only one or two paragraphs) is almost entirely redacted, with the exception of one paragraph that notes the "scope of [the FBI agent's] alleged offenses" warranted reporting to the IOB: the three pages detailing the offenses, however, are almost entirely redacted.[45] Moreover, solely from the documents provided to EFF, it is evident that the FBI is withholding information on an inconsistent and arbitrary basis. For example, one IOB report, which details the issuance of NSLs without proper authority in the wake of the attacks on September 11th, was inadvertently included twice in the FBI's document release: one is nearly entirely redacted; the other, almost entirely free from redactions.[46] Numerous documents throughout the FBI's release provide similar evidence of the agency's inconsistent and arbitrary practice of redacting and withholding documents.[47]

While the reports documenting the FBI's abuse of the Constitution, FISA, and other intelligence laws are troubling, EFF's analysis is necessarily incomplete: it is impossible to know the severity of the FBI's legal violations until the Bureau stops concealing its most serious violations behind a wall of arbitrary secrecy.

TOTAL NUMBER OF VIOLATIONS FROM 2001 TO 2008

Both the frequency and type of violations revealed in the FBI's release to EFF are staggering. At a minimum, these documents already demonstrate the need for greater accountability and improved oversight mechanisms for American intelligence agencies. Yet, at the same time, the FBI continues to withhold critical information on the circumstances, rate of occurrence, and severity of these violations. And, if past experience is any guide, it is likely that the FBI is either withholding or failing to report many violations altogether.

---

[41] FBI IOB Report 2002-72, Appendix 8; FBI IOB Report 2002-74, Appendix 9.
[42] FBI IOB Report 2005-03, Appendix 10.
[43] FBI IOB Report 2007-1693, Appendix 11.
[44] FBI IOB Report 2006-224, Appendix 12.
[45] FBI IOB Report 2008-255, Appendix 13.
[46] FBI IOB Report 2001-69, Appendix 14.
[47] *See* Jennifer Lynch, *FBI Arbitrarily Covers up Evidence of Misconduct: Is this the Transparency Obama Promised?*, Electronic Frontier Foundation Deeplinks, *available at* https://www.eff.org/deeplinks/2010/12/fbi-arbitrarily-covers-evidence-misconduct.

In the absence of robust auditing and full disclosure from the Bureau, the only method for approximating the scope of the FBI's abusive intelligence practices is to extrapolate from information contained within these releases and public statements made by government officials. The IOB reports, themselves, provide some insight into the sheer number of FBI intelligence violations. In previous litigation, EFF fought the FBI to release the IOB matter numbers that accompany every IOB report. While not every IOB "matter" is ultimately reported to the IOB, the numbers provide some indication of the number of violations investigated by the FBI. Based on IOB matter numbers on the reports released to EFF, it is clear that, at minimum, the FBI investigated approximately 7,000 instances of alleged misconduct from 2001 to 2008.

The number of FBI intelligence violations since 9/11 could approach 40,000.

The actual number of violations that occurred from 2001 to 2008, however, is likely much higher. The Inspector General has acknowledged that as many as 6,400 potential NSL violations may have occurred between 2003-2006;[48] if the proportion of violations released to EFF is representative of all FBI intelligence violations during that time period, then the number of *total* violations during that four year time-period may have topped 17,000 — or an average of 4,250 serious intelligence violations per year. In the nine years since 2001, EFF estimates that total could approach 40,000 possible violations.[49]

CONCLUSION

From 2001 to 2008, the FBI frequently and flagrantly violated laws intended to check abusive intelligence investigations of American citizens. While many believed the era of abusive FBI practices would end with the Bush Administration, there is little evidence that President Obama has taken significant measures to change past FBI practices. Two years into his term, the President has not publicly disclosed any appointments to the IOB,

[48] *See* Jason Ryan, *FBI Search Abuses Could Number Thousands*, ABC NEWS, Apr. 16, 2008, *available at* http://abcnews.go.com/TheLaw/DOJ/story?id=4661216&page=1.

[49] This figure is an estimate based, first, on the fact that a significant number of FBI violations went unreported, both internally and to the IOB; second, this estimate assumes the sample of violations reported to the IOB and released to EFF is representative of all violations that occurred, including those that went unreported; third, the estimate assumes violations occurred at the same rate over time. In the reports released to EFF, roughly 33% were violations of the NSIG, 33% were NSL violations, and 20% were other violations (the remaining violations were too heavily redacted to categorize). The estimate is based on an extrapolation from the OIG's estimate that 6,400 NSL violations occurred from 2003-2006. In the absence of robust FBI auditing and thorough oversight, however, estimates are the only reasonable method to approximate the scope of the FBI's investigatory misconduct.

and his campaign promise of unprecedented transparency within the executive branch has gone largely unfulfilled — especially within the intelligence community.

Congress, however, has an opportunity to remedy these abuses: portions of the USA PATRIOT Act expire in late February, and a bill has already been introduced in the House of Representatives to reauthorize it. Instead of simply rubber-stamping the intelligence community's continuing abuse of American's civil liberties, Congress should seize this opportunity to investigate the practices of the FBI and other intelligence agencies, and to demand greater accountability, disclosure, and reporting from these agencies. Until then, the FBI's pattern of misconduct will continue.

For further information on this Report, contact Mark Rumold, mark@eff.org, or Jennifer Lynch, jen@eff.org.

Appendix:
IOB Reports

Appendix 1—IOB Report 2007-1402

U.S. Department of Justice

Federal Bureau of Investigation

~~SECRET~~

Office of the General Counsel

Washington, D.C. 20535

June 3, 2008

VIA SECURE FACSIMILE
AND U.S. MAIL

COPY

Homer S. Pointer, Counsel
Intelligence Oversight Board
Room 5020
New Executive Office Building
725 17th Street, N.W.
Washington, D.C. 20503
Secure Facsimile: [redacted]

Dear Mr. Pointer:

(U) This letter is in response to your request that the Federal Bureau of Investigation, Office of the General Counsel (OGC), clarify three of its recent reports to the Intelligence Oversight Board and the Office of the Director of National Intelligence. The three matters to which you seek clarification are: 2007-1402; 2007-1733; and 2007-2160.

(U) ~~(S)~~ In 2007-1402, the [redacted] Field Office opened a [redacted] of a United States person on [redacted] The [redacted] was extended on [redacted] and converted to a [redacted] on [redacted] No notification of this investigation was provided to FBI Headquarters (FBIHQ) until [redacted]

(U) ~~(S)~~ [redacted] of the Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations (AGG), effective March 8, 1999. However, once the investigation was

(U) Derived From : FBI NSISCG 20080301
Declassify On: 06/03/2018

~~SECRET~~

DECLASSIFIED BY 45170MR/plj
ON 05-05-2010

Cardozo-IOB-11

~~SECRET~~

[redacted]

(U) ~~(S)~~ [redacted] was further required to provide annual summaries of the [redacted] under both the AGG and The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSIG), effective October 31, 2003. This did not occur until March 2[illegible] 2007, more than three years after the case was converted to a [redacted] As such, OGC determined that OIPR's oversight ability was impaired, and reported the matter to the IOB.

(U) ~~(S)~~ Next, in IOB matter 2007-1733, on April 11, 2005, [redacted] issued an approved Right to Financial Privacy Act (RFPA) National Security Letter (NSL) to a financial institution for the subject's financial records from [redacted] The financial institution returned financial records for the time period requested, plus additional records prior to [redacted] analyzed the results and uploaded a summary to an FBI database. The data exceeding the scope of the NSL has since been sequestered and purged from the FBI database. [redacted] was unaware of the need to report this matter as a potential IOB error until the Inspection Division (INSD) audit of March 2007.

(U) ~~(S)~~ By agreement with the Counsel to the IOB, third party errors in the collection of information pursuant to an NSL are not reportable unless the FBI has compounded the error. Here, [redacted] analyzed and uploaded the overproduction into an FBI database, thus compounding the error. Accordingly, OGC reported this matter to the IOB.

(U) ~~(S)~~ OGC advised [redacted]

(U) ~~(S)~~ Finally, in IOB matter 2007-2160, the [redacted] Field Office [redacted] reported that, on [redacted] it opened a [redacted] on a Non-United States person. The [redacted] expired on [redacted]. Following the expiration of the [redacted] on [redacted]

~~SECRET~~

2

Cardozo-IOB-12

Appendix 2—IOB Report 2001-46

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DATE: 07-02-2010
CLASSIFIED BY 65179/DMH/plj/lcw
REASON: 1.4 (c)
DECLASSIFY ON: 07-02-2035

~~SECRET~~

INTELLIGENCE OVERSIGHT BOARD (IOB) MATTER

[redacted]

IOB MATTER 2001-46 (U)

b2
b7E

(S) Inquiry has determined that in conducting a [redacted] of [redacted] a United States person, the Federal Bureau of Investigation (FBI) failed to meet the initial reporting requirements prescribed in [redacted] of the Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations (FCIG). In this regard, the [redacted] Division [redacted] opened a [redacted] of the subject on [redacted]. Thereafter, due to administrative error, the [redacted] -- failed to forward [redacted] initial 90-day letterhead memorandum (LHM) to the Office of Intelligence Policy and Review (OIPR), Department of Justice, as required by the FCIG. The error was not realized until [redacted] when [redacted] LHM was received by the [redacted] and forwarded to OIPR for review. The delayed submission clearly precluded meaningful oversight and review of [redacted] ongoing investigation by OIPR, which is contrary to the requirements of [redacted] of the FCIG. The [redacted] initial error was further compounded by the unit's failure to report the error for [redacted] following the discovery of the mistake. FBI regulations specify that potential IOB matters shall be reported with 14 days of discovery. [redacted]s handling of this case has been reported to the FBI's Office of Professional

(U) Responsibility. (S)

b1
b2
b6
b7C
b7E

Classified by: 39646; NSA/OGC
Reason: 1.5(c)
Declassify on: ~~MR~~

~~SECRET~~

APPROVED: Director [redacted] Deputy Director [redacted] Inspection [redacted] Laboratory [redacted] Finance [redacted] National Sec. [redacted] OPA [redacted] Personnel [redacted] Training [redacted] Off. of Public A. [redacted] Cong. Affs. [redacted]

7-7-01

Hofmann-IOB-2234

Appendix 3—IOB Report 2003-25

~~SECRET~~

(U) (S) In IOB matter 2003-04, the FBI initiated a [redacted] on a non-United States person. The [redacted] Due to an administrative error, and after the [redacted] had expired, the FBI conducted an [redacted]

(U) (S) Finally, in IOB matter 2003-25, the FBI initiated a [redacted] on a United States person. The [redacted] expired on [redacted] Due to administrative error, and after the expiration of the [redacted] the FBI interviewed the subject of the inquiry on [redacted] Upon realizing that the [redacted] had expired, the FBI extended the investigation.

(U) (S) [redacted]

(U) Please do not hesitate to contact [redacted] or me if you have any questions regarding these or any other IOB matters.

Sincerely,

Julie F. Thomas
Deputy General Counsel
National Security Law Branch

~~SECRET~~

3

Cardozo-IOB-16

Appendix 4—IOB Report 2006-246

DATE: 06-30-2010
CLASSIFIED BY 65179/DMH/PLJ/LCB
REASON: 1.4 (c)
DECLASSIFY ON: 06-30-2035

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

SECRET

INTELLIGENCE OVERSIGHT BOARD (IOB) MATTER
[redacted] DIVISION
IOB MATTER 2006-246 (U)

b2
b7E

(U) (S) The [redacted] Division reported this potential IOB matter involving unauthorized surveillance.

(S) (S) [redacted] opened a [redacted], who was and remains a "United States person" as that term is used in Section 1014(i) of the Foreign Intelligence Surveillance Act of 1978 (FISA). During the course of the investigation, [redacted] issued two NSLs, [redacted] pursuant to the Electronic Communications Privacy Act, 18 U.S.C. § 2709. The subject NSL requested [redacted]

b1
b2
b6
b7C
b7E

(U) (S) In [redacted] responded to the two NSLs by transmitting information responsive to both on a single compact disk (CD). Subsequently [redacted] determined that the CD contained full email content for both accounts. Pursuant to the direction of NSLB, SA [redacted] sealed and sequestered in A1 envelopes the CD, along with all paper copies of its contents.

b2
b7E

(S) On [redacted] contacted [redacted] and advised regarding overproduction and requested verification of compliance with the limits of National Security Letters. In the interest of administrative parity, on [redacted] served [redacted] with another NSL, requesting [redacted]

b2
b7E
b1
b6
b7C

(S) [redacted] On [redacted] transmitted a CD to the FBI [redacted] Office. Once again information responsive to multiple NSLs was included on the CD.

(S) (S) On [redacted] after having the information separated by email account/NSL, [redacted] determined that once again [redacted] had provided full email content. Based upon advice of CDC [redacted] and NSLB SSA [redacted] and SA [redacted] took corrective action and ensured that the CDs, along with all paper copies of their contents, were sealed and sequestered in 1A envelopes.

b2
b6
b7C
b7E

(S) (S) Despite the fact that [redacted] limited the scope of the subject NSL to [redacted] provided content information concerning an e-mail account. Thus, the FBI unintentionally received that content information not contemplated by the NSL. Such viewing of [redacted] was not authorized under the Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act and/or E.O. 12333. Under these circumstances, it is OGC's opinion that the error, although inadvertent, must be reported to IOB.

b2
b7E

(U) OGC has referred this matter to the FBI's Inspection Division for action deemed appropriate.

(U) ~~(S)Derived From : G-3~~
~~Declassify On: X1~~

Hofmann-IOB-666

~~SECRET~~

Appendix 5—IOB Report 2007-718

~~SECRET~~

DECLASSIFIED BY 65179 DCH/SLP/CW
ON 07-31-2010

INTELLIGENCE OVERSIGHT BOARD (IOB) MATTER
[redacted] FIELD OFFICE
IOB MATTER 2007-718

(U) [redacted] Division reported on 02/23/2007 [redacted] a National Security Letter (NSL) was issued for financial records [redacted] under authority of the Electronic Communications Privacy Act rather than the Right to Financial Privacy Act. The NSL was approved in an EC which also cited the incorrect legal authority and did not articulate the facts supporting its issuance.

b1
b4
b7E
b7E

(U) This matter has been reported to the FBI's Inspection Division for appropriate action.

Hoffman-IOB-1072

~~SECRET~~

Appendix 6—IOB Report 2004-80

DECLASSIFIED BY 65179/DMH/PLJ/sdb
ON 06-30-2010

~~SECRET~~

INTELLIGENCE OVERSIGHT BOARD (IOB) MATTER
IOB 2004-80 (U)

(U)

~~(S)~~ Investigation of this IOB matter has determined that the [redacted] Field Office obtained consumer credit reports from two credit reporting companies in connection with an authorized counterintelligence investigation using a National Security Letter (NSL) that referred to Title 15, United States Code, Section 1681v, when in fact that section only permits the use of NSLs to request credit reports for authorized counterterrorism cases. Title 15, United States Code, Section 1681u, allows the FBI to use an NSL to obtain certain information from credit reporting agencies in authorized counterintelligence cases, specifically, the names and addresses of financial institutions at which the subject of the investigation maintains an account. In order for the FBI to obtain a credit report in a counterintelligence case, it must apply for an ex parte court order under the terms of Title 18, United States Code, Section 1681u(c). b2 b7E

(U)

~~(S)~~ The credit reports that were procured from credit reporting companies by citing 15 U.S.C. §1681v were not properly obtained. Although the error in statutory citation appears to have been inadvertent, and the [redacted] office immediately retrieved and sealed the credit reports once the error was discovered, this matter has been referred to the FBI's Office of Professional Responsibility for such action as may be appropriate. b2 b7E

~~Derived from: G-3~~
~~Declassify on: X25-1~~

~~SECRET~~

Hofmann-IOB-301

Appendix 7—IOB Report 2007-1209

DECLASSIFIED BY 65179/DMH/ab
ON 05-05-2010

SECRET//20180131

(U) INTELLIGENCE OVERSIGHT BOARD (IOB) MATTER
[redacted] FIELD OFFICE
IOB MATTER 2007-1209-NSL (U)

b2
b7E

(S) During an authorized [redacted] of a presumed U.S. person, [redacted] sent a National Security Letter (NSL) under the Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2709. The NSL requested subscriber information and transactional records from the service provider. [redacted] did not, however, include in the NSL a certification that the information sought was relevant to an authorized investigation to protect against international terrorism and that the investigation of a United States person is not conducted solely on the basis of activities protected by the First Amendment to the Constitution of the United States. Notwithstanding the lack of certification, the service provider produced materials in response to the NSL.

(U) This matter is being reported because the field office's NSL did not comply with the requirements imposed by ECPA to obtain subscriber information and transactional records. Specifically, the NSL did not include the appropriate certification. The field office was instructed to sequester the NSL results. The [redacted] has expired; therefore, the field office cannot issue a curative NSL at this time. The field office must contact the service provider and ask whether the NSL results should be returned or destroyed, with appropriate documentation to the file.

b2
b7E

(U)

(S) Derived From: G-3
Declassify On: 11/30/2017

SECRET//20180131
Cardozo-IOB-271

Appendix 8—IOB Report 2002-72

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DATE: 07-02-2010
CLASSIFIED BY 65179/DMH/plj/lcw
REASON: 1.4 (c)
DECLASSIFY ON: 07-02-2035

~~SECRET~~

INTELLIGENCE OVERSIGHT BOARD (IOB) MATTER
[redacted] DIVISION AND THE
[redacted] DIVISION,
FBI HEADQUARTERS
IOB MATTER 2002-72 (U)

b2
b7E

As reported by the [redacted] FBI Headquarters on [redacted]. On [redacted]. In each of the declarations that accompanied the Government's applications [redacted], the Government described events that took place on [redacted], and stated, in pertinent part, that "[redacted]." This was incorrect. In fact, [redacted]. Additionally, a footnote in the Government's [redacted] declaration indicated that [redacted]. This, too, was incorrect. As stated above, [redacted]. These errors, detected on [redacted], were repeated in all three declarations. They were reported [redacted] on [redacted] and subsequently were briefed to [redacted]. They have also been reported to the FBI's Office of Professional Responsibility for action deemed appropriate.

b1
b2
b6
b7C
b7E

~~Derived from: G-3~~
~~Declassify on: X1~~

~~SECRET~~

APPROVED: Crim Inv ____ Inspection ____ Training ____
CJIS ____ Laboratory ____ Off of IOB ____
Finance ____ National Sec ____ Admin ____
Director ____ Gen Counsel ____ OPR ____ Off of Public A ____
Deputy Director ____ Info Res ____ Personnel ____ Cong Aff ____

Hofman-IOB-2374

Appendix 9—IOB Report 2002-74

DATE: 06-29-2010
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (c)
DECLASSIFY ON: 06-29-2035

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

~~SECRET~~

INTELLIGENCE OVERSIGHT BOARD (IOB) MATTER
[redacted] DIVISION AND
COUNTERTERRORISM DIVISION
2002-74 (U)

b2
b7E

Investigation of this IOB matter has determined that, on [redacted] the [redacted] Division obtained an order, (S) [redacted] who was a "United States person" as that term is used in Foreign Intelligence Surveillance Act of 1978 (FISA).[1] The declaration provided by the FBI [redacted] for [redacted] of the target provided incorrect information. The declaration referred to a previously installed audio [redacted] of other subjects at the same location and specifically described how the surveillance is being conducted. However, the technology to implement this surveillance was never installed.[2] The inaccurate representations in the declaration submitted [redacted] were material misstatements of fact, contrary to the Executive Order 12333 and [redacted] thus requiring an IOB reporting. (U)

b1
b2
b6
b7C
b7E

This matter has been referred to the FBI's Office of Professional Responsibility for action deemed appropriate. (U)

~~Derived from: G-3~~
~~Declassify on: X25-1~~

USE/CLU

~~SECRET~~ APPROVED: Dep. Dir. / Associate Dir. / Training / Gen. Counsel / Laboratory / CR. of FBI / Finance / Administrative / Affairs / Director / Gen. Counsel / OPR / Dir. of Public & Deputy Director / Info. Res. / Personnel / Cong. Affs.

[1] (U) The FISA is codified at 50 U.S.C. 1801 et seq. A "United States person" is defined in Section 101(i) of the FISA as: "a citizen of the United States, [or] an alien lawfully admitted for permanent residence . . . ."

[2] (U) The Office of Intelligence Policy and Review was timely notified of this error.

Hofmann-IOB-174

Appendix 10—IOB Report 2005-03

DATE: 09-30-2010
CLASSIFIED BY 65179/DMH/STW/SSR
REASON: 1.4 (D)
DECLASSIFY ON: 09-30-2035

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

INTELLIGENCE OVERSIGHT BOARD (IOB) MATTER
[redacted] FIELD OFFICE
IOB MATTER 2005-03 (U)

(S)

Review of this IOB matter has determined that on [redacted] opened a [redacted] on U.S. persons. [redacted] provided [redacted] and other [redacted] sections information derived from surveillance that had been authorized pursuant to the [redacted] Electronic Communications (ECs) to [redacted] clearly instructed that [redacted] information provided could not be incorporated into any criminal affidavit, criminal court proceedings, subpoenas, or for other legal or judicial purposes. Despite the caveats to this effect contained in the ECs, the [redacted] Division sought and obtained Federal Grand Jury Subpoenas (FGSKIN) [redacted] based on [redacted] information. (S)

(U) To prevent future IOB violations, [redacted] stated that the squad supervisor would closely monitor Federal Grand Jury and National Security Letter requests, and instruct the case agent to review the web-based training regarding the handling of classified information. Additionally, [redacted] instructed the case agent to remove all information provided pursuant to the Federal Grand Jury Subpoena from the case file, seal it in an envelope, and secure it in the squad supervisor's safe [redacted] Department of Justice (DOJ), for delivery to [redacted] and eventual destruction. (S)

This matter has been referred to the FBI's Inspection Division for action deemed appropriate. (U)

(S) ~~Derived From : G-3~~
~~Declassify On: X1~~

~~SECRET~~ Hofmann IOB-432

Appendix 11—IOB Report 2007-1693

DECLASSIFIED BY [illegible]
ON 03-10-2010

~~SECRET//20180205~~

(U) INTELLIGENCE OVERSIGHT BOARD (IOB) MATTER
[redacted] FIELD OFFICE
IOB MATTER 2007-1693 (U)

b2
b7E

(U) [redacted]

(U) [redacted]

b2
b7E

(U) [redacted]

(U) [redacted]

b2
b7E

(U) [redacted] Based Upon our analysis, in accordance with the reporting requirements of Section 2.4 of E.O. 12863, the CE's unauthorized activities of logging onto the target's [redacted] with the target's username and password, and downloading activity reports from the target's account must be reported to the IOB because the surveillance resulted in the unauthorized acquisition of information from a [redacted] not authorized to be monitored under the Foreign Intelligence Surveillance Act or Executive Order 12333.

~~Derived From : G-3~~
~~Declassify on: 01/07/2018~~ ~~[illegible]-IOB-301~~

~~SECRET//20180205~~

Appendix 12—IOB Report 2006-224

DATE: 06-30-2010
CLASSIFIED BY 65179/DMH/PLJ/SCW
REASON: 1.4 (c)
DECLASSIFY ON: 06-30-2035

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

SECRET/ORCON,NOFORN

INTELLIGENCE OVERSIGHT BOARD (IOB) MATTER
[redacted] DIVISION
IOB MATTER 2006-224(U)

(U) (S) The [redacted] Division reported this potential IOB matter involving unauthorized surveillance. b2 b7E

(U) [redacted] b2 b7E

(S/OC/NF) On December 5, 2005, SA [redacted] was presented with information regarding the [redacted]

(S) [redacted] b2 b7E b1

[redacted] NSLB was promptly contacted.

(U) (S/OC/NF) Later on December 5, 2005, NSLB determined that the file could not be viewed without a court order because of the password protection. The file was sequestered, and all individuals receiving the file were told to sequester the information.

(U) (S/OC/NF) Emergency search authority was granted by the Attorney General on [redacted] for the FBI [redacted] b2 b7E

(U) While neither the subject of the investigation, nor the sender of the email are US-PERS, because the server where the file was located is in the US, Fourth Amendment protections apply. Applicable decisional law holds that the password-protected file should not have been viewed without a specifically tailored order. As a consequence of opening a password-protected file, the FBI improperly obtained electronic data. Thus, the surveillance was not authorized under the Foreign Intelligence Surveillance Act or E.O. 12333.

OGC has referred this matter to the FBI's Inspection Division for action deemed appropriate. (U)

(U) (S) Derived From : G-3
Declassify On: X1

Hofmann-IOB-675

SECRET/ORCON,NOFORN

Appendix 13—IOB Report 2008-255

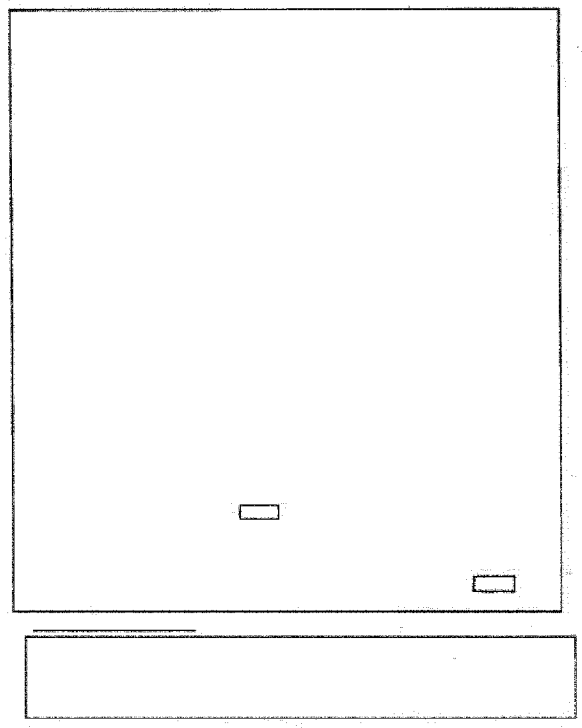
ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-06-2010 BY 65179/DMH/sab

INTELLIGENCE OVERSIGHT BOARD MATTER
2008-255

This adjudication relates to a series of alleged actions by FBI Special Agent [redacted] (SSA [redacted]) which were the subject of a Department of Justice Office of the Inspector General (OIG) and FBI internal investigation. The alleged facts of this case have already been brought to the attention of the IOB. On or about April 10, 2008, OGC orally notified the Counsel to the Intelligence Oversight Board of the details of this incident, and memorialized that report in the form of a letter dated April 15, 2008. This memorandum provides greater details about the matter. b6, b7c

[redacted] b2, b6, b7c, b7E

Carduzo-IOB-73



Cardozo-108-74

[redacted]

Lapses of internal FBI controls or FBI policies, without more, are generally not reportable to the IOB. In the instant case, however, OGC is reporting these FBI policy violations to the IOB based upon the scope of these alleged offenses and for the reasons described below.

[redacted]

b2
b6
b7c
b7e

[redacted]

3 Cardozo-IOB-75

[redacted]

b2
b6
b7C
b7E

Further, OGC concludes that these matters may constitute a violation of the Attorney General Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSIG), [redacted]

b2
b7E

Internal FBI review found while some of SSA [redacted]s

[redacted]

b2
b6
b7C
b7E

OGC does not believe any other provisions of the NSIG are implicated by SSA [redacted]s alleged misconduct.

Accordingly, OGC concludes that SSA [redacted]s alleged misconduct is reportable to the IOB pursuant to Executive Order 13462, the July 17, 2008 Intelligence Board Reporting Criteria, and the April 17, 2007 Memorandum Authored by Stephen J. Hadley, Assistant to the President for National Security Affairs.

b6
b7C

4 Cardozo-IOB-75

Appendix 14—IOB Report 2001-69

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DATE: 07-02-2010
CLASSIFIED BY 65179/DMH/KSR/lrw
REASON: 1.4 (c)
DECLASSIFY ON: 07-02-2035

~~SECRET~~

INTELLIGENCE OVERSIGHT BOARD (IOB) MATTER
[redacted] DIVISION
IOB MATTER 2001-69 (U)

b3
b7E

The Federal Bureau of Investigation (FBI) has determined the [redacted] Division [redacted]

(S) [redacted]

(S) [redacted]

b1
b2
b4
b6
b7C
b7D
b7E

[redacted] as the legal authority to request the information. The letters were signed by the Acting Special Agent in Charge who, at that time, did not have legal authority to issue National Security Letters. This matter has been reported to the FBI's Office of Professional Responsibility for action deemed appropriate.

Classified by: 39645, NSB/OGC
Reason: 1.5(g)
Declassify on: X

~~SECRET~~

APPROVED: Director ____ Deputy Director ____ Inspection ____ Training ____ Off. of EEO ____ Off. of Public & Congr. Affs. ____

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

DATE: 07-01-2010
CLASSIFIED BY 65179 DMH/plj/lsw
REASON: 1.4 (c)
DECLASSIFY ON: 07-01-2035

INTELLIGENCE OVERSIGHT BOARD (IOB) MATTER
[redacted] DIVISION
IOB MATTER 2001-69 (U)

The Federal Bureau of Investigation (FBI) has determined the [redacted] Division obtained financial records pertaining to a suspected terrorist without proper authority. In this regard, in [redacted] in conjunction with an on-going international terrorism investigation of [redacted] Division personnel prepared and issued requests for hotel records pertaining to the subject and his companion, [redacted] and financial records pertaining to the subject. The latter request was sent by facsimile within hours of the attacks on the World Trade Center and the Pentagon to [redacted] requesting bank and credit card records. Although the letters prepared by [redacted] only "requested" information from the record-holders, those responsible for preparing the correspondence incorrectly styled them as National Security Letters (see 50 U.S.C. § 1851 and 12 U.S.C. § 3414) and recited the certification language [redacted] as the legal authority to request the information. The letters were signed by the Acting Special Agent in Charge who, at that time, did not have legal authority to issue National Security Letters. This matter has been reported to the FBI's Office of Professional Responsibility for action deemed appropriate.

(S)
(S)

Classified by: [redacted], NSA/CSC
Reason: 1.5(g)
Declassify on: X1

~~SECRET~~

APPROVED: Dir. Inv. Inspection Training
OIPR Laboratory Off. of ESD
Director FBI Rec. Div. Admin.
Director Gen. Counsel Off. of Public &
Deputy Director Inv. Res. Congr. Aff. Legal Aff.

Hofmann-IOB-1143

Mr. SENSENBRENNER. Mr. Fein?

TESTIMONY OF BRUCE FEIN, CAMPAIGN FOR LIBERTY

Mr. FEIN. Thank you, Mr. Chairman and Members of the Subcommittee.

I would like to amplify on my prior colleague's statement about liberty and go back to first principles, because I think we have turned them on their head in discussing the PATRIOT Act, national security, and otherwise.

Now, as Thomas Paine who wrote, "It's the duty of the patriot to protect his country from his government," and it is in that spirit I wish to address the PATRIOT Act, because it seems to me its fundamental principles are upside down.

This country's bedrock birth certificate was placing the liberty of the individual above the powers of government. The Declaration of Independence, we are all born with unalienable rights. We are endowed with our Creator with a right to liberty. And the purpose of government is to secure those rights. The purpose of government is exhausted after it secures those rights.

And these were not marginal to the fight for our independence from Great Britain. James Otis in 1761 deplored the British general writs of assistance because they did not require probable cause or particularity in searching persons' homes. And it was John Adams who said that was the bell that sounded the independence march of the United States of America. And it's Patrick Henry who is noted for saying, what, "Give me liberty or give me death," not give me liberty, but give me bigger government to protect my liberty.

And I underscore these things to emphasize that where you start in asking the question determines where you end nine times out of 10, why that is so important. And the Founding Fathers did not cherish the right to be left alone just as an intellectual abstraction. It was Justice Louis Brandeis who wrote in 1928, "The architects, the makers of the Constitution, venerated man's spiritual nature, his moods, and his intellect. They sought to protect Americans in their beliefs, their attitudes, seclusions, and challenges to conventional wisdom. They crown citizens with the right to be free from government encroachments, the hallmark of every civilized society." And he concluded, "Every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment."

Now, it is has been said by many, well, where are these court decisions, saying the PATRIOT Act is unconstitutional. There have been a few, but I can see there are few. But the Supreme Court and courts err. In the opinion I was quoting from Justice Brandeis, the court then held conversations were not even protected by the Fourth Amendment, that the government could wiretap and surveil free from any restraints because conversation was not in the text of the Fourth Amendment that addressed persons, houses, papers, and effects. Thirty-nine years later, the Supreme Court reversed.

And we all remember it was this body in 1988 told the Supreme Court during World War II, they got it wrong when they said, you could use race-based concentration camps for Japanese-Americans. Courts can get it wrong. The Supreme Court itself has reversed perhaps 200 times bedrock constitutional principles. So, we should not be complacent with the fact that, well, where are the courts out there?

Moreover, there are reasons why there would not be a plethora of suits challenging the PATRIOT Act. Number one, a former attorney general said, to criticize the Act was to aid and abet enemies in terrorism. There is a climate out there that if you challenge the government on the PATRIOT Act, you are then unpatriotic. You then deserve a opprobrium, and that has been true with many who

defended those who were detained at Guantanamo Bay. That is not the United States of America that was born in 1776. Remember John Adams? He defended the British soldiers accused in the Boston Massacre. He defended them. He did not say, well, this is time when we have to be angry at Great Britain. Due process is out the window. That explains why you do not have a mushrooming number of lawsuits, aside from the fact that in intelligence collection, the target of the investigation is never alerted as they are in a Title III case. How would they know that there is a violation? There is just a huge database, and the fact that the database exists is an abuse of itself.

Now, I want to address specifically the idea, the need to gather just intelligence on Americans because need to protect against international terrorist. Harlan Fiske Stone was appointed attorney general in 1924. He was later appointed Chief Justice of the United States, and he shut down all—all—of the FBI's intelligence collection methods. He said, we have to limit this to law enforcement only. There had been abuses. He styled what the Bureau is doing as tyrannical. So, that is a red herring, in my judgment.

The United States lived securely for over 100 years without just intelligence collection in databases, and I think we can do that today. Probable cause to suspect of crime or the discovery of evidence of crime? Of course the government can seek that kind of evidence. But this is a free country, and the fact that we have limited government, just as Robert Jackson said, does not mean we have weak government. And this is very important. Justice Jackson, of course, was a prosecutor at Nuremberg in addition to being on the United States Supreme Court. And if you would indulge me, let me read his opinion here, because I think——

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

Mr. FEIN. All right. Well, thank you.

[The prepared statement of Mr. Fein follows:]

STATEMENT OF BRUCE FEIN*

ON BEHALF OF CAMPAIGN FOR LIBERTY

RE: THE USA PATRIOT ACT: DISPELLING THE MYTHS

BEFORE THE HOUSE JUDICIARY COMMITTEE

MAY 11, 2011

*Bruce Fein & Associates, Inc.
1025 Connecticut Avenue, N.W., Suite 1000
Washington, D.C. 20036
Phone: 703-963-4968
bruce@thelichfieldgroup.com

Mr. Chairman and Members of the Subcommittee:

I am grateful for the opportunity to speak on behalf of the Campaign for Liberty about the USA Patriot Act. Provoked largely by the gruesome abominations of 9/11, the legislation was born of fear and uncertainty from abroad. Fear, however, is the fount of tyranny. James Madison, father of the Constitution, warned centuries ago in opposing the tyrannical Alien and Sedition Acts of 1798: "Perhaps it is a universal truth that the loss of liberty at home is to be charged to provisions against danger real or pretended from abroad." At the constitutional convention of 1787, Madison similarly recognized the inclination of government to wave a banner of foreign danger to excuse the destruction of domestic liberties: "The means of defence agst. foreign danger, have been always the instruments of tyranny at home. Among the Romans it was a standing maxim to excite a war, whenever a revolt was apprehended. Throughout all Europe, the armies kept up under the pretext of defending, have enslaved the people."

The 342-page USA Patriot Act passed without inquiry into whether arming the government with muscular investigatory tools justified the corresponding intrusions on the right to be left alone—the right most valued by civilized people. The Patriot Act was portrayed as a necessary defense against foreign agents and international terrorists. Citizen liberties were relegated to extras in a Cecil B. De Mille cinematic extravaganza

Despite the good intentions of its architects, the Patriot Act betrays bedrock constitutional principles. The individual is the center of the Constitution's universe. Aggrandizing government is the center of the Patriot Act. The Constitution salutes freedom and citizen sovereignty over absolute safety and citizen vassalage. The Patriot

Act turns that hierarchy on its head. Where experience and facts are inconclusive as regards the need for government authority, the Constitution's default position is liberty. Under the Patriot Act, if a threat passes a microscopic threshold of danger, a Big Brother government is exalted, a descendant of the 1% doctrine. The authorization of "lone wolf" surveillance under the Foreign Intelligence Surveillance Act (FISA) is exemplary. It has never been employed, yet it is defended as a cornerstone of the nation's defense against a second edition of 9/11.

The Alien Act of 1798 was similar. It answered political or popular fears of French immigrants. The President was empowered to deport unilaterally any immigrant thought "dangerous to the peace and safety of the United States." During its two-year life, the President never once invoked the Act's deportation authority. Congress sensibly declined to renew it.

The makers of the Constitution venerated man's spiritual nature, his moods, and his intellect, to borrow from Justice Louis D. Brandeis. They sought to protect Americans in their beliefs, their attitudes, their seclusions, and their challenges to conventional wisdom. They crowned citizens with the right to be left free from government encroachments, the hallmark of every civilized society. To protect that right, Justice Brandeis sermonized, "[E]very unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment." The Patriot Act, nevertheless, shrivels the right to be left alone from Government snooping and surveillance. It sneers at Benjamin Franklin's

admonition: "Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety."

Patriot Act champions boast that only a handful of judicial rulings have cast a cloud over its provisions, for instance, gag orders on National Security Letter recipients. But even the U.S. Supreme Court stumbles. In *Olmstead v. United States* (1928), the Court held conversations were outside the ambit of the Fourth Amendment because its text protected only "persons, houses, papers, and effects." In *Katz v. United States* (1967), thirty-nine years later, the Court overruled *Olmstead* and held the Amendment protected "reasonable expectations of privacy." As Saint Paul preached, "the letter killeth, but the spirit giveth life." 2 Corinthians 3: 6. The Supreme Court sustained the constitutionality of race-based concentration camps for Japanese Americans during World War II. Congress repudiated the Court's odious decisions in the Civil Liberties Act of 1988.

No federal court voided the Sedition Act of 1798, despite its flagrant trespass on free speech. Over 150 years later in *New York Times v. Sullivan* (1964), the Supreme Court denounced the Act as unconstitutional. Many Patriot Act provisions hinge on the decision of the High Court in *U.S. v. Miller* (1976), that bank records or other information "voluntarily" shared with third parties are outside a suspect's zone of privacy protected by the Fourth Amendment. The *Miller* precedent seems increasingly anachronistic in the Age of the Internet in which a virtual diary of individual activities is in the hands of third party Internet Service Providers.

Moreover, extra-constitutional reasons explain the dearth of court challenges. The lion's share of information sought under the Patriot Act is aimed at third parties, not the target of surveillance or investigation. The former have little or no incentive to incur the legal costs and public opprobrium inherent in fighting the government. In addition, many recipients of Patriot Act demands, like telecommunications companies or banks, are motivated to cultivate government goodwill to preserve contracts or friendly regulatory relations. The government has also sought to stigmatize any opponent of the USA Patriot Act as semi-traitorous or un-American through its title or otherwise. Then Attorney General John Ashcroft decried its critics as "aiding and abetting terrorists." But in the true Republic created by our Founding Fathers, the people censure the government; the government does not censure the people. Finally, the vast majority of victims of illegal or unconstitutional surveillance under FISA are never informed of the spying. They do not know the government has compiled a dossier against them.

In light of the hostility toward Patriot Act dissenters generated by the Government and general concealment of violations, the diminutive number of federal court cases is readily understandable. Why bring a lawsuit and risk losing your neighbor, your friends, your job, and your public standing? It might equally be said in defense of Jim Crow that "separate but equal" must have been benign because so few blacks initiated lawsuits seeking its reversal (at the risk of their homes, families, ostracisms, and lives).

At least one Member of Congress has insinuated that a constitutional violation is harmless as long as the Government conceals the violation from the victim, for example, an unconstitutionally seized and retained email or phone call. That assertion seems first

cousin to the nonsense that government assassinations are innocuous if the victims are never acknowledged and their bodies are never found.

Every Founding Father—every Member of the Constitutional Convention of 1787—would have been appalled at the Patriot Act. They were electrified by patriot James Otis' denunciation in 1761 of villainous Writs of Assistance—general search warrants which empowered petty officers to invade privacy and liberty on bare suspicion without oath. Otis elaborated: "It appears to me 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…Every one with this writ may be a tyrant; if this commission be legal, a tyrant in a legal manner, also, may control, imprison, and murder any one within the realm." Patriot John Adams was awed, and remarked, "[T]hen and there was the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child Independence was born."

The spirit of the Fourth Amendment was similarly captured in William Pitt's forceful address to the British Parliament which reverberated throughout the American colonies: "The poorest man in his cottage may bid defiance to all the force of the crown. It may be frail—its roof may shake—the wind may blow through it—the storm may enter—but the King of England cannot enter. All his force dares not cross the threshold of the ruined tenement."

The Patriot Act was misnamed. Thomas Paine lectured: "It is the duty of the patriot to protect his country from its government." Accordingly, the true patriots of the Constitution and the Republic are the "band of brothers" who stood or are standing in

opposition. They understand that the secret of happiness is freedom. And the secret of freedom is the courage to accept risk as inherent to an enlightened and civilized existence. Proponents of the Patriot Act acted from weakness, not strength. I do not, however, question their motives. They are all honorable men and women. But as Justice Brandeis presciently observed: "Experience should teach us to be most on our guard to protect liberty when the Government's purposes are beneficent…The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well meaning but without understanding."

President John F. Kennedy taught, "Two thousand years ago, the proudest boast was "civis Romanus sum." Today, among the disciples of liberty, the proudest boast should be, "I am an American." On Gettysburg battlefield, seven score and eight years ago, President Lincoln noted that our forefathers "brought forth upon this continent a new nation, conceived in Liberty…." Repealing the Patriot Act would honor what they so nobly begot.

Persons are born with unalienable rights to liberty. Liberty for its own sake is the definition of America. Lectures that only citizens with something to hide would balk at invasions of liberty are counter-constitutional and un-American. The whole purpose of the Fourth Amendment is to saddle government with a heavy burden of demonstrating by indisputable evidence a compelling need to disturb the domain of any citizen before crossing his threshold. Non-particularized roving wiretaps justified to prevent surveillance targets from outfoxing the government miss the point. Making the

convenience of law enforcement or intelligence collection subservient to liberty is the Amendment's whole purpose.

The Government has been endowed with Patriot Act authorities for a decade—ample time to prove their indispensability to national security. Every provision should be repealed forthwith absent proof by the executive that but for the authority conferred an act of international terrorism would have succeeded. If the evidence is vague or inconclusive, the Constitution's default position favoring liberty dictates repeal.

Authorizing government to collect intelligence on citizens for non-law enforcement purposes offends the spirit if not the letter of the Fourth Amendment. Spying for domestic security predictably mushroomed during World War I and its aftermath fueled by the "Red Scare." President Calvin Coolidge appointed Harlan Fiske Stone as Attorney General in 1924. Stone was later appointed Chief Justice of the United States. His signature achievement was to terminate investigations or intelligence collection by the Bureau of Investigation, except for law enforcement. Stone observed, "The organization was lawless, maintaining many activities which were without any authority in federal statutes and engaging in many practices which were brutal and tyrannical in the extreme." He asked for the resignation of the Bureau Director William J. Burns, former head of the Burns Detective Agency, and directed that the activities of the Bureau "be limited strictly to investigations of violations of law, under my direction or under the direction of an Assistant Attorney General regularly conducting the work of the Department of Justice."

Citizen loyalty and love for the United States is the mainstay of national security. It is fostered by the Government's scrupulous adherence to constitutional limitations and restraints, not by coercion or suspicion that every citizen could be a Benedict Arnold. As World War II raged, Justice Robert Jackson observed: "Government of limited power need not be anemic government. Assurance that rights are secure tends to diminish fear and jealousy of strong government, and by making us feel safe to live under it makes for its better support. Without promise of a limiting Bill of Rights it is doubtful if our Constitution could have mustered enough strength to enable its ratification. To enforce those rights today is not to choose weak government over strong government. It is only to adhere as a means of strength to individual freedom of mind in preference to officially disciplined uniformity for which history indicates a disappointing and disastrous end."

Patriot Act defenders argue that the absence of "bodies on the sidewalk" proves its respect for the Constitution and civil liberties. The argument misconceives the fundamental premises of America. Every citizen is born with the unalienable right to be left alone. Government is instituted to secure that right, not to cripple it. Government in the United States, as opposed to the People's Republic of China, has no business collecting or retaining information about citizens without "probable cause" to believe that a crime has been or will be committed by a target who is identified with "particularity; or, that a particularized search will unearth evidence of crime. Each and every Patriot Act investigation involving citizens triggered by less than probable cause or involving non-particularized targets or searches is an abuse of government power. At present, the

number of victims probably exceeds one million, including recipients of National Security Letters or targets of section 215 surveillances.

Section 206 of the Patriot Act authorizing roving wiretaps to collect foreign intelligence; section 215 authorizing orders to seize any "tangible thing" like books or computer hard drives to protect against international terrorism or clandestine intelligence activities; section 505 authorizing National Security Letters to seize customer records of financial institutions, credit bureaus, and telecommunications providers by the government's assertion of relevance to preventing international terrorism or clandestine intelligence activities; and, section 6001 of the Intelligence Reform and Terrorism Prevention Act of 2004 authorizing surveillance against hypothetical "lone wolf" international terrorists are all abusive of citizen liberty because they encroach on the right to be left alone without probable cause to believe the target is implicated in crime.

Since 9/11, the nation has witnessed approximately 170,000 murders. But that ghastliness has not provoked the suspension of habeas corpus or civil liberties in a quest for absolute safety. The Supreme Court lectured in *United States v. United States District Court,* 407 U.S. 297, 314 (1972): "The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of Government action in private conversation. For private dissent, no less than open public discourse, is essential to our free society."

The Patriot Act, in isolation, is no mortal blow to the Constitution. But James Madison instructed: "It is proper to take alarm at the first experiment upon our liberties.

We hold this prudent jealousy to be the first duty of citizens and one of the noblest characteristics of the late Revolution. The freemen of America did not wait till usurped power had strengthened itself by exercise and entangled the question in precedents. They saw all the consequences in the principle, and they avoided the consequences by denying the principle. We revere this lesson too much …to forget it."

Many argue that the Constitution is an unaffordable luxury in confronting the danger of Al Qaeda. The Supreme Court's answer in *Ex Parte Milligan* (1866) is unanswerable: "The Constitution of the United States is a law for rulers and people, equally in war and in peace, and covers with the shield of its protection all classes of men, at all times, and under all circumstances. No doctrine, involving more pernicious consequences, was ever invented by the wit of man than that any of its provisions can be suspended during any of the great exigencies of government. Such a doctrine leads directly to anarchy or despotism, but the theory of necessity on which it is based is false; for the government, within the Constitution, has all the powers granted to it, which are necessary to preserve its existence…."[1]

---

[1] Violations of the Patriot Act compound the abuse inherent in investigations without probable cause to suspect crime. Estimating their frequency is problematic. Implementation of the Act is shrouded in secrecy; and, the involved parties have little incentive to disclose compounded abuses. The absence of public documentation of a single sanction against a government official despite thousands of violations publicly reported by the Inspector General of the Department of Justice is worrisome.

The climate of antagonism towards liberty fostered by the Patriot Act has facilitated abusive application, as chronicled below.

A. Brandon Mayfield. Brandon Mayfield is an attorney, a veteran of the United States Army, a Muslim, and a United States citizen. The government aggressively investigated him under the Patriot Act for alleged complicity in the March 11, 2004 bombings of several commuter trains in Madrid, Spain,

despite definitive exculpatory evidence supplied by the Spanish National Police. He was detained for two weeks. He was subject to electronic surveillance with no showing of probable cause to believe he was complicit in crime. His home was repeatedly invaded and scoured. He was consistently followed, and his "shared and intimate" rooms were "bugged." Personal information obtained as a result of the investigation was shared among several intelligence agencies and stored in government databases.

B. Sami Al-Hussayen. Sami Al-Hussayen was known to his Moscow, Idaho community as a family-oriented father of three who, shortly after the Sept. 11 attacks, organized a blood drive and a candlelight vigil that condemned the attacks as an affront to Islam. The government investigated and detained him for providing "expert advice or assistance" to international terrorists outlawed by a Patriot Act amendment to 18 U.S.C. 2339. His alleged crime was volunteering to use his computer skills to run Websites for a Muslim charity. While the charity generally promoted peaceful religious teachings, prosecutors alleged that buried deep within the Web sites were a handful of violent messages — written by others — encouraging attacks on the United States and donations to terrorist organizations. Al-Hussayen was eventually acquitted of all terrorism-related charges.

C. Tariq Ramadan. Tariq Ramadan is an Oxford University professor and a leading Muslim scholar who advocates the peaceful integration of Muslim values and western culture. His lectures include a discussion on "Why Islam Needs a Feminist Movement" and "Muslim Democrats in the West and Democratization in the Muslim World: Prospects for Engagement." In August 2005, at the invitation of Prime Minister Tony Blair, Professor Ramadan accepted an invitation to join a U.K. government taskforce to examine the roots of extremism in Britain.

Professor Ramadan has been a consistent critic of terrorism and those who use it. In October 2001, Professor Ramadan publicly deplored the September 11 attacks, saying to fellow Muslims, "Now more than ever we need to criticize some of our brothers . . . You are unjustified if you use the Koran to justify murder." Professor Ramadan publicly condemned the kidnapping of two French journalists in Iraq in August 2004; the attacks on Jewish synagogues in Istanbul in November 2003; and the terrorist bombing in London in July 2005.

In January 2004, Professor Ramadan was offered a tenured position as the Henry R. Luce Professor of Religion, Conflict and Peacebuilding at the University of Notre Dame's Joan B. Kroc Institute for International Peace Studies. Professor Ramadan was granted a specialized nonimmigrant visa on May 5, 2004, but on July 28, just nine days before Professor Ramadan and his family were to move to Indiana, he was informed that his visa had been revoked. Professor Ramadan was not directly provided an explanation for the revocation and neither Professor Ramadan nor the University of Notre Dame has ever received a written explanation. At a press conference on August 25, 2004, however, Russ

Knocke, a spokesman for the Immigration and Customs Enforcement division of the Department of Homeland Security, cited the ideological exclusion provision of the Patriot Act as the basis for the revocation.

D. Wiretapping of Children. After FOIA requests and a review of FBI responses, the Electronic Frontier Foundation discovered that, in 2005, FBI Agents devoted five consecutive days to monitoring the telephone conversations of two "young children" under a roving wiretap mandate.

Mr. SENSENBRENNER. Mr. Mullins?

TESTIMONY OF ED MULLINS, PRESIDENT, SERGEANTS BENEVOLENT ASSOCIATION OF NEW YORK

Mr. MULLINS. Mr. Chairman, Ranking Member Scott, and Members of the Subcommittee, thank you for having me here today. I am here as the head of a police labor organization representing my

members and their family. I also speak with the perspective of a sworn law enforcement officer with 30 years of experience.

I responded to the scene of the terrorist attacks on September 11th, 2001. I also responded in 1993 to the terrorists' first attempt to topple the Twin Towers.

I am a third generation New Yorker whose life was forever changed by the terrorist attacks of 9/11. These unprovoked attacks devastated New York City and the ranks of its fire and police departments. The 2,973 innocent men, women, and children killed on 9/11 surpassed the death toll America suffered in the surprise attack on Pearl Harbor that triggered our entry into World War II.

Sadly, the final casualty figures from 9/11 are not yet known. Those terrorist acts continue right up to the present day to claim the lives of more firefighters, police officers, construction workers, and ordinary citizens who were caught in the events of that fateful day. These are the people who, in the years after 9/11, have developed debilitating illnesses and died from their exposure to the toxins released when the World Trade Center Towers collapsed.

The James Zadroga 9/11 Health and Compensation Act, passed late last year to help discontinue victims, is a stark reminder that while justice has been served on bin Laden, innocent Americans continue to die and suffer as a result of his evil.

The USA PATRIOT Act was enacted in direct response to these terrorist attacks for the purpose of preventing any repetition. I appreciate the chance to help clear up some of the myths surrounding the deliberations over whether to reauthorized three specific expiring PATRIOT Act authorities. Let me begin by setting aside the false clarities and simplicity that seek to impose on these deliberations.

Reauthorizing these authorities is not a stark choice between whether we place a greater value on our civil liberties than our security. It is not a choice between freedom and a police state. Let us not lose sight of how much alike every one of us in this room today really is. We share the same values. We are all Americans who love our country and the liberties upon which it is founded. We all hate seeing our fellow citizens slaughtered by bin Laden's demented disciples. None of us desire or intend to extinguish liberty in the pursuit of security. We only differ as to how, not if, our elected representatives should strike a balance between the universal value of protecting innocent lives from murderers and our uniquely American notion of individual liberty.

Reauthorizing the three provisions set to expire later this month strikes the right balance. By any historical yardstick, these authorities are a measured response to an unprecedented and undeniably real threat to our Nation. A generation learned from struggles, the heroes of our past encountered imbalance in liberty and security while reacting to the unprecedented threats. We did not respond by rounding up and committing to internment camps all members of the ethnic and religious minorities from which the perpetrators of 9/11 were descended. We did not grant law enforcement wholly unprecedented powers never before entrusted to police on our shores. What we did was to extend the Federal agents hunting terrorist powers analogous to those that state and local enforce-

ment have long used to investigate drug dealers, burglars, and other common criminals.

In closing, let me dispel one final myth. We can let our guard down and permit these authorities to sunset because bin Laden is dead. The Pakistani Taliban, which was behind last year's attempt to bomb Time Square, has vowed revenge. They have bragged, "We already have our people in America and are sending more." Do not allow our recent success to obscure the fact that 10 years ago in less than 2 hours we lost more Americans at the hands of bin Laden's henchman than we did almost 70 years ago on the Island of Guadalcanal.

Our enemies are more desperate than ever to replicate this horror. A generation faces an unprecedented threat from a new kind of foe. Still, we are very fortunate. Responding to the great crisis of our age does not require drafting citizens to fight. It has not necessitated the conversion of our economy to wartime footing. There is no rationing of fuel, food, and other resources. Citizens are not even asked to buy war bonds. It is a testament to America's strength that most citizens can go about their lives much as they did before 9/11 and delegate defeating the terrorists who declared war on us to a relatively small group of volunteers.

As cops, my members are among those volunteers. We pray that as you debate the tools available to our Federal counterparts that played a critical role in this mission, they will be pragmatic in balancing the defense of our Nation with the preservation of the freedoms we cherish. We hope that you will not be seduced by rigid ideologies that demand the sacrifice of one of the fundamental values of another.

As you know, this week is Police Week in our Nation's capital. As we recognize all those officers who made the ultimate sacrifice, I beg that you do not disarm those sworn to protect you at a time when our enemies are bringing a renewed fervor and new tactics in their efforts to murder Americans.

[The prepared statement of Mr. Mullins follows:]

TESTIMONY

Of

Ed Mullins
President
Sergeants Benevolent Association of New York City

On

"The USA PATRIOT Act: Dispelling the Myths"

Before the

Subcommittee on Crime Terrorism and Homeland Security
Committee on the Judiciary
U.S. House of Representatives

May 11, 2011

Mr. Chairman, Ranking Member Scott, and Members of the Subcommittee:

Thank you for having me here today to provide the perspective of local law enforcement concerning whether Congress should reauthorize the three Patriot Act authorities scheduled to sunset at the end of this month.

I am here as the head of a police labor organization representing my members and their families. I also speak with the perspective of a sworn law enforcement officer with almost 30 years of experience. I responded to the scene of the terrorist attacks on September 11, 2001. I also responded in1993 to the terrorists' first attempt to topple the Twin Towers. I am a third generation New Yorker whose life was forever changed by the terrorists attacks of 9/11. These unprovoked attacks devastated New York City and the ranks of its Fire and Police Departments. To put these attacks in historical perspective, the 2,973 innocent men, women and children killed in less than two hours on 9/11 surpassed the death toll America suffered in the surprise attack on Pearl Harbor[1] that triggered our entry into World War II. It is almost equivalent to the total number of American troops killed in Iraq and Afghanistan over the last decade.[2]

Among the dead on 9/11 were 343 firefighters and seventy-two federal, state and local law enforcement officers, including, thirty-seven members of the Port Authority Police Department and twenty-three members of the NYPD. According to the 9/11 Commission the FDNY's losses were "the largest loss of life of any emergency response agency in history."[3] The losses of the Port Authority Police and the NYPD on 9/11 constitute the first and second "largest loss of life of any police force in history." [4]

Let us also not forget that the final casualty figures from 9/11 are not yet known. Those terrorist acts continue right up to the present day to claim the lives of more firefighters, police officers, construction workers, and ordinary citizens who were caught in the events of that fateful day. These are the people who in the years after 9/11 have developed debilitating illnesses and died from their exposure to the toxins released when the World Trade Center Towers collapsed. The James Zadroga 9/11 Health and Compensation Act passed late last year to help this continuing tide of victims is a stark reminder that while Seal Team Six has visited justice upon bin-Laden, innocent Americans continue to die and suffer as a result of his evil. Let us also not forget the many parents, children, sisters and brothers who have struggled for the last decade to live their lives without a child, a parent or a sibling lost on that tragic day.

These heart-wrenching statistics are appropriate to dwell upon as we commemorate National Police Week. They remind us that our countrymen have died in large numbers and continue to die as a result of a very real war that terrorists declared upon America. They also

---

[1] According to the National Park Service 2,388 military personnel and civilians were killed in the attack on Pearl Harbor December 7, 1941. http://www.nps.gov/nr/twhp/wwwlps/lessons/18arizona/18charts1.htm

[2] According to the non-profit organization icasualties.org, to date a total of 3,063 U.S. troops have been killed in Iraq and "in and around" Afghanistan (1,572 in Iraq and 1,491 "in and around Afghanistan"). http://icasualties.org/OEF/Index.aspx

[3] Report of the National Commission on Terrorist Attacks Upon the United States at 311 www.9-11Commission.gov/report/index.htm

[4] *Id.*

remind us that although the three expiring Patriot Act authorities are tools reserved for federal agents, it is state and local first responders and the citizens we are sworn to protect and serve who will suffer most of the consequences that may be realized if these authorities expire before the War on Terror is won.

The USA PATRIOT Act was enacted in direct response to the 9/11 terrorist attacks and to prevent their repetition. I have been dismayed to hear people avoid the serious and complex questions involved in the discussion of whether to reauthorize the expiring authorities by reverting to generalizations such as Benjamin Franklin's statement that "[t]hose who would give up essential liberty to purchase a little temporary safety deserve neither liberty nor safety." Reasonable minds can differ as to whether the expiring authorities, one of which cannot even be used against U.S. citizens, implicate what Ben Franklin and the Founding Fathers would have deemed "essential liberty." No one, however, should trivialize the tragedy of 9/11 by describing efforts to prevent its repetition as a quest for "a *little temporary* safety." To those content to revert to sound bites divorced from the context of experience I counter with Abraham Lincoln's admonitions that "the dogmas of the quiet past are inadequate to the stormy present" and that:

> *If there ever could be a proper time for catch arguments, that time surely is not now. In times like the present, men should utter nothing for which they would not willingly be responsible through time and eternity.*[5]

Let us set aside the false clarity and simplicity that some seek to impose on these deliberations. My members and I are not timid souls begging some tyrant to take our liberties from us if only he would guarantee our physical safety from an imagined threat. Reauthorizing these expiring authorities is not a stark choice between whether some people place a greater value on our civil liberties than on our security. It is not a choice between freedom and a police state. Let us not lose sight of how much alike every one of us in this room today really is. We share the same values. We are all Americans who love our country and the liberties upon which it is founded. We all abhor seeing our fellow citizens slaughtered by bin-Laden's demented disciples. None of us desire or intend to extinguish liberty in the pursuit of security. We differ as to how, not if, our elected representatives should strike a balance between the universal value of protecting innocent lives from murderers and our uniquely American notions of individual liberty.

As a citizen who values his liberty as much as any other, and as a police officer who has witnessed the awful cost of letting one pitch from the terrorists get past us, it is my opinion that reauthorizing the three provisions set to expire later this month strikes the right balance. By any historical yardstick, these authorities are a measured response to an unprecedented and undeniably real threat to our nation. Our generation learned from struggles the heroes of our past encountered in balancing liberty with security at home in the face of unprecedented threats. We did not respond by rounding up and committing to internment camps all members of the ethnic or religious minorities from which the perpetrators of 9/11 were descended. We did not grant law enforcement wholly unprecedented powers never before entrusted to police on our shores. What we did was to extend to federal agents hunting terrorists powers analogous to those that

[5] Lincoln's Second Annual Message to Congress December 1, 1862.

state and local law enforcement have long used to investigate drug dealers, burglars and other common criminals who pose far less of a threat to society than bin-Laden's followers.

You do not have to be a constitutional law scholar to make some observations about the expiring specific Patriot Act authorities that ordinary people find pretty compelling:

> There is no record of a pattern of abuse by federal law enforcement of these three specific authorities.
>
> The expiring authorities do not relate to National Security Letters, for which Congress did have to tighten procedures and controls.
>
> If abuses materialize, Congress can always make adjustments after reauthorization.
>
> All three of the expiring authorities require the prior approval of a federal judge experienced in criminal matters whose integrity, wisdom, and impartiality have been scrutinized by your Senate colleagues during the confirmation process.
>
> Under the Patriot Act it is *more difficult* for federal agents to get authority to use the investigative tools the three expiring provisions extended to federal law enforcement involved in terrorist cases than it is for local police officers to use similar techniques when looking into drug dealers or mobsters.
>
> Over the last decade none of the three authorities has been found unconstitutional.[6]

People like Mr. Barr and Mr. Fein play a valuable role in our society by ensuring that Congress does not pass laws that are on their face unconstitutional or that are used in a manner that violates constitutionally protected rights. For this I thank them. They keep us mindful of how these authorities *may* be abused to deprive people of their rights. But let's be clear that concerns about systemic abuses of the three expiring Patriot Act authorities are a risk that has not yet been realized. I wish I could say the same about terrorism on American soil.

Since 9/11 the United States has foiled no less that 32 terrorist plots to murder innocent Americans.[7] While it's been estimated that post-9//11 PATRIOT Act authorities were instrumental in about one-sixth of these efforts,[8] the nature of diligent police work makes that a hard thing to quantify. By its nature good police work is a mixture of the lucky-breaks that often accompany hard work combined with facts gathered in myriad ways that come into clear focus only with the application of experience and a seasoned intuition. It is tough to say just what ingredient in this recipe makes it work. It may differ in each case. But even if the expiring

---

[6] In *Mayfield v. U.S.*, a federal district court in Oregon did rule that the aspects of roving wiretaps under section 206 may infringe on 4th amendment rights, but this decision was vacated by the United States 9th Circuit Court of Appeals in *Mayfield v. U.S.*, 599 F.3d 964, 970 (9th Cir. 2010) *cert. denied,* 131 S. Ct. 503, 178 L. Ed. 2d 369 (U.S. 2010).

[7] *Ordinary Measures, Extraordinary Results: An Assessment of Foiled Plots Since 9/11.* http://americansecurityproject.org

[8] *Id.*

Patriot Act authorities have been the key ingredient in stopping just one or two more 9/11s, or one or two more Pearl Harbors, that is significant.

The argument that since one of these authorities, the "Lone Wolf" provision, may never have been used and therefore should be repealed does not make sense to me. We arm police officers in this country because experience and common sense show it is necessary. We do not take away a cop's gun if he has failed to fire it after ten years. We rejoice that he has never had to do so, but require him to remain proficient and able to use his weapon if he must.

With disclosure of plans for new plots and tactics found in bin-Laden's lair we are reminded that the terrorists are still intent on replicating the nightmare of 9/11. We are all relieved that bin-Laden is dead, but many who subscribe to his hateful, anti-American ideology remain. The Pakistani Taliban, which was behind last year's attempt to bomb Times Square, has vowed revenge. They've bragged "[w]e already have our people in America, and we are sending more there."[9] We should not dismiss these threats. In my experience when a crime family or a street gang loses its leader, there is often a competition among his surviving followers to become the new boss. The hallmark of such contests often takes the form of novel displays of brutality and cruelty that gain the perpetrator the obedience of the group. I do not see any reason to expect anything different from Al-Qaeda, except that instead of perpetrating their brutality on each other or a rival gang, they will direct it at us. As they seek to do so, I would argue that federal agents will need more and not less flexibility to adjust and respond. Do not allow our recent success to obscure the fact that ten years ago in less than two hours, we lost more Americans at the hands of bin-Laden's henchmen than we did almost seventy years ago at Guadalcanal.[10] Our enemies are more desperate than ever to replicate this horror. Do not punish law enforcement for the success it has had in pitching a shutout every day for the last ten years by assuming that this success is the result of a half-hearted effort by a foe that has given up.

Our generation faces an unprecedented threat from a new kind of foe. We have tough fighting ahead. Still, we are very fortunate. Responding to the great crisis of our age has not required drafting citizens to fight. It has not necessitated the conversion of our economy to a war-time footing. There is no rationing of fuel, food, and other resources. Citizens are not even asked to buy war bonds. It is a testament to America's strength that most citizens can go about their lives much as they did before 9-11 and delegate defeating the terrorists who declared war on us to a relatively small group of volunteers. But this strength poses a risk. This is the risk that the vast majority of Americans are so far removed from the exertions and exactions of this war that they do not fully appreciate the danger it presents or the commitment it requires.

As cops, my members are among those volunteers who understand the risk and what must be done. We ask that as you debate the tools available to our federal counterparts to play their critical role in this mission that you will be pragmatic in balancing the defense of our nation with the preservation of the freedoms we cherish. We hope you will not be seduced by rigid ideologies that demand the sacrifice of one of these fundamental values for the other. As you

---

[9] *Threat of Revenge Emerges After bin Laden Killed* (May 3, 2011) www.kpax.com/news/threat-of-revenge-emerges-after-bin-laden-killed/

[10] According to the National Park Service the battle for Guadalcanal resulted in the death of "1,598 officers and men killed." www.nps.gov/archive/wapa/indepth/extcontent/usmc/pcn-190-003117-00/sec6.htm

commemorate National Police Week and the sacrifices law enforcement makes to protect America, we beg that you do not disarm those sworn to protect you just as our enemies are bringing a renewed fervor and new tactics to their efforts to murder Americans.

Thank you again for considering my views.

Respectfully,

Edward D. Mullins

Mr. SENSENBRENNER. Thank you very much, Sergeant.

The Chair will now recognize Members alternatively by side for 5 minutes to ask questions of the members of the panel. And the Chair has made note of the approximate order in which Members have appeared, and will use that list in terms of recognizing folks.

And the Chair recognizes himself for 5 minutes.

Mr. Barr, you voted in favor of the PATRIOT Act when it was considered in the Committee, and then you voted in favor of another version that was less favorable to civil liberties when it appeared on the floor in October of 2001. The Committee has done extensive oversight under both Republican and Democratic control. Why do you think we failed, and why are you opposing just a simple extension of what has been the law since 2005 in these three areas given your votes in favor of it?

Mr. BARR. I certainly, Mr. Chairman, would not deign to try and speculate on what Members have done or not done or why. I can certainly speak for myself.

Yes, I did vote both for the better version more protective of civil liberties that was reported out unanimously by the full Judiciary Committee. Subsequent to that, when a very different bill came to the floor, I had several conversations, including some personal ones, with the Attorney General and some other members of the Department of Justice with regard to certain promises or assurances that the provisions in the PATRIOT Act then to be voted on would be used in certain ways for certain investigations that were indeed important national security terrorism related investigations. There were promises made that the executive branch, the President and the Attorney General, would report regularly and openly and extensively on the use of the PATRIOT Act.

Mr. SENSENBRENNER. Oh, I think they did that after you left the Congress. As a matter of fact, there was one time I cancelled a hearing of Attorney General Ashcroft because he didn't submit his testimony on time. So, you know, maybe we were busy doing something else.

Let me ask you another question. There was an outstanding warrant against Osama bin Laden. You condemned the President for sending a U.S. military unit to strike and kill him when the civilian justice system was waiting to grind slowly away at him?

Mr. BARR. No, I think this was one of those instances in which the resolution the use of military force does provide and did provide proper authority for the presidential action of taking out Osama bin Laden.

Mr. SENSENBRENNER. Okay. But should not the President have used what you refer to as tried and true methods of capturing what you call a criminal-like bin Laden, like pursuant to an arrest warrant?

Mr. BARR. No, simply because an individual can be pursued either through the criminal justice system or militarily in certain circumstances does not make it improper to choose one over the other. And in this instance, I think the President chose wisely and properly, and it was properly authorized by the Congress, unlike some of the other actions by the current and former Administration using the resolution for the use of military force which does not provide proper authority.

Mr. SENSENBRENNER. The PATRIOT Act was passed after 9/11. Do you think the U.S. attorneys of New York, New England, and Washington, D.C. could have prevented the 9/11 attack by using traditional law enforcement methods?

Mr. BARR. Certainly not being privy to all of the information that they had or did not have or the circumstances under which certain

acts were authorized or not authorized, it does seem to me that there was more than sufficient authority to have given us—the U.S. government, that is—a much greater chance, likelihood of having prevented the attacks had those proper preexisting authorities been used. They were not used.

Mr. SENSENBRENNER. Well, the PATRIOT Act repealed the wall that prevented the FBI and the CIA from exchanging information. So, if the CIA knew that there were Al-Qaeda terrorists loose in the United States and, specifically, in the New York City area, it would have been a violation of the pre-PATRIOT Act law for the CIA to walk that information across the hall and give it to the FBI.

Mr. BARR. Not necessarily.

Mr. SENSENBRENNER. Oh, yes, it would have. Yes, it would have. Yes, it would have been.

Mr. BARR. And on circumstances under which it was required, Mr. Chairman.

Mr. SENSENBRENNER. Well, if the circumstances were, you know, that they acquired it overseas and then they found out that they appeared in New York, it was still giving them intelligence that they had found overseas. And the 9/11 Commission determined that the wall prevented that, and they studied it extensively for a couple of years.

Mr. BARR. Well, we also now know, and with hindsight, that the—is the 19th or 20th hijacker—I forget the number—that had the government gone before a court and sought a warrant to access that person's computer, which a court, based on the circumstances we know now existed at the time, almost certainly would have granted a warrant. The fact of the matter is, the government chose not to do that. They made a policy error. It was not that the law did not allow it. They made a policy error.

Mr. SENSENBRENNER. Well, you know, from what I have heard you say, I think that you are advocating that before 9/11, the FBI would have violated the law that that was put up by the Church Commission if they ended up exchanging intelligence information. And as a result of the PATRIOT Act, we do not have that any more.

The gentleman from Virginia, Mr. Scott?

Mr. SCOTT. Thank you, Mr. Chairman.

One of the problems with the PATRIOT Act is understanding exactly what it does. And so, Mr. Rowan, let me ask you a question. In declaring someone to be a "Lone-Wolf", where you can begin surveilling them, what information and what standard is there that you would not be able to get a run of the mill criminal warrant?

Mr. ROWAN. Congressman, as you know, the FISA statute, with respect to the "Lone-Wolf" definition, talks about an individual engaged in activities relating to terrorism or preparation therefor. So, potentially you could think of circumstances where an individual was engaged in preparation for terrorist activities, and yet an Article III judge looking at it from a criminal law enforcement perspective might determine that there is not probable cause.

But I agree with the thrust of your question, which is that most of the circumstances one can conceive of would also describe a crime that you could obtain a Title III wiretap under.

Mr. SCOTT. Okay. Let me ask the same question about business records. You've suggested it is the kind of same as criminal. What kind of investigation could you get business records under PATRIOT Act that you cannot get them under a regular criminal warrant?

Mr. ROWAN. Well, when you say a warrant, I presume you mean a grand jury subpoena. Certainly, a——

Mr. SCOTT. Well, whatever the warrant, grand jury subpoena, or however else you want to get it.

Mr. ROWAN. Yeah. No, I think you are right, that you could get all those tangible things with a grand jury subpoena. The critical difference is obviously not what you can get, but the circumstances under which you can get it. If you get it under a business records under FISA, you have the opportunity to gather it covertly, to use it for an intelligence investigation with far less risk that your investigation is going to be exposed.

Mr. SCOTT. And if you get it with a criminal warrant, you cannot keep it secret?

Mr. ROWAN. You cannot. I mean, with a grand jury subpoena, you are in a position when it hand it to a third party custodian. That custodian has every right and opportunity to turn around and share it with whoever else he or she cares to include in the target.

Mr. SCOTT. And you cannot have an order prohibiting the dissemination of that information in the criminal court?

Mr. ROWAN. I think what conventionally occurs is an AUSA will write a letter. They will request the third party custodian not to share the information. The actual getting an order from a judge, there may be circumstances under which you can obtain that. I think there are some judges that would provide it, others that might not.

Mr. SCOTT. Roving wiretap—who gets to approve it, and after approval, what kind of oversight is there that is different under the PATRIOT Act that you cannot do in a normal criminal warrant?

Mr. ROWAN. Well, a roving wiretap is obviously a FISA wiretap, so the approval mechanism——

Mr. SCOTT. Well, no. Under FISA, you have to designate it to be roving rather than kind of a stationary wiretap, or all wiretaps under FISA roving wiretaps?

Mr. ROWAN. No, they are not all roving wiretaps. The way it kicks in is when you are asking the court—the FISA judge—what sort of orders you are going to need, and that is when the circumstances under which you described this as being an occasion where you need a roving wiretap. So, the approval mechanisms there, both within the Department of Justice, they are higher for a roving wiretap in a FISA context than you would have in an ordinary Title III wiretap. The approval with respect to the judiciary is going to be the same thing. It is going to be an Article III judge, and one of them happens to sit on the FISA court, the other does not.

Mr. SCOTT. Once you get personal information subject to surveillance, exactly how many people have access to that information?

Mr. ROWAN. When you say surveillance, you mean in the FISA world.

Mr. SCOTT. Yeah, in the FISA world, you got a FISA wiretap. In Northern Virginia, a lot of people work for the "government." How many people get access to the private information that you have listened into?

Mr. ROWAN. As you know, in the FISA statute there are a requirement for minimization procedures, which are procedures that are approved by the FISA court, which restrict the government's dissemination of information. With the respect to——

Mr. SCOTT. Well, the whole point of this is for the FBI to talk to the CIA, to talk to everybody else. I mean, how many people get access to this information?

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

Gentleman from California, Mr. Lungren?

Mr. LUNGREN. Thank you very much, Mr. Chairman, and thank you for these hearings.

Mr. Fein, you and I have been on the same side of arguments before, but we find ourselves on the opposite side of the argument this time. You make a statement that I hope is an overstatement, where in your written testimony you say that repealing the PATRIOT Act would honor what the Americans who fought in the Civil War begot. Do you really favor repealing the entire PATRIOT Act, even that section which dismantled the so-called wall between law enforcement intelligence that the 9/11 Commission indicated was one of the major vulnerabilities that we had, and one of the reasons why we could not connect the dots so that we might be able to prevent the kind of attacks that we saw on 9/11?

Mr. FEIN. I believe that the 9/11 Commission concluded that the 9/11 abominations would have been thwarted if the so-called wall of separation had been absent. And I believe Jamie Gorelick, who was on the 9/11 Commission, who was deputy attorney general, I believe, when the alleged wall of separation was erected, denied that there really was that wall. And I do not believe that in passing the USA PATRIOT Act, that this Congress made a finding that if the wall was not erected, 9/11 would not have occurred.

Mr. LUNGREN. My question, though, is do you really favor repealing the entire PATRIOT Act?

Mr. FEIN. What I stated in the testimony, Mr. Congressman, was that the burden is on the government in this country to demonstrate the need and urgency to compromise the customary probable cause to suspect crime to endow government with authority——

Mr. LUNGREN. So, you think the probable cause to suspect a crime is sufficient to give us the kind of information necessary to find out about the possibility of a terrorist act and thwart it before it is carried out. You think the criminal law intelligence, criminal law procedures that we have talked about are sufficient to do that?

Mr. FEIN. I believe the Constitution places the burden on government, when it wants to encroach on liberties to be justified.

Mr. LUNGREN. No, I understand that. But what I am saying——

Mr. FEIN. And so, the burden——

Mr. LUNGREN [continuing]. Are you telling us what we have are sufficient to thwart terrorist attacks as opposed to gathering the evidence after in fact is has occurred to be able to convict those who may be involved in it?

Mr. FEIN. Well, first of all, you can gather evidence before any attack has concurred under the conspiracy laws. As you well know, conspiracy can reach before you come close to even getting that attempt.

Secondly, I have stated that if this Committee can establish by empirical evidence, make a finding that these powers are indispensable to preventing a terrorist attack, then you have a justification for breaching the wall. But I do not have——

Mr. LUNGREN. Okay. So, do you have confidence in this Committee that we could make such a finding?

Mr. FEIN. Ordinarily findings should not be made out of trifles lai desaire, meaning you have got to define based upon evidence——

Mr. LUNGREN. Well, I guess your answer is no. I guess you do not trust us to be able to make that finding.

Mr. FEIN. No, I expect there to be empirical evidence with the experts who would state, yes, if we had this power, this particular investigation would have reached fruition and then blocked a terrorism act, and otherwise could not have happened.

Mr. LUNGREN. Well, the predicate——

Mr. FEIN. Those decisions are made all the time.

Mr. LUNGREN. The predicate for wiretaps is not that a crime is being committed, but that surveillance is necessary because the person to be surveilled is a foreign power or agent of a foreign power. It does not mean that they are involved in a crime at that point in time? Do you not think that is a sufficient basis for being able to have a wiretap?

Mr. FEIN. I think that Title III does require suspicion of implication in crime, and I think that ought to be the standard.

Mr. LUNGREN. So——

Mr. FEIN. That is the standard that Harlan Fiske Stone, Chief Justice——

Mr. LUNGREN. I understand.

Mr. FEIN [continuing]. And former attorney general adopted for the——

Mr. LUNGREN. So, you are saying that we do not have the right to spy on foreign powers in our own country unless we have evidence that they are about to ready to commit a criminal act.

Mr. FEIN. Now, if you are spying on citizens on the United States or people that are here lawfully, that is one thing. It is something else if you are spying on diplomats who are involved in embassies or otherwise. They are not loyal to the United States. They do not have the same protection.

Mr. LUNGREN. And the definition of a U.S. person in this Act is, someone who is a citizen or someone who is a permanent resident alien. Other people are allowed under this, but those are not.

Mr. Mullins, you have had more than a slight participation in the criminal justice system. Are you satisfied that the criminal tools that are available to law enforcement are sufficient that we do not the PATRIOT Act in our anti-terrorism efforts?

Mr. MULLINS. Not at all.

Mr. LUNGREN. Well, why is that? I mean, you use that every day. If I listen to Mr. Barr and Mr. Fein, you should be very satisfied. You guys are professional. You know what you are doing. You have

been able to do a great job in the city that you represent. Why do we need this?

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

The gentleman from Michigan, Mr. Conyers?

Mr. CONYERS. Thank you. This is a quite interesting discussion because what we are exchanging views on is whether the failure of 9/11 was a failure of intelligence analysis or law enforcement. And I hear Members on the Committee claiming that law enforcement dropped the ball and that is how it happened. But I think that it was failure of intelligence, and I would like you two to comment on it, because since 9/11, of course, we have reorganized our whole Federal law enforcement, given the FBI, for example, the mission of preventing terrorism. And so, the failure of 9/11 was in one sense a failure to connect the dots. It was a failure to use the information that we had. And I would like you to expand on that.

Mr. FEIN. Representative Conyers, I do not know whether I would be all that critical of the intelligence people. They make errors make from time to time. 9/11 was unprecedented in many ways. People did not think that that kind of dastardly abomination would be plausible, but certainly think, and I think Mr. Barr mentioned, that Mr. Moussaoui, the 20th hijacker, there was clearly probable cause to search his computer that could have uncovered the plot, and simply was not exercised on that score.

And with regard, I think, to the general idea that anything that makes it easier to thwart terrorism is justified, then you might as well say, go into anybody's home and spy whenever you want. And if the question is, DoE sit make it more likely for us to thwart terrorism, the answer is yes, but it destroys the country that we know and we fought to maintain as a country give to freedom rather than national security.

Mr. BARR. I would say probably, not to coin a phrase, but what happened in the lead up to 9/11 was probably a perfect storm of failures. I do not think that it was, nor is it the case today, that these terrorists are all rocket scientists, and know exactly what they are doing, and never make mistakes.

They got very lucky on 9/11. There were numerous opportunities, from enforcing our immigration laws to enforcing the laws requiring and establishing security at airports, to laws allowing the government to access computers, that were simply not exercised by the government at all levels, state government as well as Federal Government. There were licenses that were obtained, driver's licenses based on false pretenses and false information that were never checked out. There were immigration statuses that were overstayed that the Federal Government did not enforce. There were not proper steps taken to search the baggage and so forth. And the 20th hijacker did not have his computer access, which the government could have. There was authority to do that. Yet, I do not recall, and maybe the Chairman does, but I do not recall that the post-9/11 hearings that we had leading up to the PATRIOT Act, any government witnesses coming in and saying they had made a mistake. They all paraded in here and said, oh, we did not have enough authority. We did not have enough money. Give us more authority, give us more money, rather than address the mistakes that had been made by failing to use existing powers.

Mr. CONYERS. I ask unanimous consent to put in a New York Times story that said that the leaders—"Bush Was Warned Bin Laden Wanted to Hijack Planes."

Mr. SENSENBRENNER. Without objection.

[The information referred to follows:]

The New York Times **Archives**

BUSH WAS WARNED BIN LADEN WANTED TO HIJACK PLANES

By DAVID E. SANGER
Published: May 16, 2002

The White House said tonight that President Bush had been warned by American intelligence agencies in early August that Osama bin Laden was seeking to hijack aircraft but that the warnings did not contemplate the possibility that the hijackers would turn the planes into guided missiles for a terrorist attack.

"It is widely known that we had information that bin Laden wanted to attack the United States or United States interests abroad," Ari Fleischer, the president's press secretary, said this evening. "The president was also provided information about bin Laden wanting to engage in hijacking in the traditional pre-9/11 sense, not for the use of suicide bombing, not for the use of an airplane as a missile."

Nonetheless the revelation by the White House, made in response to a report about the intelligence warning this evening on CBS News, is bound to fuel Congressional demands for a deeper investigation into why American intelligence agencies and the Federal Bureau of Investigation had failed to put together individual pieces of evidence that, in retrospect, now seem to suggest what was coming.

In the past few days, government officials have acknowledged for the first time that an F.B.I. agent in Phoenix had urged the F.B.I. headquarters to investigate Middle Eastern men enrolled in American flight schools. That memorandum also cited Mr. bin Laden by name and suggested that his followers could use the schools to train for terror operations, officials who have seen the memorandum said.

Administration officials reached this evening said the warning given to Mr. Bush did not come from the F.B.I. or from the information developed by the Phoenix agent. Instead, it was provided as part of the C.I.A. briefing he is given each morning, suggesting that it was probably based on evidence gathered abroad.

The C.I.A. had been listening intently over the July 4 holiday last year, after what one investigator called "a lot of static in the system suggesting something was coming." But then the evidence disappeared as quickly as it had arisen, and by August, officials have said, little was heard from Al Qaeda.

The warning of the hijacking was given to the president at his ranch in Crawford, Tex., where he was on vacation.

Taken together, the news of the C.I.A. warning and the information developed separately by the F.B.I. explains Mr. Bush's anger after Sept. 11 that intelligence gathered on American soil and abroad was not being centrally analyzed and that the agencies were not working well together.

Several times he has told audiences that he is working on solving that problem, and these days he is briefed jointly by the F.B.I and the C.I.A., ensuring that each hears information from the other agency.

It was not clear this evening why the White House waited eight months after the terrorist attacks in New York and Washington to reveal what Mr. Bush had been told.

But Mr. Fleischer noted that in the daily flow of intelligence information the president receives, the warning of what appeared to be the threat of a conventional hijacking was not as serious as it appears in retrospect. "We were a peacetime society, and the F.B.I. had a different mission," he said.

Mr. Fleischer said the information given to the president in Texas had prompted the administration to put law enforcement agencies on alert. But there was no public announcement.

Nonetheless, a senior administration official said tonight that there was speculation within the government that heightened security -- if it truly existed in August and September -- might have prompted the hijackers to use box cutters and plastic knives to avoid detection.

The C.I.A. warning might also explain why Mr. Bush's aides were so certain that Mr. bin Laden was behind the attacks almost as soon as they happened. "We never had any real doubt," one senior official involved in the crucial decisions at the White House on Sept. 11 said several months ago.

Until recently, Mr. Bush has deflected demands for a lengthy and detailed investigation into the intelligence failures surrounding the Sept. 11 attacks. White House officials were concerned that the investigation would feed into demands by Senator Richard C. Shelby, the Alabama Republican who is the vice chairman of the Senate Intelligence Committee, for the replacement of George J. Tenet as director of central

intelligence.

But the news that the hijacking warning was in the president's brief, which Mr. Tenet sees and approves, and that it was linked to Mr. bin Laden is almost certain to widen the scope of the investigation.

Already, several lawmakers who have read the Phoenix memorandum written by the F.B.I. agent have described it as the most significant document to emerge in Congressional inquiries into whether the government might have been warned about possible hijackings.

Now those investigators are almost certain to demand the details of the president's August briefing by the C.I.A. and may ask to hear about how that evidence was developed.

Home : Times topics : Member Center

Copyright 2011 The New York Times Company : Privacy Policy : Help | Contact Us | Work for Us : Site Map : Index by Keyword

---

Mr. CONYERS. Thanks, sir. And another one from the Washington Post, the heading, "Two Months Before 9/11, an Urgent Warning To Rice."

Mr. SENSENBRENNER. Without objection.

[The information referred to follows:]

The Washington Post

Two Months Before 9/11, an Urgent Warning to Rice

Sunday, October 1, 2006

On July 10, 2001, two months before the attacks on the World Trade Center and the Pentagon, then-CIA Director George J. Tenet met with his counterterrorism chief, J. Cofer Black, at CIA headquarters to review the latest on Osama bin Laden and his al-Qaeda terrorist organization. Black laid out the case, consisting of communications intercepts and other top-secret intelligence showing the increasing likelihood that al-Qaeda would soon attack the United States. It was a mass of fragments and dots that nonetheless made a compelling case, so compelling to Tenet that he decided he and Black should go to the White House immediately.

Tenet called Condoleezza Rice, then national security adviser, from the car and said he needed to see her right away. There was no practical way she could refuse such a request from the CIA director.

For months, Tenet had been pressing Rice to set a clear counterterrorism policy, including specific presidential orders called "findings" that would give the CIA stronger authority to conduct covert action against bin Laden. Perhaps a dramatic appearance -- Black called it an "out of cycle" session, beyond Tenet's regular weekly meeting with Rice -- would get her attention.

Tenet had been losing sleep over the recent intelligence he'd seen. There was no conclusive, smoking-gun intelligence, but there was such a huge volume of data that an intelligence officer's instinct strongly suggested that something was coming. He and Black hoped to convey the depth of their anxiety and get Rice to kick-start the government into immediate action.

He did not know when, where or how, but Tenet felt there was too much noise in the intelligence systems. Two weeks earlier, he had told Richard A. Clarke, the National Security Council's counterterrorism director: "It's my sixth sense, but I feel it coming. This is going to be the big one."

But Tenet had been having difficulty getting traction on an immediate bin Laden action plan, in part because Defense Secretary Donald H. Rumsfeld had questioned all the National Security Agency intercepts and other intelligence. Could all this be a grand deception? Rumsfeld had asked. Perhaps it was a plan to measure U.S. reactions and defenses.

Tenet had the NSA review all the intercepts, and the agency concluded they were of genuine al-Qaeda communications. On June 30, a top-secret senior executive intelligence brief contained an article headlined "Bin Laden Threats Are Real."

Tenet hoped his abrupt request for an immediate meeting would shake Rice. He and Black, a veteran covert operator, had two main points when they met with her. First, al-Qaeda was going to attack

American interests, possibly in the United States itself. Black emphasized that this amounted to a strategic warning, meaning the problem was so serious that it required an overall plan and strategy. Second, this was a major foreign policy problem that needed to be addressed immediately. They needed to take action that moment -- covert, military, whatever -- to thwart bin Laden.

The United States had human and technical sources, and all the intelligence was consistent, the two men told Rice. Black acknowledged that some of it was uncertain "voodoo" but said it was often this voodoo that was the best indicator.

Tenet and Black felt they were not getting through to Rice. She was polite, but they felt the brush-off. President Bush had said he didn't want to swat at flies.

As they all knew, a coherent plan for covert action against bin Laden was in the pipeline, but it would take some time. In recent closed-door meetings the entire National Security Council apparatus had been considering action against bin Laden, including using a new secret weapon: the Predator unmanned aerial vehicle, or drone, that could fire Hellfire missiles to kill him or his lieutenants. It looked like a possible solution, but there was a raging debate between the CIA and the Pentagon about who would pay for it and who would have authority to shoot.

Besides, Rice seemed focused on other administration priorities, especially the ballistic missile defense system that Bush had campaigned on. She was in a different place.

Tenet left the meeting feeling frustrated. Though Rice had given them a fair hearing, no immediate action meant great risk. Black felt the decision to just keep planning was a sustained policy failure. Rice and the Bush team had been in hibernation too long. "Adults should not have a system like this," he said later.

The July 10 meeting between Tenet, Black and Rice went unmentioned in the various reports of investigations into the Sept. 11 attacks, but it stood out in the minds of Tenet and Black as the starkest warning they had given the White House on bin Laden and al-Qaeda. Though the investigators had access to all the paperwork on the meeting, Black felt there were things the commissions wanted to know about and things they didn't want to know about.

Philip D. Zelikow, the aggressive executive director of the Sept. 11 commission and a University of Virginia professor who had co-authored a book with Rice on Germany, knew something about the July 10 meeting, but it was not clear to him what immediate action really would have meant. In 2005 Rice hired Zelikow as a top aide at the State Department.

Afterward, Tenet looked back on the meeting with Rice as a tremendous lost opportunity to prevent or disrupt the Sept. 11 attacks. Rice could have gotten through to Bush on the threat, but she just didn't get it in time, Tenet thought. He felt that he had done his job and had been very direct about the threat, but that Rice had not moved quickly. He felt she was not organized and did not push people, as he tried to do at the CIA.

Black later said, "The only thing we didn't do was pull the trigger to the gun we were holding to her head."

Editor's Note: How much effort the Bush administration made in going after Osama bin Laden before the attacks of Sept. 11, 2001, became an issue last week after former president Bill Clinton accused President Bush's "neocons" and other Republicans of ignoring bin Laden until the attacks. Rice responded in an interview that "what we did in the eight months was at least as aggressive as

what the Clinton administration did in the preceding years."

View all comments that have been posted about this article.

© 2006 The Washington Post Company

Sponsored Links

57 Year Old Mom Looks 27!
Mom Reveals $5 Wrinkle Trick That Has Angered Doctors!
FDXNews8.com

Hot Stock Pick - OBJE
New Issue, Obscene Jeans Inc Explosive Investment Potential
www.ObsceneJeans.com

AndroidT is Affordable
Great deals on AT&T Android phones!
www.wireless.att.com

Buy a link here

Mr. CONYERS. Thank you again.

Now, I want to dispel this misunderstanding that some Members seem to be articulating up here. This is not about a hearing of whether we have no PATRIOT Act or we continue the same PATRIOT Act. I want to make that clear. This is about how we improve the PATRIOT Act, and that is why I have a compromise bill that I strongly suggest that we try to have some hearings on. We are not having hearings on the bill itself. This a hearing called "Dispelling the Myths." That is not a hearing, and I insist that——

Mr. SENSENBRENNER. The gentleman's time has expired. The gentleman from Michigan knows full well that the Committee Rules require advance notice of hearings so that everybody can be prepared, and he dropped his bill last night, which was well after the time deadline that was required for a hearing today. And the full committee Chair has scheduled a markup tomorrow. So, I think the gentleman is a little bit too late in meeting deadlines of rules that everybody knows.

The Chair now recognizes——

Mr. CONYERS. Would the Chairman allow me 30 seconds?

Mr. SENSENBRENNER. Certainly, without objection?

Mr. CONYERS. You dropped your bill Friday.

Mr. SENSENBRENNER. Mm-hmm.

Mr. CONYERS. I guess that makes your bill okay and my bill too late.

Mr. SENSENBRENNER. My bill was dropped in time for the full Committee Chair to notice the bill for a markup tomorrow, so we complied with the rules on that. And everybody has now had 5 days to see what was in the legislation that I dropped. You dropped yours last night. You did not see me on the floor. You did not see the gentleman from Texas, Mr. Smith, the full Committee Chair, on the floor. So, we got here today to find out that you dropped your bill, and we found out a couple of hours before this hearing.

The gentleman from Florida, Ms. Adams?

Ms. ADAMS. Thank you, Mr. Chair. I will yield my time to the gentleman from South Carolina.

Mr. SENSENBRENNER. Okay. The gentleman from South Carolina is next up on the Republican side. Without objection, the Chair will recognize the gentleman from South Carolina, Mr. Gowdy, for 10 minutes?

Mr. GOWDY. Thank you, Mr. Chairman, and I want to thank the gentle lady from Florida for yielding and also for her service as a distinguished law enforcement officer prior to coming to Congress.

Mr. Fein, I want to be very, very clear about this. I do not and have never challenged the patriotism of anyone who holds a contrary viewpoint on this Act. In fact, I applaud you for probing and questioning and challenging. And I would hope in that spirit that you would also help those of us who have a contrary view on the constitutionality of this Act to beat back the rhetoric, to instruct it with fact. And when I read that this hearing is about national security letters, or jackbooted thuggery, or sneak and peak search warrants when it demonstrably false, just as I would rise in defense of your patriotism, I would hope that you would rise in defense of the truth about what these hearings are about.

And as you mentioned, the spirit of the Fourth Amendment, that is the conversation I would like to have with you, one grounded in civility, but one about the depth and breadth and spirit of the Fourth Amendment. Fair enough?

Mr. FEIN. That is fair enough.

Mr. GOWDY. All right. You mentioned in your testimony, and I will quote, "Government in the United States has no business collecting or retaining information about citizens without probable cause to believe that crime has been or will be committed." So, you

allow that there needs to be government involvement in the investigation of future crimes.

Mr. FEIN. Yes, conspiracy is a perfect example, yes, sir.

Mr. GOWDY. Right, and there are other examples. I mean, you cannot wait until something happens to begin to investigate.

Mr. FEIN. Well, that is what conspiracy law is about. Conspiracy means nothing has happened; you just have an agreement, and you can investigate the agreement to commit an unlawful act, and that is permissible.

Mr. GOWDY. Well, the difference is, in a conspiracy case, nothing ever has to happen. It is a crime just to conspire to commit an offense. You can have conspiracies all day long and not ever have a crime. Agreed?

Mr. FEIN. Well——

Mr. GOWDY. I mean, there does not have to be——

Mr. FEIN [continuing]. Some conspiracies you do not need any overt action.

Mr. GOWDY. You need no overt action Title XXI conspiracy.

Mr.. Fein. You can go ahead and prosecute, but all I am saying is that you can begin an investigation before anything happens under the criminal law.

Mr. GOWDY. Agreed, but you used the word probable cause in that sentence. And then in another sentence you said the whole purpose of the Fourth Amendment is to saddle government with a heavy burden of demonstrating by indisputable evidence. Now, you would agree with me, Mr. Fein, that is not the standard. Indisputable evidence is not the standard by which the Fourth Amendment is judged.

Mr. FEIN. Indisputable evidence that the inquiry would produce is focused on somebody who is probably implicated in crime or the evidence unearthed would shed light on a crime.

Mr. GOWDY. Well, the word "indisputable" and "probably" do not fit nicely in the same sentence. What is your definition of probable cause?

Mr. FEIN. The one that the U.S. Supreme Court has said you have got some reasonable foundation and suspicion that ordinary people applying their intellect would conclude makes it substantially likely that the individual is engaged in crime.

Mr. GOWDY. It is a fair probability, right?

Mr. FEIN. Fair probability, yes.

Mr. GOWDY. That is what the Supreme Court said, and that is very different from indisputable evidence.

Mr. FEIN. Yes, but I believe my statement with regard to indisputable evidence is indisputable showing that this particular investigatory tool is necessary to investigate crime under those standards, not the standard for getting a warrant.

Mr. GOWDY. But you will agree with me that there are several areas of criminal law where the standard is not probable cause. You do not have to have probable cause for a terry-like encounter with law enforcement. You have a distinguished law enforcement officer right beside you. If there were to be a police citizen encounter on the street, he does not have to have probable cause to frisk me for weapons, right?

Mr. FEIN. And that is not viewed as a search. It is a stop and frisk.

Mr. GOWDY. Well, you can remove weapons and contraband from their hand or from their pocket under another exception to the Fourth Amendment, which is the Plain Feel Doctrine. Do you agree or disagree with the Plain Feel Doctrine?

Mr. FEIN. No. The Plain Feel is you have got plain evidence that a crime or contraband is in your vision.

Mr. GOWDY. But you do not have a warrant.

Mr. FEIN [continuing]. Probable cause. No, I am not saying—probable cause does not mean you have to get a warrant in every circumstance. Sometimes you can act without a warrant, but you would have to establish probable cause if it were challenged after the fact.

Mr. GOWDY. And you will agree that there are areas of criminal law where well before the PATRIOT Act, all you had to have was a reasonable suspicion or an articulable suspicion, or, in some instances, just a hunch.

Mr. FEIN. With regard to full scale searches and seizures, no, sir, I do not believe that is the law.

Mr. GOWDY. Well, but then we get into a discussion of what is a full scale search and seizure. Can I put a tracking device on an automobile?

Mr. FEIN. I think that is in dispute now, depending upon whether the tracking device is there 24 hours a day. I believe that case is just in the U.S. Court of Appeals for the District of Columbia.

Mr. GOWDY. But there are courts of appeals, including the 4th Circuit, which have said you can put electronic tracking devices on automobiles, right?

Mr. FEIN. Yes, there are, and they may be wrong.

Mr. GOWDY. They may be, but what if they find out in 10 years we are all wrong?

Mr. FEIN. You have an independent judgment to make as well. The Olmstead case in 1928 said wiretaps are free, that you do not have to have any cause whatsoever, and it was overruled 3o9 years later.

Mr. GOWDY. Right.

Mr. FEIN. And this body has a tradition of looking at court decisions and maybe overruling them. They did that with regard to Korematsu and Haribiyashi when they enacted the Civil Liberties Act.

Mr. GOWDY. We are having a hard time getting the laws we have passed enforced right now with respect. This executive branch does not enforce the laws we do pass, so the notion that we are going to foresee——

Let me ask you this. Do you agree that law enforcement should be able to search the computer records of a suspected child pornographer who uses a taxpayer funded computer at a public library?

Mr. FEIN. If it satisfies probable cause, they will come up with evidence of crime. Of course, yes.

Mr. GOWDY. They have no—well, it does not have to be probable cause. An assistant United States attorney can send a subpoena, right? You do not have to have a search warrant.

Mr. FEIN. I am talking about probable cause. If it just——

Mr. GOWDY. I know you are talking about probable cause, but what I am trying to establish is there is a rich jurisprudence in this country where probable cause is not the only standard. An assistant United States attorney can send a grand jury subpoena to a library and get your library records today, correct?

Mr. FEIN. That is correct because the Supreme Court, and I think they got it wrong, says that if the information is in the hands of a third party, then you have no protectable——

Mr. GOWDY. You have no understanding.

Mr. FEIN [continuing]. Reasonable expectation—yeah.

Mr. GOWDY. You have no expectation of privacy.

Mr. FEIN. I believe that is an incorrect interpretation of the Fourth Amendment. In today's Internet era, you can have your virtual digital diary of everything you have done tracked in the hands of third parties, and that doctrine enables then the government to find—really look in your diary——

Mr. GOWDY. Or you can be on notice that the law is what it is and not keep things that you have an expectation of privacy——

Mr. FEIN. I think if you are an American, you are endowed with liberty, and the burden is on the government to overcome your right to be left alone, not the other way around.

Mr. GOWDY. You think that you are endowed with the liberty to use a taxpayer funded computer at a taxpayer funded library and search for child pornography, and have standing to contest whether or not the government can get those records.

Mr. FEIN. If the government is providing it and they place certain conditions that the government places certain conditions on use, that may be different because you are then given alert that you are using government property. It is like if you are living in government operated house, they may say, well, then you are going to be searched to make sure you do not have guns or something in there. So, that changes——

Mr. GOWDY. Well, that raises a wonderful point. Would you agree with me that as a condition of probation, the government can say we have the right to search you when we want to? As a condition of parole or probation, you consent to be searched.

Mr. FEIN. If they wish to—if you have already established that they violated the law, this is a privilege they have got now to go out on probation. The government can set those conditions.

Mr. GOWDY. Well, wait a minute. You have already served your debt to society.

Mr. FEIN. Well, with regard to parole, I am not sure——

Mr. GOWDY. Or probation. There is no parole in the Federal system.

Mr. FEIN [continuing]. That if you violate the conditions of parole, you return to——

Mr. GOWDY. Could we make it a condition on admittance to this country that you consent to be searched?

Mr. FEIN. If you are not a U.S. citizen, that is——

Mr. GOWDY. So, you do not have a problem with that.

Mr. FEIN. The rule on border searches is that you do not have to—yeah, you do not cause whatsoever. It is an exception to the Fourth Amendment.

Mr. GOWDY. Border searches, probation searches. So, there has already been an erosion in your judgment of the probable cause standard, the warrant standard, of the Fourth Amendment.

Mr. FEIN. In very narrow circumstances, yes.

Mr. GOWDY. All right. Do you disagree with the lawfulness of anticipatory search warrants?

Mr. FEIN. Of what search warrants?

Mr. GOWDY. Anticipatory. The crime has not even been committed yet, but law enforcement can go get a search warrant for that crime.

Mr. FEIN. Well, as I say, if there is a conspiracy and there is suspicion——

Mr. GOWDY. Not a conspiracy case.

Mr. FEIN. No, I do not believe that you should just go out and be able to spy on citizens because of somebody's individual hunch.

Mr. GOWDY. Not a spy.

Mr. FEIN. Hey, maybe it will come out.

Mr. GOWDY. It is not a spy. It is an undercover case where somebody has ordered contraband, and it is going to be delivered to their home. So, you go get a search warrant in anticipation of delivery. The crime has not been committed yet.

Mr. FEIN. No, if the search warrant is based upon probable cause to believe you will uncover evidence of crimes, of course you can do that.

Mr. GOWDY. So, again, the strictures of the Fourth Amendment do not require a warrant before every arrest, agreed?

Mr. FEIN. Right. Probable cause is different than a warrant.

Mr. GOWDY. And they do not require a warrant for all searches, agreed?

Mr. FEIN. Right, but they may require probable cause if——

Mr. SENSENBRENNER. The time of the gentleman has expired. The gentlewoman from California, Ms. Chu?

Ms. CHU. Thank you, Mr. Chair.

I would like to ask Mr. Fein, pertaining to the business records provision and gag orders, we know that secrecy is essential when conducting any intelligence investigation. But Section 215 orders come armed with significant gag orders that are the subject of the order from discussing it with anyone. In fact, you have to wait an entire year before you can even challenge the gag order in court. And uninformed person might not even know that they actually challenge it, or how to it.

Judicial review is the essential mechanism that we arm citizens with to ensure that they can protect their rights, but under the PATRIOT Act it is practically impossible to bring these cases to court.

How can we change the rules? What would be your recommendation with regard to changing the rules surrounding gag orders to more adequately provide innocent Americans with an avenue to challenge them in court?

Mr. FEIN. Well, I would authorize them certainly to consult with lawyers and to bring court challenges without waiting, because 1 year all sorts of damage could happen in the interim, because I believe that the PATRIOT Act, again, is premised largely on the idea that government generally never gets it wrong, and the burden is on the citizen to establish their right to be free from government

snooping rather than the burden on the government to say, why are you crossing the threshold of the citizen.

And certainly there have been instances where the gag orders were challenged. A couple of cases held that they were unconstitutional because they interfered with the due process right to challenge an alleged violation of the law. And I do not believe that there is any demonstration. In some of these instances when the gag orders were lifted, the FBI just dropped the investigation without showing that we had a terrorism crime that ensued because there wasn't that particular authority to keep the entire matter under wraps, if you will. And I think that anyone who receives some government issued document should have a right to go into court and challenge its legality. That is what the rule of law is about.

Ms. CHU. You mean immediately without having to wait a year.

Mr. FEIN. Correct.

Ms. CHU. And also you discussed the fact that subjects are frequently kept in the dark when they are the subject of these investigations because much of the information is requested directly from third parties, such as telecommunication companies or Internet service providers. And not only is the subject never told that their information is being shared with the government, the third parties hardly ever have any incentive to even question the government's actions. In fact, the legal costs for those third parties are a strong barrier, and they find that it is just easier for them to cooperate.

This essentially allows the government to compile information regarding individuals without notice, providing they claim it as relevant to a national security investigation.

Should the government be required to give notice to the subjects of these investigations?

Mr. FEIN. Yes. I believe that is true, and I believe in other circumstances, for instance when there are tax investigations or the Bank Privacy Act, Congress went out of its way and, by statute, did allow in limited circumstances the target of the investigation to be notified, even though the target was not specifically the recipient of the subpoena or for the investigative demand. And it seems to me more, rather than less, urgent today to do that because so much of the data about any individual in the hands of third party Internet service providers. It is hard to suggest that you volunteer information on the Internet. It is hard to even run or live today without having huge stores of information on the Internet.

And without being cynical, you are exactly right. The incentive of the provider of the information is to cooperate. They are regulated by the government. They have huge amounts of contracts. I think we discovered that with regard to the cooperation of the telephone companies concerning the President's terrorist surveillance program, and they were eager. We will give you all of our phone records even without asking for an attorney general assertion that this is constitutionally mandated because they have got $10, $20 billion contracts with the Defense Department, and you cannot expect them—they are out for their interests—to defend the third party target of the investigation.

Ms. CHU. Mr. Barr, I wanted to ask a question about oversight. At the end of last month, the Department of Justice submitted an annual report that Congress had detailed a number of times that the government want FISA support authority to conduct secret electronic surveillance for access to certain business records and the number of national security letters. And this report found out that the government used these special tools much more often than in the past years. For instance, they made 96 applications for access to business records for foreign intelligence purpose, and that is five times more than the year before. And the FBI used national security letters to get information on over 14,000 different U.S. persons; that is over double the individuals of the year before.

I am greatly concerned about the increase in government access to personal information without the proper checks and balances. And we know that there have been times when the FBI has abused this——

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

Gentleman from Virginia, Mr. Goodlatte?

Mr. GOODLATTE. Thank you, Mr. Chairman. Thank you for holding this hearing, and I want to thank all the panelists for their contribution.

I want to start out, Mr. Rowan, and ask you to comment on what I think is the core point that Mr. Barr and Mr. Fein have made here. And that is that with regard to the business records provision, that there needs to be illegal activity or a known terrorist, that somehow this legislation has broken the link between the right to privacy and the requirement that the government show a reasonable suspicion before being able to examine these third party held business records. I wonder if you would comment on that.

Mr. ROWAN. Well, I think that, first of all, there is a standard in there. A statement of facts needs to be submitted to a judge showing that there are reasonable grounds to believe that the——

Mr. GOODLATTE. So, to be clear. No one is looking at anybody's business records without a judge first saying they are going to be able to do so. Is that correct?

Mr. ROWAN. Right. And, again, from the perspective of somebody who knows how Federal criminal law enforcement investigations go, this is an extraordinary bar. The director of the FBI and the attorney general or his designate are signing off on these applications. This is such a more stringent mechanism in place——

Mr. GOODLATTE. So, in order to look at somebody's business records, the top level people in our law enforcement agencies are having to approve this.

Mr. ROWAN. That is right. These are being treated with the same set of protections as a request for electronic surveillance under FISA. And there is an application made to an Article III judge sitting on a FISA court who is going to determine whether or not the standard has been met.

The standard is, relatively speaking to electronic surveillance, it is lower, but it needs to be lower because——

Mr. GOODLATTE. I understand there three categories it has to fit into—foreign intelligence investigation—not just a whim, but there is an actual investigation that this will be a part of—international

terrorism or clandestine intelligence activity, all under Section 501(a). Is that correct?

Mr. ROWAN. That is correct.

Mr. GOODLATTE. And then the court that this is brought to has to make a number of specific findings before one can look at one's business records. And these are not business records held by the individual; these are, as have been discussed here, business records held by a third party.

Mr. ROWAN. That is right, and keep in mind that in addition to making those findings, the court is imposing minimization procedures on the government effectively telling the government, if and when you get these records, you need to take great care in how you handle them. You need to determine whether or not they are in fact intelligence information before you disseminate them. And, moreover, there is going to be at the end of the year or whenever it is appropriate, there is going to be a report made to the Congress that is going to list this particular order as one of those that was secured during the year. So——

Mr. GOODLATTE. Now, let me interrupt you. Mr. Fein has said in his testimony that every provision of the PATRIOT Act should be repealed unless the government can prove that, "but for the authority," an act of international terrorism would have succeeded. That is a pretty high standard to meet in terms of trying to look forward to prevent something like 9/11 happening again, because it will not happen exactly the same as it happened previously.

So, let me ask you. Are you confident that the PATRIOT Act has helped to thwart acts of international terrorism since its enactment in 2001?

Mr. ROWAN. Yes, I am.

Mr. GOODLATTE. And in September 2004 before the Senate Judiciary Committee, former Congressman Barr, my former colleague and friend, and hopefully still a current friend, stated that a Federal agent could randomly wiretap an entire apartment complex. Is there any legal authority in the PATRIOT Act or in the U.S. Code anywhere that would authorize a court to authorize such a wiretap?

Mr. ROWAN. No.

Mr. GOODLATTE. And in your experience, have you ever heard of such a wiretap taking place?

Mr. ROWAN. No.

Mr. GOODLATTE. Sergeant Mullins, in your experience, do your Federal law enforcement counterparts exercise care, restraint, and discretion in the exercise of PATRIOT Act provisions?

Mr. MULLINS. Yes.

Mr. GOODLATTE. Do you want to elaborate?

Mr. MULLINS. Well, to my understanding, there has been approximately 32 events to which terrorist acts were about to inflicted upon Americans here in this country. And those events were prevented as a result of the intelligence that was gathered by Federal authorities. And to date, again, my understanding, there has been no Supreme Court decisions, no major court cases that have challenged that.

Mr. GOODLATTE. Thank you.

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

The gentleman from Arizona, Mr. Quayle?

Mr. QUAYLE. Thank you, Mr. Chairman, and thanks to all the witnesses for being here today.

Mr. Fein, I enjoyed your constitutional back and forth with Mr. Gowdy, and obviously there is a differing of opinion between the constitutionality of the PATRIOT Act. But aside from the constitutionality, we just have to decide, even if we stipulate that it is constitutional, I mean, the Constitution is a set of rights that cannot be trampled on by the majority. So, even if you stipulate that it is constitutional, you still have to figure out whether it is the right thing to do.

Mr. FEIN. Correct.

Mr. QUAYLE. And I think that that sometimes is lost in this argument when people continue to say this is constitutional, so it is constitutional, so it is okay to do. And I just wanted to say that at the beginning because there are some concerns that I have.

And, Mr. Rowan, one of the things that I want to just get some clarification on, when you are talking about the grand jury subpoenas that you had issued, and you said that they were obviously issued without any court order and without any judicial oversight, was that with a criminal investigation to a crime that already occurred, or was it something that was to try to prevent a crime from occurring in the future?

Mr. ROWAN. Well, it would certainly be in the context of either historical criminal activity or ongoing criminal activity. As Mr. Fein has pointed out, you know, the conspiracy law is broad, and you can be investigating a series of activities, including what you think is going to happen in the future, in the context of a grand jury investigation because you can identify somewhere in there an offense that is going on at the time.

Mr. QUAYLE. Okay. And one thing that I was just wondering is, with the Foreign Intelligence Surveillance Act of 1978, they required specific and articulable facts. Why do you think it is imperative to have that removed from that level of relevancy and actually having to be able to state, these are the facts that show the reasonable grounds to go and get the business records of an individual or to have a surveillance?

Mr. ROWAN. Well, I think there are two different things here. I think that the factual showing that needs to be made for electronic surveillance is higher in FISA than it is for business records, and that is appropriate because it is far more intrusive than going after third party documents.

With respect to Section 215, the business records provision, if you are going to ask the FBI to do a lengthy factual narrative of why they want these third party records, there is a huge disincentive for the FBI to pursue that because it is a time consuming activity. Remember, these orders are written by an agent in Phoenix, who then forwards it to his supervisor, who forwards it to Washington, who takes it to the Justice Department. And the Justice Department and the FBI headquarters work on it together, and then they eventually say, this is good enough that it can be signed by the director of the FBI and the attorney general and sent to a Federal judge. All that takes time, and they can do it very quickly when they have to. And they do it all the time very quickly when

they need to. But when you are asking the agents to get a lengthy factual narrative explaining exactly why you need these records, that is a lot of work to do under circumstances where they have, you know, potentially they may well decide, you know what? I would rather risk exposing my investigation and using a grand jury subpoena because I can get this quickly, and I need to move. I cannot wait to go through everything that you are asking me to go through to meet the standards of a 215 order.

That may not be a good thing, that agents make decisions like that, but I think that is the real world of conducting national security investigations.

Mr. QUAYLE. And I understand that, and I understand the importance of being able to balance and give Federal law enforcement officers and intelligence officers the ability to thwart attacks against the United States. But the one thing that I have been looking and reading about, sometimes when you have laws that are vague or overly broad, it opens up to misuse by various agencies, not to say that it would actually happen, but it actually has the potential to have—when you have vague and overbroad laws. Do you think that that is the case in this instance?

Mr. ROWAN. I understand your general point, but I think that when you consider all the informal and formal executive branch oversight that exists for these orders, that the chances of abuse are far—it is just not very likely, I think, under these circumstances. I mean, if you look back at the history of the business orders, it took the FBI and the DoJ several years to even use this provision because it was new, it was different, it asked them for things they had not been required to do in the past. It took a long time for agents to get comfortable with this approach. And to be blunt, if you raise the bar further in terms of what needs to be provided, it is even harder to see this used in the future.

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

The Vice Chairman of the Committee, the gentleman from Texas, Mr. Gohmert?

Mr. GOHMERT. Thank you, Mr. Chairman, and do appreciate each of you being here and the attention that each of you have given to this subject. Obviously there are differing opinions.

There is no question in my mind, and hopefully in yours, that there are people who are war with us. They have declared war on the United States and on western civilization. They feel like the freedoms we have lead to debauchery and lead to things that can be avoided if you have on religious zealot controlling what people get to do. I do not want to get there. I believe God gave us freedom of choice.

And yet when you are dealing with people at war with you, are often different parts of the Constitution come into play. I have been struck that people demand constitutional rights for people who have declared war against us that actually are not constitutional rights for them at all. The Constitution anticipates that in time of war or in time of peace, our own military will not have the constitutional rights. When I was in the Army, I did not have the constitutional rights everybody else did. That is just all part of the Constitution.

I have been concerned about parts of the PATRIOT Act, but felt that if it were pertaining to foreign non-U.S. citizens and we had some terrific discussions about this back in my first term, '05 and '06. But even then it needed to be properly monitored.

There were a couple of us that really pushed hard, some of us harder than others, but really pushed for having sunsets so we could have this discussion down the road. And I was pleased that we got them in on anything in the House version so that when it got to conference it could still be used.

But as the last 5 years have unfolded, it seems to be that the biggest abuses have not come in 206 or 215, the "Lone-Wolf" provision, but in the national security letters. That is where we had the IG report that was just devastating of how abusive that has been. And that is not something that is up for renewal, but I have concerns if maybe we ought to slide the NSL authority under the business records provision. I am just uncomfortable after we saw how easily abused that could be.

I think because of some of the presentations some have made in public that America is confused about the report of the national security letter abuses, which have not been similarly abused that I can find under 215 or 206.

So, I am curious. I asked in a prior hearing if one proponent against NSLs, if he wanted to see them disappear because I was entertaining that, and he said, oh, no, I do not think so.

How would you feel if NSL authority were somehow merged with 215 to at least give some requirement of court authority before you could just send out what basically amounts to a subpoena for records and other things? Yes, sir, Mr. Fein?

Mr. FEIN. Congressman Gohmert, the first thing I would like to do before I get specifically that is read from this statement of the unanimous consent ex parte Milligan about the idea of war changing the constitutional matrix. And this was, of course, after the existence of the republic had been shaken by the Civil War.

Mr. GOHMERT. I understand Milligan, and I understand, and perhaps I did not make myself clear. I am not talking so much in war there are different things that apply to prisoners of war, enemy combatants, and things like that. But I would like to one answer to my question.

Mr. FEIN. I think in one of the prior hearings, it was shown that on a couple of occasions when 215 authority was sought and turned down because the judge thought it was focused on First Amendment activity, the government then went and got national security letters to, in some sense, circumvent the standards of 215. And I do not see any reason why the national security letters seem to me historically the ones that have been most abused. They have the most lax standards administratively. It is not like 215 where you have to get a court involved, just the FBI goes out there and say it is relevant. That covers about everything——

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

And the Chair will clarify is that the national security letters were never a part of the PATRIOT Act.

Mr. GOHMERT. Right.

Mr. SENSENBRENNER. They were originally enacted in 1986 on a bill that was sponsored by Senator Leahy of Vermont and Representative Kastenmeier of Wisconsin.

The Chair now recognizes the gentleman from George, Mr. Johnson?

Mr. JOHNSON. Thank you, Mr. Chairman.

Mr. Bob Barr, we have seen you many times here testifying on behalf of liberty, Fourth Amendment issues particularly. And you know well this area, having served as a U.S. congressman on this Committee for a number of years, and then prior to that as a U.S. attorney down in the northern district of Georgia, where, in my opinion, you exercised prosecutorial authority in a nonpartisan way. And I appreciate your service to the Nation.

I have just a few questions that I would like to ask you. Does a relevance standard impose any real check on the government's ability to secretly collect information about American citizens using Section 215? And cannot a good lawyer almost always come up with a reason why information is relevant?

Mr. BARR. The standard that you refer to is virtually no standard at all. To come before a judge or any other authority and say we need this and you need to issue an order allowing us to access this information because it is relevant to an investigation that we are undertaking, in effect, means absolutely nothing. It is no standard, and it is particularly problematic here because the relevance standard, so to speak, is being used to access information or may be used to access information on individuals with no connection whatsoever to a terrorist, a suspected terrorist, or even an associate of a known terrorist.

Mr. JOHNSON. Well, let me ask you this question. If a terrorist suspect—and before I do that, though, I must point out the fact that as a congressman, you served as a Republican, and now I have not heard you renounce your political leanings, so I assume you are still a Republican with some libertarian leanings. But I will not——

Mr. BAR. Probably a little more than that, but I am here today in a nonpartisan capacity.

Mr. JOHNSON. Well, I do appreciate that, sir.

If a terrorist suspect used a U.S. online dating site and viewed your profile or sent you a message, could the government collect your online dating history or other records about you? And would not such information be relevant to the investigation and possibly even presumptively relevant since it involved contact with a foreign power?

Mr. BARR. I would like to make clear for the record that the congressman is referring to a hypothetical, not a real situation. [Laughter.]

Mr. JOHNSON. Well, I mean, many people use dating services these days. [Laughter.]

Mr. BARR. With that understanding, I think probably in that case, there would be a justification for accessing those records because there would be a link, certainly one that could be dispelled, but certainly a link that would be apparent. You have a known or suspected terrorist communicating with an individual, and that individual may have no connection whatsoever and may be entirely

innocent. But I think in that situation, there probably would be an appropriate justification for the government to look at those records.

Mr. JOHNSON. And what if there was no message at all and there was just a viewing of the records?

Mr. BARR. There was just what?

Mr. JOHNSON. A viewing of the records.

Mr. BARR. Well, that would establish nothing. If an individual just goes online to a dating service, as I understand it—never having used one—they can look at virtually an unlimited number of persons with no connection whatsoever. So, in that situation, there would seem to be no nexus whatsoever that would provide a justification for the government to then look at that other individual and their data.

Mr. JOHNSON. Well, that is kind of using a reasonable standard, but I guess someone could eke out a relevancy purpose.

Mr. SENSENBRENNER. The gentleman's time has expired, and the Chair will observe that the use of dating services, either hypothetically or actually, is not within the purview of this hearing.

So, with that note, I would like to thank all of the witnesses for their testimony today. And 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.

Mr. SENSENBRENNER. Without objection, all Members will have 5 legislative days to submit any additional materials for inclusion in the record.

Also without objection, letters from the Federal Law Enforcement Officers Association, the Sergeants Benevolent Association of New York City, the Society of Former Special Agents of the FBI, the FBI Agents Association, Keep America Safe, the National Association of Assistant United States Attorneys, and the National Fraternal Order of Police in support of the reauthorization of the PATRIOT Act, will be submitted to the record.*

And without objection those three requests are so ordered.

The gentleman——

Mr. BARR. Mr. Chairman, I may have missed the beginning, but might I ask permission to have my entire printed statement made a part of the record?

Mr. SENSENBRENNER. Well, just to make clear, without objection, the printed statements of all four of the witnesses will be made part of the record at the beginning of their testimony.

And if there is no further business to be brought before the Subcommittee, the Subcommittee stands adjourned.

[Whereupon, at 11:53 a.m., the Subcommittee was adjourned.]

*The submissions referred to are located in the Appendix of this hearing record.

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

SHEILA JACKSON LEE
18TH DISTRICT, TEXAS

WASHINGTON OFFICE:
2160 Rayburn House Office Building
Washington, DC 20515
(202) 225-3816

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

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

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

FIFTH WARD OFFICE:
4300 LYONS AVENUE, SUITE 200
HOUSTON, TX 77020
(713) 227-7740

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

COMMITTEES:
JUDICIARY
SUBCOMMITTEES:
COURTS AND COMPETITION POLICY
IMMIGRATION, CITIZENSHIP, REFUGEES, BORDER SECURITY, AND INTERNATIONAL LAW
CRIME, TERRORISM AND HOMELAND SECURITY
CONSTITUTION, CIVIL RIGHTS, AND CIVIL LIBERTIES

HOMELAND SECURITY
SUBCOMMITTEES:
CHAIR
TRANSPORTATION SECURITY AND INFRASTRUCTURE PROTECTION
BORDER, MARITIME, AND GLOBAL COUNTERTERRORISM

FOREIGN AFFAIRS
SUBCOMMITTEES:
AFRICA AND GLOBAL HEALTH
MIDDLE EAST AND SOUTH ASIA
TERRORISM, NONPROLIFERATION, AND TRADE

SENIOR WHIP
DEMOCRATIC CAUCUS

SENIOR WHIP
DEMOCRATIC CAUCUS

CONGRESSWOMAN SHEILA JACKSON LEE, OF TEXAS
(TX-18)

STATEMENT BEFORE THE

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

HEARING ON

"The USA PATRIOT ACT: DISPELLING THE MYTHS"

WEDNESDAY, MAY 11, 2011; 10:00 PM
2141 RAYBURN HOUSE OFFICE BUILDING

STATEMENT

First and foremost, I would like to thank Chairman Sensenbrenner and Ranking Member Scott for convening this very important hearing on the Patriot Act and its expiring provisions.

I would also like to thank today's witnesses for coming in and sharing their expertise and experiences with us.

- Patrick J. Rowan, Partner, McGuireWoods LLP
- The Honorable Robert Barr, Former Congressman (GA-7)
- Bruce Fein, Campaign for Liberty
- Ed Mullins, President, Sergeants Benevolent Association of New York City

In today's hearing, we will have an opportunity to discuss the expiring provisions of the Patriot Act and the Foreign Intelligence Surveillance Act ("FISA"), particularly, the "roving wiretap," "lone wolf," and "business records" provisions. Unless action is taken soon, these provisions are due to sunset on May 27, 2011, after being renewed for two months back in March to allow for more oversight, investigation, and consideration.

We are not strangers to these provisions, as they become a controversial topic of discussion in every debate about the Patriot Act or FISA. As a matter of fact, just a couple of months ago we stood on

constitutional and civil liberties concerns they raise as we debated H.R. 514, which would have extended the expiring provisions.

As a member of the Homeland Security Committee, I understand and appreciate the importance of national security, and the challenges we face as we strive to protect our nation from foreign threats. However, as an American citizen, I am deeply concerned when our Constitutional rights run the risk of being infringed upon in the name of national security.

To win the war on terror, the United States must remain true to the founding architects of this democracy who created a Constitution which enshrined an inalienable set of rights. These Bills Of Rights guarantee certain fundamental freedoms that cannot be limited by the government. One of these freedoms, the Fourth Amendment, is the *right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures.*

We do not circumvent the Fourth Amendment, or any other provision in the United States Constitution, merely because it is inconvenient. While the PATRIOT Act is intended to improve our ability to protect our nation, it needs to be revised and amended to

jewel of democracy. However, in their current state, the provisions we are examining today do not do that.

First, we will look at Section 215 of the PATRIOT Act which enlarges the scope of materials that may be obtained under FISA, and lowers the standard required before a court order may be issued to compel production. This is sometimes referred to as the "business records" provision because it is often used to seize that type of information. As the "business records" provisions is currently written, an executive branch agent can obtain a FISA court order requiring a person or business to produce essentially any record that is relevant to a national security investigation *without showing probable cause* or even a direct connection to a foreign power.

The second provision, known commonly as the "roving John Doe wiretap," allows the government to obtain intelligence surveillance orders that identify neither the person nor the facility to be tapped. Like the first provision, this, too, was addressed in the Judiciary Committee during the last Congress, and is also contrary to traditional notions of search and seizure, which require government to state "with particularity" what it seeks to search or seize. If this

should be done so to mirror similar and longstanding criminal laws that permit roving wiretaps, but require the naming of a specific target.

The third provision that H.R. 514 would extend is the "lone wolf" provision, which permits secret intelligence surveillance of non-US persons who are not affiliated with a foreign organization. This type of authorization, which is only granted in secret courts, is subject to abuse, and threatens our longtime understandings of the limits of the government's investigatory powers within the borders of the United States. Moreover, according to government testimony, this provision has *never been used*. Because of the potential for abuse created by this provision, and the lack of need for its existence, it, too, should be allowed to expire.

Issues surrounding these particular provisions are not a stranger to us, for we have been dealing with them since 2001 when the PATRIOT Act was introduced. In 2005, the Patriot was examined in the Judiciary Committee. I, along with other Members of the Judiciary Committee like Mr. Conyers and Mr. Nadler, offered multiple amendments that not only addressed these three

of intent.

Again, these same issues came before us in 2007. On August 3, 2007, I stood before you on the House floor discussing the Foreign Intelligence Surveillance Act (FISA), another piece of law used in conjunction with the PATRIOT Act and essential to combating the war on terror, but one that was in need of improvements to protect Americans' Constitutionally enshrined civil liberties. On that day, I said that, "we must ensure that our intelligence professionals have the tools that they need to protect our Nation, while also safeguarding the rights of law-abiding Americans," and I stand firmly behind that notion today.

When we were considering FISA, there were Fourth Amendment concerns around secret surveillance and secret searches, which were kept permanently secret from the Americans whose homes and conversations were targeted. There were also concerns such secret searches intended for non-U.S. citizens, could be used to target Americans.

I offered amendments to ensure that any surveillance of an American is done through established legal procedures pursuant to

Intelligence Surveillance Court is indispensable and would play a meaningful role in ensuring compliance with our constitution. I stand here today urging my colleagues to consider allowing similar amendments to the PATRIOT Act that better protect Americans' right to privacy before moving this legislation out of the House on Representatives and onto the other legislative body.

Furthermore, a bill considering an extension of these provisions was considered last year in the 111th Congress, and went through oversight hearings and two days of mark-up in the Judiciary Committee. Yet, none of those voted-on, bipartisan amendments that resulted from those hearings have been included in any recent legislation. In those hearings, multiple concerns were raised about the breadth of the PATRIOT Act and the leeway it gives to infringe upon an individual's privacy and civil liberties.

In the mark-up, I personally introduced amendments that would allow for greater transparency in the PATRIOT Act and enhanced protection against violation of individuals' civil liberties. None of my amendments, or those introduced by any of my

been included in any recent legislation.

As an American citizen, the security and safety of my constituency is pinnacle, but I will never stand for legislation that infringes on the basic rights afforded in our Constitution. When our founding fathers drafted the constitution, after living under an oppressive regime in Britain, they ensured that the American people would never experience such subjugation. Where are the protective measures for our citizens in the PATRIOT Act? Why are the measures addressed in the last Congress not included in the bill?

Tomorrow, we will have an opportunity, once again, to make substantive changes to these provisions to ensure that we are striking the right balance between giving the Executive branch the powers it needs while preserving the civil liberties and privacy of Americans.

There is nothing more important than providing the United States of America, especially our military and national security personnel, the right tools to protect our citizens and prevail in the global war on terror. Holding true to our fundamental constitutional principles is the only way to prove to the world that **it is** indeed possible to secure America while preserving our way of life.

From this hearing, it is my hope that we will come away with a better knowledge of how to best address the needs of those agencies which uphold our national security, while upholding constitutional principles and protecting the rights of privacy of the American people.

I would like to thank the witnesses again for their testimony. Thank you Chairman, and I yield back the remainder of my time.

Policy Analysis

No. 675 May 16, 2011

Leashing the Surveillance State
How to Reform Patriot Act Surveillance Authorities

by Julian Sanchez

Executive Summary

Congress recently approved a temporary extension of three controversial surveillance provisions of the USA Patriot Act and successor legislation, which had previously been set to expire at the end of February. In the coming weeks, lawmakers have an opportunity to review the sweeping expansion of domestic counter-terror powers since 9/11 and, with the benefit of a decade's perspective, strengthen crucial civil-liberties safeguards without unduly burdening legitimate intelligence gathering. Two of the provisions slated for sunset—roving wiretap authority and the so-called "Section 215" orders for the production of records—should be narrowed to mitigate the risk of overcollection of sensitive information about innocent Americans. A third—authority to employ the broad investigative powers of the Foreign Intelligence Surveillance Act against "lone wolf" suspects who lack ties to any foreign terror group—does not appear to be necessary at all.

More urgent than any of these, however, is the need to review and substantially modify the statutes authorizing the Federal Bureau of Investigation to secretly demand records, without any prior court approval, using National Security Letters. Though not slated to sunset with the other three Patriot provisions, NSLs were the focus of multiple proposed legislative reforms during the 2009 reauthorization debates, and are also addressed in at least one bill already introduced this year. Federal courts have already held parts of the current NSL statutes unconstitutional, and the government's own internal audits have uncovered widespread, systematic misuse of expanded NSL powers. Congress should resist recent Justice Department pressure to further broaden the scope of NSL authority—and, indeed, should significantly curtail it. In light of this history of misuse, as well as the uncertain constitutional status of NSLs, a sunset should be imposed along with more robust reporting and oversight requirements.

Julian Sanchez is a Cato Institute research fellow

CATO INSTITUTE

The Patriot Act significantly expanded government surveillance authorities with minimal Congressional deliberation.

Introduction

It is nearly a decade now since Congress responded to the terror attacks of 9/11 by granting its hasty approval to the USA Patriot Act, a sprawling piece of legislation comprising hundreds of amendments to an array of complex intelligence and law enforcement statutes.[1] 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."[2]

Recognizing that Patriot had significantly expanded government surveillance authorities with minimal deliberation, Congress established expiration dates for 16 of the Act's most controversial provisions. It similarly established a sunset for the so-called "Lone Wolf" provision of the Intelligence Reform and Terrorism Prevention Act of 2004, which allowed non-U.S. persons to be monitored under the aegis of the Foreign Intelligence Surveillance Act even if they were unaffiliated with any foreign power.[3] In 2005, Congress made 14 of those provisions permanent, but retained sunsets for the Lone Wolf provision, as well as Patriot Act provisions authorizing the secretive Foreign Intelligence Surveillance Court to issue warrants for "roving wiretaps" and broad orders compelling the production of business records or any other "tangible thing."[4] In the process, legislators added a number of safeguards aimed, in part, at assuaging the concerns of civil libertarians.[5]

In late 2009, as the sunset date loomed, the judiciary committees of both the House and Senate held extensive hearings to consider how these new powers had been used and what modifications to the existing statutes might be appropriate.[6] Additionally, in response to a series of increasingly damning reports from the Justice Department's Office of the Inspector General, showing large-scale and systematic abuse of the Patriot Act's expanded authority to issue National Security Letters,[7] Congress held further hearings focused on these powerful tools, which allow the Federal Bureau of Investigation to demand a wide array of telecommunications and financial records without judicial approval.[8]

The hearings and associated debate generated both substantial press coverage[9] and an array of substantive reform bills.[10] Ultimately, however, and despite a temporary short-term extension aimed at allowing further debate, Congress passed—and President Obama signed—a one-year reauthorization of the expiring provisions without modification.[11]

The rationale for the limited reauthorization was that the intervening time would be used for fruitful deliberation on needed reforms, but that hope was not borne out. Until February, there had been almost no further debate in Congress concerning the expiring Patriot provisions or the pressing need for National Security Letter reform, and press attention had been correspondingly scant.

At least some legislators, however, appear to be growing weary of these deferrals. The same one-year reauthorization that easily garnered the two-thirds majority required for fast-track passage in 2009 fell short this year, to the surprise of many observers.[12] Instead, Congress approved an extension of the expiring provisions for just three months, with leaders in both parties pledging that there would now—finally—be serious deliberation on the need for substantive reform.[13]

As of this writing, most of the legislative proposals that have been advanced involve either long-term reauthorization without alteration or modest amendments. Sen. Dianne Feinstein (D-CA) supports reauthorization through the end of December 2013, along with an extension of the controversial FISA Amendments Act of 2008 to the same date,[14] while Sen. Chuck Grassley (R-IA) is seeking permanent reauthorization of the expiring provisions.[15] Sen. Patrick Leahy (D-VT), meanwhile, has reintroduced the

relatively mild reform legislation he sponsored in 2009, which at the time was approved by a bipartisan majority of the Senate Judiciary Committee.[16]

With additional time for deliberation, however, Congress should consider more far-reaching changes. With minor modifications, the roving wiretap provision can safely be made permanent, providing greater clarity and certainty to intelligence investigators. The Section 215 "tangible things" provision, by contrast, requires additional Congressional scrutiny: it should be extended only in a narrowed form, and with further reporting and auditing requirements. The Lone Wolf provision, which as of last year the Justice Department said had never been used, can simply be allowed to expire. (In the event that consensus has not been achieved when the new deadline arrives, there is little reason to believe their expiration would cause any near-term impediment to intelligence gathering: all three sunsetting provisions have been used fairly sparingly, and are, in any event, subject to a grandfather clause that would permit their continued use for investigations already underway.[17])

Most importantly, Congress should narrow the scope of National Security Letters, which have already proven susceptible to widespread abuse, and which federal courts have already found to be seriously constitutionally defective in their current form. At an absolute minimum, a series of procedural safeguards that the Justice Department has already agreed to implement on a voluntary basis should be codified in statute. Even with these added constraints, a new sunset for expanded NSL authorities should be established, along with mandatory auditing by the Office of the Inspector General, to ensure that they are subject to adequate congressional review.

I now turn to consider each of the sunsetting provisions, as well as National Security Letters, in detail. While many of the arguments below are framed in terms of the constitutional limits on government surveillance, they also provide policy grounds for reform. Insofar as these provisions impose heavier burdens on core privacy, speech, and association interests than is necessary to the protection of national security that should be sufficient reason to seek a better balance regardless of where one comes down on the legal question.

The Lone Wolf Provision

The extraordinary tools available to investigators under the Foreign Intelligence Surveillance Act, passed over 30 years ago in response to revelations of endemic executive abuse of spying powers,[18] 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" (that is, anyone not a citizen or legal permanent resident) 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. According to a letter sent to Senator Leahy in September of 2009 by Assistant Attorney General Roland Weich, the Lone Wolf provision's authority had never been invoked as of that date, and there has been no indication that it has been used since.[19]

As with many post-9/11 intelligence reforms, the Lone Wolf provision has its genesis in the misguided assumption that every intelligence failure is evidence that investigators lack sufficient surveillance authority—a convenient scapegoat—while internal institutional dysfunction often bears the lion's share of the blame.[20] In the aftermath of the attacks, it was initially alleged that FBI investigators who had wanted to obtain a warrant to search the laptop of so-called "20th hijacker" Zacarias Moussaoui were unable to do so because FISA lacked such a Lone Wolf provision. This claim, according to the Congressional Research Service, provided the "historical impetus" for Lone Wolf authority.[21]

Congress should narrow the scope of National Security Letters, which have already proven susceptible to widespread abuse.

But a 2003 bipartisan report from the Senate Judiciary Committee tells a very different story.[22] It notes that on September 11, 2001, investigators were able to obtain a conventional warrant using the exact same evidence that had previously been considered insufficient. Worse, the Committee found that supervisors at FBI Headquarters had failed to link related reports from different field offices, or to pass those reports on to the lawyers tasked with determining when a FISA warrant should be sought. Officials in charge, the Senate report concluded, misapplied such crucial legal standards as "probable cause" and falsely believed that they could not seek a FISA order unless the specific foreign terror group with which a target was affiliated could be definitively identified.

"In performing this faitly straightforward task," the report concludes, "FBI headquarters personnel failed miserably."[23] In short, the problem was not that investigators lacked Lone Wolf powers, but that they had not properly applied the powers they already had. Nevertheless, the new power was granted.

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, but also that it has not yielded any practical harm. The Lone Wolf provision does, however, threaten to blur the vital and traditional distinction in American law between the constraints on strictly domestic national security investigations and foreign intelligence.

The problem was not that investigators lacked Lone Wolf powers, but that they had not properly applied the powers they already had.

Foreign Intelligence versus Domestic Security

Courts have always extended greater deference to the executive in the realm of foreign intelligence than in cases involving strictly domestic security concerns. In a seminal ruling in what has come to be known as the *Keith* Case, a unanimous Supreme Court held that the Fourth Amendment's warrant requirement applied with full force to strictly domestic intelligence investigations, even where the national security was implicated.[24] The Court did, however, echo the language of prior rulings, suggesting that less stringent limits might apply where foreign powers were concerned:

> Further, the instant case requires no judgment on the scope of the President's surveillance power with respect to the activities of foreign powers, within or without this country. The Attorney General's affidavit in this case states that the surveillances were "deemed necessary to protect the nation from attempts of *domestic organizations* to attack and subvert the existing structure of Government" (emphasis supplied). There is no evidence of any involvement, directly or indirectly, of a foreign power.[25]

The Court clearly saw the involvement of a foreign power as a crucial factor demarcating two constitutionally distinct realms. Prior to 2005, the Foreign Intelligence Surveillance Act tracked this distinction, enabling broad surveillance—subject to the oversight of a secret court, and governed by laxer restrictions than apply in domestic criminal investigations—of persons demonstrated to be tied to foreign powers, including international terrorist groups.[26] Absent the involvement of such a foreign power, the salient considerations bearing on investigations of true lone wolves are nearly indistinguishable from those that apply to investigation of domestic terrorists and violent criminals. While the *Keith* Court did suggest Congress might create procedures for domestic national security investigations distinct from those governing criminal investigations, the Lone Wolf provision simply adds an additional trigger condition to a framework otherwise exclusively used for investigations of foreign powers.

FISA's definition of international terrorism still requires some foreign "nexus" before a suspected lone wolf can be targeted, but the statute provides only the vague guidance that its aims or methods "transcend" national boundaries. Construed strictly, this

might be sufficient to keep the boundary between foreign and domestic intelligence intact. But Justice Department officials have suggested that the definition would cover a suspect who "self-radicalizes by means of information and training provided by a variety of international terrorist groups via the Internet," which potentially makes a YouTube clip the distinction between a domestic threat and an international one.[27] Activities "in preparation" for terrorism, according to the legislative history, may include the provision of "personnel, training, funding, or other means" for either a particular act of terrorism or for a group engaged in terrorism.[28]

The FISA definitions of an agent of a foreign power applicable to citizens explicitly require that a U.S. person targeted under the statute must knowingly assist a foreign power. They also prohibit investigations conducted exclusively on the basis of protected First Amendment activities, such as political advocacy.[29] There are no such explicit limitations in the Lone Wolf provision.

Moreover, while international terrorism is defined by statute, an analysis by the Syracuse University's Transactional Records Access Clearinghouse, a research institution focused on government oversight, suggests that government entities apply the classification inconsistently. Federal prosecutors decline to bring charges in a substantial majority of the terrorism cases referred for prosecution by intelligence and law enforcement agencies, but in the recent cases where charges *have* been brought, more than a quarter of defendants identified as terror related by the Justice Department's National Security Division were not so categorized by prosecutors. Only 8 percent of defendants appeared on all of three lists of terror-related cases independently compiled by the Justice Department, federal prosecutors, and federal courts.[30] In light of this discrepancy—and especially in the absence of the scrutiny imposed by a sunset—there are grounds to worry that removing the bright-line requirement of a link to a foreign power may permit the FISA process to be invoked for investigations involving non-citizens that would more properly be classified as criminal inquiries.

The Broad Scope of FISA Surveillance

Though the evidentiary showing needed to target a person under FISA is looser than under criminal law, the surveillance powers it affords are substantially broader. So-called "Title III" wiretaps in criminal cases require evidence of a "nexus" between suspected criminal activity and each location or communications facility monitored.[31] Even then, agents are only supposed to record conversations that are pertinent to the investigation.

Once someone is designated as an agent of a foreign power, by contrast, information collection is "heavily weighted toward the government's need for foreign intelligence information," meaning that "large amounts of information are collected by automatic recording to be minimized after the fact," with the minimization of irrelevant information occurring "hours, days, or weeks after collection."[32] In general, FISA "permits acquisition of nearly all information from a monitored facility or a searched location."[33] And as the discussion of the other provisions analyzed below should make clear, even casual associates of a target of FISA surveillance become susceptible to acquisition of private records detailing their activities.

Even when information has been formally minimized, it may remain, in practice, available to intelligence agencies. In the 2003 case *U.S. v. Sattar*, the FBI had reported that it had conducted FISA surveillance subsequent to which "approximately 5,175 pertinent voice calls . . . were not minimized." When it came time for the discovery phase of a criminal trial against the FISA targets, however, the FBI "retrieved and disclosed to the defendants over 85,000 audio files . . . obtained through FISA surveillance."[34] Moreover, while targets of Title III surveillance are typically eventually informed of the eavesdropping, after the investigation has finished, FISA targets are not—enhancing the secrecy of intelligence practices, but removing a powerful check against abuses.[35]

Removing the bright-line requirement of a link to a foreign power may permit the FISA process to be invoked for investigations that would more properly be classified as criminal inquiries.

Recommendations

In sum, 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 under Title III wiretaps. 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.

The need for secrecy is heightened when the target is a member of a larger group generally beyond the immediate reach of U.S. authorities—a group that may even have some capability to infiltrate traditional law enforcement systems. The interest in continued investigation of that larger group—whether by turning or simply continuing to monitor their agent in the United States—also means that intelligence investigations may not have criminal prosecution of the target as their goal. As a rule, these considerations simply do not apply to genuine lone wolves.

In the absence of the special needs created by the involvement of foreign powers, then, reliance on the more stringent provisions of Title III should be the norm. This should pose no problem for investigators, because any application meeting the standard for the Lone Wolf provision, if legitimately construed to cover actual terror plotters, will also meet the standards of Title III.

Because Lone Wolf authority does not yet appear to have been invoked, it is difficult to gauge the appropriate level of concern about its potential future uses. Since, however, it does not appear to have been necessary in practice, and by its own terms would only properly apply when parallel criminal authorities would also be available, there is little good reason to leave it on the books.

Roving Wiretaps

Section 206 of the Patriot Act established authority for multipoint or roving wiretaps under the auspices of the Foreign Intelligence Surveillance Act. The idea behind a roving wiretap should be familiar to fans of the acclaimed HBO series *The Wire*, in which drug dealers rapidly cycled through disposable "burner" cell phones to evade police eavesdropping. A roving wiretap is used when a target is thought to be employing such measures to frustrate investigators, and allows the eavesdropper to quickly begin listening on whatever new phone line or Internet account her quarry may be using, without having to go back to a judge for a new warrant every time. In 2009, FBI Director Robert Mueller testified that roving authority under FISA had been used 147 times.[36]

Roving wiretaps have existed for criminal investigations since 1986.[37] There is broad agreement, even among staunch civil libertarians, that similar authority should be available for terror investigations conducted under the supervision of the Foreign Intelligence Surveillance Court.[38]

Serious civil liberties concerns remain about the specific statutory language authorizing roving intelligence wiretaps.

Serious civil liberties concerns remain about the specific statutory language authorizing roving intelligence wiretaps, however. To understand why, it's necessary to examine some of the broad differences between electronic surveillance warrants under FISA and the Title III wiretaps employed in criminal investigations.

The Fourth Amendment imposes two central requirements on warrants authorizing government searches: "probable cause" and "particularity."[39] Under Title III, that means warrant applications must connect the proposed surveillance to some specific criminal act, and must "particularly [describe] the place to be searched and the persons or things to be seized." For an ordinary non-roving wiretap, law enforcement satisfies that requirement by establishing a nexus between evidence of a crime and a particular place (such as a phone line, an e-mail address, or a physical location). This will often involve a named target, but it need not. For example, a warrant might be obtained to bug a location known to be used for gang meetings, or a mobile phone used to discuss criminal

activity with another target already under surveillance, even if the identities of the persons making use of those facilities are not yet known. The requirement of a demonstrable nexus to criminal activity remains, however. Authority to bug Tony Soprano's office will not entail a power to eavesdrop on his therapy session or bug his bedroom, absent good reason to think he's discussing mob activity in those places. Since places and communications facilities may be used for both criminal and innocent purposes, the officer monitoring the facility is only supposed to record what's pertinent to the investigation.

When a roving wiretap is authorized under Title III, things necessarily work somewhat differently.[40] For roving taps, the warrant application shows a nexus between the suspected crime and an identified target person rather than a particular facility. Then, as surveillance gets underway, the eavesdroppers can "go up" on a line once investigators have "ascertained" that the target is "proximate" to a location or communications facility. Perhaps in part because they require an additional showing that a traditional facilities-based wiretap is unlikely to succeed, these broad warrants are used relatively sparingly: only 16 were issued in 2009 at the state level, and none at the federal level.[41]

Problems of Particularity

A number of Fourth Amendment challenges have been raised to Title III criminal roving wiretaps, on the grounds that a warrant naming a target, rather than a specific place or facility, cannot meet the constitutional particularity requirement. In rejecting such challenges, the courts have invariably stressed that, in the modern context, the substitution of a *named target* for a named facility is a key feature that allows Title III multipoint wiretap orders to pass the particularity test. For instance, in *United States v. Bianco*, the Court of Appeals for the Second Circuit emphasized that:

> unlike other orders under Title III, which requires identification of the anticipated speaker only "if known," Section 2518(1)(b)(iv), to satisfy the roving intercept statute, the person targeted for roving interception must be identified, and only conversation involving the specified individual may be intercepted.[42]

Similarly, in *United States v. Petti*, the Ninth Circuit wrote:

> 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.[43]

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.

An amendment in 2006 did at least add the requirement that the description identify a specific target—which would *appear* to entail that each target must be a particular individual person, rather than some indeterminate group or class of persons satisfying a general characterization. But when the identity of the target cannot be determined conclusively, this too becomes difficult to guarantee. So, for example, an application targeting the person residing at a particular location or using a particular phone will be indeterminate in scope if (unbeknownst to the applicant) multiple people in fact fit the description—rendering the communications of those other (potentially innocent) persons over multiple facilities susceptible to interception. A similar error may cause an

Challenges have been raised to Title III criminal roving wiretaps on the grounds that a warrant naming a target cannot meet the constitutional particularity requirement.

An *identity*—as opposed to a description—is a key to a broad universe of records, and thus provides a multidimensional stream of information that can be used for error correction.

agent to follow the wrong person to a new facility in the case of a warrant with a named target—but then, at least, the fact that there clearly *is* a wrong person enables the error to be corrected more readily and acquisitions falling outside the scope of the warrant to be decisively identified.

A reported intelligence violation uncovered by a Freedom of Information Act request from the Electronic Frontier Foundation provides a concrete illustration of the point.[44] In an investigation of an apparently named, identified couple under FISA roving authority, a clerical error resulted in a line no longer used by the targets being included in an order renewing electronic surveillance. Subsequently, a phone apparently used by a young child was monitored for five days until agents realized the mistake. The error was detected, in part, because technicians noticed that the subjects identified in the warrant had previously been assigned the targeted line, but disconnected their service. Knowledge of the identity of the subjects also gave analysts a series of expectations about the parties to the communication, against which the fruits of surveillance could be checked. An *identity*—as opposed to a description—is a key to a broad universe of records, and thus provides a multidimensional stream of information that can be used for error correction. It might become apparent, for example, that a phone is making calls from one location when the target specified in the warrant is known to be elsewhere. When the target is known only by a description sufficiently specific to enable targeting of a wiretap, robust error correction is far less likely.

The Risks of "John Doe" Warrants

While permitting John Doe warrants under Title III would be problematic for all these reasons, the risk of improper overcollection is actually far greater in the intelligence context because, as discussed above in the analysis of the Lone Wolf provision, FISA surveillance is in general far broader than its Title III counterpart. "[L]arge amounts of information are collected by automatic recording to be minimized after the fact," and that after-the-fact "minimization" may not always entail the destruction of the "minimized" information.[45] Had the case discussed above occurred under Title III, real-time minimization should have prevented recording of communications on the targeted line unless a known target could be positively identified as party to the conversation.

This risk may be especially high when surveillance involves the use of sophisticated online filtering technology at an array of unknown facilities. Such overcollection is a risk even when a target *is* named, because the global scope of the Internet increases the likelihood that (for example) multiple users with similar names, or who have connected from the same IP address at different times, will hold accounts at a new facility. In the course of a recent criminal investigation, for example, the FBI inadvertently obtained the full e-mail archives of an unrelated person because of a typo in a warrant application.[46] But the risk is greatly heightened without the anchor of a named target.

As an illustration, consider the hypothetical (but presumably representative) wiretap order described at a 2009 surveillance conference by attorney Joel M. Margolis, who handles government surveillance requests for the telecommunications company Neustar.[47] Margolis outlined the difficulties an Internet service provider might face interpreting an order instructing an ISP to target the keyword, or virtual identifier, "RedWolf" using Deep Packet Inspection technology.[48]

Targeting on a virtual identifier will often be perfectly legitimate, provided there is evidence that the person using that ID at a particular website or online service is acting as an agent of a foreign power. Indeed, in the case of a warrant naming a specific facility, "the person using the ID RedWolf might be an adequately specific characterization of the target *within the context of surveillance directed at that facility*. But even when there is an identified target, such monitoring creates an inferential gap between the individual target

and the mechanism used to acquire his communications. John Doe" warrants add a second inferential gap.

Investigators will presumably be fairly sophisticated about this; they are likely to understand, for instance, that evidence sufficient to target RedWolf at *one particular site* will not by itself justify acquisition on that identifier elsewhere on the Internet. But the probability of error is inevitably magnified when a descriptive targeting mechanism is transplanted across facilities, and especially when the target is unknown *independently* of that description. We are, as a result, far removed from the scenario in *Petti*, where there was "virtually no possibility of abuse or mistake."[49] In light of the range of powerful tools that will already be available to investigators by the time probable cause is established—including wiretaps of specified facilities, National Security Letters, and Section 215 orders—it should be possible to determine a name for most targets without an unacceptable delay. If this is not possible, however, we should question whether the same tools that are inadequate to yield a target's identity *will* permit that target to be reliably tracked from facility to facility.

Why Ex Post Oversight Isn't Enough

Congress made some effort to address such concerns when it reauthorized Section 206 in 2005, adding the aforementioned requirement that FISA applications describe a specific target. Under the revised roving statute, eavesdroppers must inform the FISA Court within 10 days of any new facility they eavesdrop on (60 days if cause for delay is shown), and explain the "facts justifying a belief that the target is using, or is about to use, that new facility or place."[50] That is a step in the right direction, but back-end checks and oversight are unlikely to be an adequate substitute for front-end limitations on the scope of covert surveillance, and indeed, may create a false sense of security.

Consider that in fiscal year 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 majority pursuant to FISA warrants. A recent audit of FBI backlogs by the Office of the Inspector General found that fully a quarter of the audio collected between 2003 and 2008 remained unreviewed (including 6 percent of counterterror acquisitions and 31 percent of counterintelligence acquisitions, the two categories covered by FISA wiretaps).[51] Meaningful independent review of this volume of intelligence collection must, in practice, be fairly superficial. Indeed, when the target is known only by description, a mistaken collection may not be immediately obvious even after the fact.

Other structural features of the criminal justice system do provide a form of de facto after-the-fact oversight for electronic surveillance in criminal investigations. Because Title III wiretaps aim at criminal prosecution, investigators must anticipate that they will be subject to a distributed form of de facto review by defense counsel, who have a right to seek discovery and a powerful incentive to identify any improprieties. Even when an investigation does not result in charges being brought, wiretap targets must be notified of the surveillance after the fact.[52]

FISA surveillance, by contrast, is covert by default, and often seeks intelligence for purposes other than criminal prosecution.[53] Even when the fruits of FISA collection are used at trial, discovery is far more limited.[54] Defenders of this and other Patriot Act provisions often assert that they only provide intelligence agencies the same tools available in criminal investigations, but almost invariably neglect the profound structural differences between criminal and intelligence law.

Defenders of the FISA provision and other Patriot Act provisions almost invariably neglect the profound structural differences between criminal and intelligence law.

Recommendations

Because FISA surveillance is in practice subject to less robust ex post scrutiny, it is, if anything, *more* important to constrain the discretion of investigators in selecting target facilities at the acquisition stage. Ide-

ally, Congress should impose a requirement, parallel to Title III, that the target of a roving wiretap be a named individual—as in all likelihood is already the case for the vast majority of the 22 roving FISA wiretaps issued, on average, each year. For the small number of unnamed targets, the array of other FISA tools that would already be available—including facilities-based wiretaps and authority to acquire business records—should enable identification of the target before roving surveillance begins. With that change, FISA roving authority could safely be made permanent.

If experience with previous roving investigations suggests that greater flexibility is truly essential, FISA could permit a John Doe application to make the showing needed to justify roving authority, but remain limited upon issuance to a specified set of facilities. Roving authority would be triggered only after agents had positively identified the John Doe target, and made a submission to the FISA Court of the facts supporting the conclusion that the target described in the initial order had been identified. The FISA Court would need to ratify this identification within a relatively short period—10 days seems reasonable—but without the need to approve an entirely new application. With the latter modification, roving authority could be renewed, but should not be made permanent without a further period of review.

In either case, the Justice Department's annual FISA report to Congress should be required to include a tally of the number of roving orders issued each year and, if applicable, the number of those issued without a named target. To the extent possible, any opinion of the FISC involving substantive interpretation of the scope of roving wiretap authority should be made available in a public, redacted version. Finally, Congress should direct the Justice Department's Office of the Inspector General to conduct periodic audits of roving wiretap orders and prepare reports on their use, which should be redacted as necessary to permit public release.

Third-party custodians of records would have few incentives beyond sheer public-spiritedness to expend resources challenging Section 215 orders.

Section 215 Orders

Section 215 of the Patriot Act vastly expanded the ability of investigators to compel the production of sensitive records. Between 1998 and 2001, FISA allowed the Foreign Intelligence Surveillance Court to issue orders demanding records from a few specified categories of business, provided the FISC found there to be "specific and articulable facts" supporting the belief that the records pertained to a "foreign power or an agent of a foreign power."[55] During that time, the business records authority was invoked only once.[56]

The Patriot Act expanded this authority in three crucial respects. It removed the limitation on the types of businesses to which production orders could be issued; it expanded the items covered by the orders from business records to any "tangible thing"; and perhaps most importantly, it removed any requirement that the information sought pertain to a person suspected of involvement with terrorism or a foreign government.

These demands are subject to gag orders prohibiting the recipients from disclosing their existence. Unlike National Security Letters, these gag orders are at least imposed by a federal judge, but their breadth and the highly deferential standard of review to which they are subject parallels language in the NSL statutes that has already been held incompatible with the Fourth Amendment by the U.S. Court of Appeals for the Second Circuit.[57] Third-party custodians of records would have few incentives beyond sheer public-spiritedness to expend resources challenging these orders under any circumstances, and fewer still when the reviewing judges are instructed to treat the mere assertion of a national security need for secrecy as "conclusive."[58] A challenge under such a standard requires a willingness to tilt at windmills with a gold-plated lance.

The initial wording of Section 215 required only that the records be sought for a foreign-intelligence investigation. Congress subsequently raised this standard, requiring

a recitation of facts providing "reasonable grounds to believe" that the information is relevant to an authorized investigation to protect against terrorism *or* an intelligence investigation whose target is not a U.S. person.[59] This is "an undemanding standard that requires the government to show that the tangible things may have a bearing on or produce information probative of the investigation."[60] But the FISC is further required to find that records are *presumptively* relevant on a showing that they pertain to an agent of a foreign power, a person in contact with an agent of a foreign power, or the activities of such an agent.[61]

In the modern context, that standard permits the acquisition of a wide array of sensitive information about an enormous number of Americans with no connection to terrorism, on the basis of the most tenuous connection to any actual suspect. "When combined with the broad sweep of the three areas in which a tangible-things order is presumptively relevant," according to the manual coauthored by the former head of the Justice Department's National Security Division, "FISA appears to allow the government to obtain a tangible-things order with a minimal showing that the items it seeks are connected to the activities of a foreign power or agent of a foreign power." This might include, for example, "the bank records of the grade school teacher of the child of a person who is suspected of being an agent of a foreign power."[62]

Like National Security Letters—which are issued entirely without advance judicial approval—Section 215 orders need not be supported by the individualized suspicion or finding of probable cause normally required for a Fourth Amendment search. In both cases, the legal theory underpinning such a procedure is the so-called "third-party doctrine," which rests on the dubious proposition that persons normally waive their "reasonable expectation of privacy" when they provide documents to third parties, even when those parties are contractually or statutorily bound to confidentiality.[63]

How Protected are Third-Party Records?

During the initial debate over the Patriot Act, Senator Leahy justified the expansion of Section 215 on the grounds that "the Fourth Amendment does not normally apply to such techniques and the FBI has comparable authority in its criminal investigations."[64] Supporters of the provision, since the Act's passage, have routinely invoked similar comparisons to such tools as administrative- or grand-jury subpoenas, despite significant differences between these authorities.[65]

While a detailed analysis of the third-party doctrine is beyond the scope of this paper, it bears noting that it has long been the subject of blistering criticism by legal scholars, especially as technological change has increased the quantity of personal information about each of us held by third parties.[66] One of its lonely defenders in the academy has characterized it as "the Fourth Amendment rule scholars love to hate. . . . the *Lochner* of search and seizure law, widely criticized as profoundly misguided."[67] Numerous state supreme courts have rejected it, in whole or in part, under state constitutional provisions parallel to the Fourth Amendment.[68]

If we stipulate the general validity of the third-party doctrine for the sake of argument, however, it is worth noting that it has traditionally been applied precisely to *records*, retained by firms whose employees have access to them for ordinary business purposes. It is not a blanket Fourth Amendment exception for *any* item in the possession of a third party. The exception does not, for instance, extend to the contents of rented storage lockers.[69] A recent appellate ruling has similarly suggested that it does not apply to the contents of remotely stored e-mail, which a 25-year-old federal statute had hitherto permitted to be obtained without a probable-cause warrant in many circumstances.[70]

Even within the category of records, appellate courts have begun indicating that the third-party doctrine will not always apply. The Third Circuit recently held that location records held by mobile phone provid-

The relevancy standard permits acquisition of sensitive information about Americans with no connection to terrorism.

ers *do* enjoy Fourth Amendment protection, in part because "[a] cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way."[71] A parallel argument could easily be made for much of the transactional information, or metadata, generated by online activity and collected by websites or service providers.[72] As these cases should make clear, courts are still in the early very stages of grappling with the proper application of the Fourth Amendment to the Internet era.

Moreover, there are a range of distinct First Amendment interests implicated by government access to online transactional data and other records that may reveal expressive activity, which are explored in greater detail in the section dealing with National Security Letters below.[73] In brief: numerous courts have found that heightened scrutiny is necessary when the compulsory production of records would burden the right to speak, read, or associate anonymously. Judges reviewing applications under Section 215 may, of course, take such considerations into account *sua sponte*, but with respect to covert national security investigations, recipients of these orders will typically have neither the incentive nor—just as crucially—the information necessary to mount an effective challenge on these grounds when appropriate.

There are a range of First Amendment interests implicated by government access to online transactional data and other records that may reveal expressive activity.

Language in the amended Section 215 does explicitly limit the scope of orders to items that could be obtained via grand-jury subpoena or similar compulsory process.[74] But the secrecy surrounding the orders, coupled with the broad scope of "tangible things" authority, invites uses that push the boundaries of the already overbroad Fourth Amendment loophole upon which this authority is premised, even as courts begin moving to clarify and narrow it. Secret proceedings before the FISC are, to put it mildly, not the ideal forum to test the outer limits of an evolving area of law.

Section 215 in Practice

Fortunately—and owing in part to the substantial controversy surrounding Section 215—the Justice Department was at least initially relatively circumspect in its use of this authority, limiting itself to seeking actual business records during the period covered by the Inspector General's audits.[75] Indeed, expanded Section 215 authority was not used at all for two years after the passage of the Patriot Act, and appears to have been used relatively sparingly since then.[76] Moreover, the FISC appears to be fairly active in keeping the scope of Section 215 orders narrow: of the 21 sought in 2009, for example, the Court made modifications to 9 of the orders.[77]

There are, nevertheless, several reasons for concern. First, the relatively sparing use that has been made of Section 215 may is attributable in large measure to the extraordinary breadth of post-Patriot National Security Letters, which make a wide array of the most useful records available to investigators without the need for a court order. FBI agents interviewed by the Office of the Inspector General have made it clear that, in light of the substantial delays associated with Section 215 orders,[78] they are regarded as a tool of "last resort," employed only when National Security Letters or other authorities are unavailable.[79] Indeed, the first uses of the authority appear to have been motivated primarily by a desire to justify its existence to legislators: as a Justice Department attorney explained to the Office of the Inspector General, by the summer of 2003, "there was a recognition that the FBI needed to begin obtaining Section 215 orders because . . . Congress would be scrutinizing the FBI's use of the authority in determining whether to renew the authority."[80]

Should NSL authority be narrowed along the lines recommended below, however, it is highly probable that a sharp increase in the use of Section 215 would ensue. This would be an unambiguous improvement, insofar as it substituted judicial authority for agency fiat in compelling the production of records, but could lead to attenuated scrutiny unless adequate resources are allocated to the application-review process.

Second, the Justice Department's relatively conservative approach to Section 215 appears to be, at least in part, a function of the scrutiny associated with the authority's sunset. In popular discourse, the provision has often been referred to as the "library provision" because it has generated strong opposition from librarians chary of government inquiries into their patrons' reading habits.[81] In at least one case, investigators seeking production of library records were told that a "supervisor would not permit the request to go forward because of the political controversy surrounding 215 requests for information from libraries."[82] That reticence could easily diminish were the provision made permanent.

Finally—and perhaps most worryingly—testimony from Justice Department officials during the 2009 reauthorization debate revealed that Section 215 "supports an important sensitive collection program" about which a few select legislators had been briefed.[83] The heavily redacted public versions of reports from the Office of the Inspector General do not discuss uses of Section 215 connected with this program, which in any event appears to postdate the audit period. Lawmakers familiar with the program, however, have suggested that crucial "information about the use of Section 215 orders that . . . Congress and the American people deserve to know" is absent from the public debate.[84]

In 2005, legislative language narrowing Section 215 authority to require a factual showing that records being sought pertain to terrorists and spies, or their associates, had been approved unanimously by both the Senate Judiciary Committee and the full Senate, but was ultimately removed from the reauthorization bill signed by the president. When a similar reform was rejected in 2009, apparently as a result of a classified briefing in which intelligence officials alleged that such a modification would interfere with this "sensitive collection program," Sen. Richard Durbin (D-IL) complained:

> [T]he real reason for resisting this obvious, common-sense modification of Section 215 is unfortunately cloaked in secrecy. Some day that cloak will be lifted, and future generations will whether ask our actions today meet the test of a democratic society: transparency, accountability, and fidelity to the rule of law and our Constitution.[85]

The most troubling and direct statement on the subject came from former senator Russ Feingold (D-WI), then a member of both the Intelligence and Judiciary Committees, who asserted that he had become aware of specific abuses of Section 215 unknown to the general public and, indeed, to most members of Congress:

> I recall during the debate in 2005 that proponents of Section 215 argued that these authorities have never been misused. *They cannot make that statement now; they have been misused.* I cannot elaborate here, but I recommend that my colleagues seek more information in a classified setting. [Emphasis added.][86]

In short, while the limited public reporting on the use of Section 215 indicates that it was used relatively conservatively through 2006, there are ample grounds for concern that the provision's broad language permits far more sweeping information collection about innocent Americans—and, indeed, there are hints that steps in this direction may have already been taken.

Former senator Russ Feingold (D-WI) asserted that he had become aware of specific abuses of Section 215 unknown to the general public.

Recommendations

Notwithstanding these concerns, greater future reliance on a properly circumscribed Section 215—as a substitute, in many cases, for National Security Letters, which lack adequate judicial supervision—would constitute a significant improvement from a civil liberties perspective, and the Justice Department and FISC should be allocated such resources as may be necessary to render

Section 215 should be tightened so as to foreclose the possibility of fishing expeditions through the sensitive records of innocent Americans.

this feasible. In order to effectively play this role, Section 215 authority that is somewhat more expansive than what existed under the pre-Patriot Act FISA may be appropriate. To compensate for the heightened risks to civil liberties inherent in covert intelligence gathering, however, the scope of Section 215 orders and the standard of review FISC judges apply to them should be tightened so as to foreclose the possibility of fishing expeditions through the sensitive records of innocent Americans only tenuously connected to terror suspects.

First, in light of the evolving state of jurisprudence concerning data entrusted to third parties, Section 215 authority should be explicitly restricted to business records whose subjects lack a Fourth Amendment expectation of privacy in their contents. This would clarify that Section 215 does not apply, for example, to private documents held by cloud-based storage systems, or to the increasingly precise and detailed information about a person's day-to-day physical movements that may be derivable from mobile-device records. It would also recognize explicitly that courts continue to grapple with the question of how far citizens' "reasonable expectation of privacy" extends to other records created by third-party information processing, but not normally subject to human review.[87] FISA's physical search and electronic surveillance authorities, subject to a probable-cause standard, would remain available for protected records and other tangible things.

Second, the presumption of relevance for certain categories of records—which the attorney general has previously indicated the Justice Department does not require—should be repealed.[88] Instead, applications for a Section 215 order should be required to cite specific and articulable facts demonstrating that the records sought are *both* relevant to an investigation *and* fall under one of three categories: records pertaining to a suspected agent of a foreign power who is the subject of an authorized investigation, to persons in contact with such suspected agent, or to the activities of such a person or group when this is the least intrusive available means of identifying the persons involved in those activities.[89]

This dual requirement would give FISC judges a clearer basis for evaluating the evidentiary showing in Section 215 applications, and ensure that something beyond mere casual contact with a suspect justifies acquisition of Americans' sensitive records. At the same time, the relative laxity of the relevance standard ensures that agents are not burdened with too high an evidentiary bar in the exploratory phases of an investigation. On the basis of the limited information available in the inspector general's public reports, it appears highly probable that most—if not all—of the Section 215 orders issued between 2003 and 2006 would already meet this standard. Where there is a compelling argument for broader routine access to specific types of records, and such access would have minimal effect on speech or privacy interests, Congress may wish to consider more narrowly tailored legislation, along the lines of the rules governing importation or sale of certain precursor chemicals for narcotics or explosives.

Finally, the process for challenging Section 215 gag orders should be explicitly altered to comport with the Second Circuit's ruling in *Doe v. Mukasey*, which held that a parallel review process in the National Security Letter statutes failed to adequately respect the First Amendment interests of recipients.[90] That standard requires recipients to wait a full year before challenging a nondisclosure order, burdens them with establishing that there is "no reason" to believe disclosure "may" interfere with any investigation or harm national security, and requires judges to treat certification by a high-ranking Justice Department official as "conclusive" on that question.[91]

The required one-year delay should be removed, and the burden of establishing some realistic likelihood of an identifiable harm shifted to the government. FISC judges will naturally—and appropriately—extend sub-

stantial deference to the government's assessment of such risks, but the "fiat of a governmental official, though senior in rank and doubtless honorable in the execution of official duties, cannot displace the judicial obligation to enforce constitutional requirements."[92] Nondisclosure orders should be narrowly tailored and, whenever possible, time limited to ensure recipients' speech rights are not constrained past the point necessary to protect national security. Similarly, the one-year delay imposed on challenges to the underlying orders—which denies recipients access to judicial review until long after the production of records—should also be removed.

While Section 215 could, in all likelihood, be made permanent if modified along these lines, it would be prudent to establish at least one additional sunset period to enable the Office of the Inspector General to audit the use of the amended authority—especially given that modifications to the National Security Letter statutes may substantially increase reliance on Section 215. If, as its proponents assert, this provision is not being used to engage in overbroad "fishing expeditions," these common-sense limitations should have a minimal practical effect on legitimate investigations.

National Security Letters

National Security Letters—once all but unknown to the general public—have emerged as perhaps the most controversial surveillance tool augmented by the Patriot Act and its successors, and with good reason.[93] This previously narrowly limited power was transformed into a sweeping mechanism enabling the FBI to acquire, without advance judicial approval, a wide array of sensitive information about Americans who are not even *suspected* of any connection with terrorism. As with Section 215 orders, the recipients are barred from disclosing the request. The ensuing explosion of NSLs has been characterized by government officials as a "hundred-fold increase over historic norms."[94] Perhaps unsurprisingly, the expanded authority has already been subject to what the inspector general called "widespread and serious misuse."[95]

NSLs have their origin in an exemption from federal privacy statutes created in the late 1970s, which permitted the voluntary disclosure of otherwise protected financial records when they concerned a suspected foreign spy. They have evolved over time into a set of extraordinarily broad compulsory tools akin to administrative subpoenas. NSLs now permit the FBI and certain other agencies to demand detailed financial records, consumer credit reports, and telecommunications transactional records without judicial authorization.[96] While there are currently five distinct NSL authorities, spread across four federal statutes, this paper will focus on the two types used exclusively by the FBI that account for the overwhelming majority of NSLs issued.

NSLs under the Right to Financial Privacy Act[97] are used to compel the production of records from "financial institutions," a statutorily defined category now encompassing a wide array of entities that, in the words of former Assistant Attorney General David Kris, "would not ordinarily be considered financial institutions."[98] NSLs under the Electronic Communications Privacy Act[99] are used to obtain telephone and Internet transaction records. They may be served on traditional telecommunications firms and Internet service providers, but also any other online service that gives users "the ability to send messages or communications to third parties"—such as Facebook, Gmail, or AOL Instant Messenger.[100] The precise range of records that can be obtained with ECPA NSLs is currently contested, but the FBI has traditionally asserted the right to demand—and has apparently received—almost anything short of actual communications content.[101] The language of the statute refers to "toll records"—traditionally meaning records of telephone numbers dialed and received—but in the modern era is generally understood

National Security Letters have emerged as perhaps the most controversial surveillance tool augmented by the Patriot Act with good reason.

to encompass Web IP addresses visited and e-mail sender and recipient addresses, at the very least.

The Patriot Act and subsequent intelligence legislation vastly expanded these authorities along multiple dimensions. The most significant is the removal of any requirement of a link to a suspected foreign power. Previously, NSLs applied only the records of persons suspected, on the basis of "specific and articulable facts," of being foreign spies (or to their contacts, if only basic subscriber information was sought).[102] In their current form, NSLs need only certify that the records sought are relevant to an authorized investigation, according to the FBI's own determination.

As the Justice Department itself explains, this "minimal evidentiary predicate . . . means that the FBI—and other law enforcement or Intelligence Community agencies with access to FBI databases—is able to review and store information about American citizens and others in the United States who are not subjects of FBI foreign counterintelligence investigations and about whom the FBI has no individualized suspicion of illegal activity."[103] While the more limited pre-Patriot authority required direct approval by a high-ranking official at FBI headquarters, power to issue NSLs has now been delegated to the Special Agents in Charge of all 56 FBI field offices.[104]

Even the weak limitation of a required connection to an authorized investigation is ultimately subject to executive branch discretion: two years *after* the passage of the Patriot Act, the Attorney General's guidelines for national security investigations were revised to permit "preliminary" inquiries—which the FBI acknowledges are subject to "no particular standard of proof"—to count as "authorized investigations."[105] Though previously restricted to full investigations, nearly half of the NSL requests in the years following the guideline change were issued in connection with preliminary inquiries.[106]

The problem was not inadequate information *collection*, but inadequate sharing and analysis of information already collected.

Later amendments also dramatically expanded the scope of NSLs for financial records, allowing them to be served not only on traditional financial institutions, such as banks and credit card companies, but also:

> insurance companies, pawnbrokers, dealers in precious stones or jewels, travel agencies, telegraph companies, licensed money transfer companies, automobile dealers, real estate closing companies, casinos, the Post Office, government agencies involved in financial transactions, and any other business "whose cash transactions have a high degree of usefulness in criminal, tax, or regulatory matters."[107]

RFPA NSLs, therefore, now cover "almost any record" in the custody of "virtually any commercial or government entity that handles cash transactions with customers."[108]

The Explosive Growth of Post-Patriot NSLs

Three extensive reports from the Office of the Inspector General show that the dramatic expansion of these authorities has led to an equally dramatic increase in their use.[109] While no reliable data exists for 2001–2002, the OIG counted nearly 200,000 NSL requests issued by the FBI from 2003–2006, with more than 56,000 issued in a single year—up from the 8,500 issued in 2000.[110] As the OIG notes, however, poor recordkeeping and reporting in the early years mean that the true figure is almost certainly substantially higher.[111]

Moreover, the proportion of those requests pertaining to U.S. persons has risen sharply over time. In 2003, roughly 39 percent of NSL requests were related to investigations of citizens or legal residents. By 2006, that figure had risen to 57 percent—meaning a total of 11,517 Americans had their records scrutinized pursuant to NSL authorities.[112]

The figures calculated by the OIG are not strictly comparable to those reported to Congress by the Department of Justice each year, which include only NSL requests pertaining to U.S. persons, and (perhaps more signifi-

cantly) exclude requests for basic subscriber information under ECPA's NSL authority. Despite these limitations, more recent reports suggest that the FBI continues to rely heavily on NSLs. In 2009, the most recent year for which reported figures are available, the FBI issued 14,788 NSL requests for information about 6,114 U.S. persons (again, not counting requests for basic subscriber information).[113]

The vast majority of those Americans are almost certainly not even suspected of involvement in espionage or terrorism. As then assistant attorney general David Kris explained in 2009, NSLs are used to "sweep more broadly than just the individual who may end up being the defendant or identified as a terrorist precisely because [investigators] are trying to develop the case."[114] NSLs are often used to map a "community of interest" based on an initial suspect's "calling circle," a process that may entail gathering information about persons "two or three steps removed" from the target.[115] Often FBI officials who signed off on boilerplate NSL language seeking broad "community of interest" data "were not even aware that they were making such requests."[116] As the OIG noted, given the statutory requirement that records be obtained via NSL only following a determination of relevance by designated officials, this practice "violated the ECPA, the Attorney General's NSI Guidelines, and FBI policy."[117]

More Letters, Diminishing Returns

Agents interviewed by the OIG have generally indicated that they find NSLs highly useful—but as with Section 215 orders, much of this usefulness consists in generating new leads and then eliminating the probable dead ends.[118] While this is, of course, an important goal, the ease of NSL information gathering may also lower the threshold for which leads are worth pursuing. It may even create a vicious cycle, where gathering more information generates more leads, requiring that still more information be collected in order to shrink the ballooning pool of potential suspects. As Michael Woods, a former senior FBI attorney has explained, reflecting on the post-9/11 climate at the Bureau:

> All of a sudden, every lead needed to be looked at. The atmosphere was such that you didn't want to be the guy who overlooked the next Moussaoui. . . . If you're telling the FBI people over and over you need to be preemptive, you need to get out there before something happens, you're pushing people toward a fishing expedition. We heard over and over again, connect the dots, and we were pushing the envelope and doing things that, in the old days, would have seemed beyond the pale.[119]

This makes sense, however, only if the inability to exhaustively pursue a large number of lower-threshold leads is a significant cause of intelligence failure. But there is little evidence for this proposition. Several perpetrators of the 9/11 terror attacks—notably Khalid al-Midhar and Nawaf al-Hazmi—were known al Qaeda associates who had been monitored by the Central Intelligence Agency well before they entered the United States. The failure to detect and disrupt that plot, then, cannot be attributed to an excessively high threshold for following up leads: those individuals plainly met any reasonable threshold for investigation, and indeed, could clearly have been extensively monitored pursuant to pre-Patriot authorities. As in the case of Zacarias Moussaoui, the problem was not inadequate information *collection*, but inadequate sharing and analysis of information already collected.[120] Other provisions of the Patriot Act and subsequent legislation have properly aimed to remedy some of these structural (and, indeed, cultural) problems—but it is far less clear that a paucity of raw data prior to the expansion of NSL authority was a genuine problem requiring a solution.

Any tool used as frequently as NSLs will, of course, retrospectively be seen to have played a role in some successful investigations. But

Investigative efforts are expanding, with easier access to records enabling a larger number of investigations to be pursued with a lower threshold of suspicion.

this is a poor metric of their general utility, especially when their primary function is preliminary filtering of large numbers of people to identify individuals—such as terrorists—with extremely low frequency in the population. We do not normally test the general public for very rare diseases, because even a very accurate test will tend to produce an unacceptably high number of false positives for each accurate diagnosis.[121] In intelligence no less than in epidemiology, the proper policy question is not whether any particular tool generates some data that is useful in a successful investigation, but whether it provides enough *necessary* information at the margin—information that could not have been obtained using (for example) a combination of narrower, pre-Patriot NSLs and judicially authorized Section 215 orders—to justify the costs of diminished privacy and resources expended chasing false positives. On the basis of these very considerations, an independent review by an expert panel of the National Research Council has cautioned against reliance on predictive data mining in the War on Terror.[122]

Records were improperly obtained on reporters for the *Washington Post* and the *New York Times*—in violation of both the law and internal regulations.

Though it is difficult to say definitively without access to classified records, publicly available data provides some reason to believe we have passed the point of diminishing returns. Of the fraction of FBI terror investigations ultimately referred to U.S. attorneys in 2001, immediately after the 9/11 attacks, 66 percent resulted in prosecutions in 2002. By 2009, the number had fallen to 21 percent—meaning federal prosecutors were declining to pursue nearly 80 percent of the cases referred to them by the FBI.[123] The average prison sentence for international terrorism prosecutions resulting in convictions fell from 40 months in 2004 to 5 months in 2006, suggesting that the great majority involved offenses substantially less serious than planned attacks on Americans.[124]

In short, it seems at least plausible that investigative efforts are expanding to fill the available space created by enhanced authorities, with easier access to records enabling a larger number of investigations to be pursued with a lower threshold of suspicion. If it is argued that NSLs are necessary to quickly sort through large numbers of ultimately unproductive leads, we should at least insist on evidence that there is some measurable benefit to opening so many investigations in the first place. It is telling, as the American Civil Liberties Union notes, that "every time an NSL recipient has challenged an NSL in court, the government has ultimately withdrawn its demand for records"—a pattern that is extremely difficult to reconcile with claims that those demands are essential to safeguard against terror attacks.[125]

After investigations are closed—and regardless of whether they result in prosecution, or any grounds for suspicion that the persons whose records have been obtained are guilty of anything—"once information is obtained in response to a national security letter, it is indefinitely retained and retrievable by the many authorized personnel who have access to various FBI databases."[126] Some 13,000 users, within both the FBI and other government agencies, have access to the billions of records contained in one of the most extensive databases, the Investigative Data Warehouse.[127] As recent large-scale releases of classified documents by the whistleblowing website WikiLeaks have shown, a single user in the digital era—whether acting from misguided idealism or more sinister motives—may be able to extract enormous quantities of sensitive information, even from putatively secure databases.[128]

A History of "Widespread and Serious Misuse"

Already, these sweeping authorities have been subject to widespread misuse. A review by the Electronic Frontier Foundation of some 800 violations of the law or internal guidelines reported to the Intelligence Oversight Board from 2001–2006 found that nearly a third involved National Security Letters.[129] Still more troubling, a small sample of case files reviewed by the OIG found that 22 percent contained potential violations that had *never* been reported, many involv-

ing the acquisition and retention of records beyond the legitimate scope of the NSL.[130]

Perhaps the most disturbing violations of the rules governing surveillance powers involve the use of so-called "exigent letters" and informal requests for telecommunications data to bypass the NSL approval and oversight process. Between 2003 and 2006, agents in the FBI's Communications Analysis Unit issued 722 of these exigent letters to obtain data from providers without appropriate legal process, often indicating that an NSL or subpoena would be provided later.[131] While ECPA does contain a provision covering disclosure in genuine emergencies, as when an attack is believed to be imminent, that exception was not invoked in these instances, and would have applied to only a tiny fraction of the putatively exigent cases.[132] Among those whose records were improperly obtained were reporters for the *Washington Post* and the *New York Times*—in violation of both the law and internal regulations requiring that the attorney general approve such requests.[133]

Still more incredibly, investigators sought records pertaining to more than 3,500 telephone numbers *without any process at all*, simply requesting records "verbally during telephone calls or visits to the providers' Communications Analysis Unit work stations, or on pieces of paper, such as Post-it notes."[134]

FBI officials would later attempt to cover these improprieties after the fact by issuing blanket NSLs covering hundreds of phone numbers.[135] But at least 266 phone numbers for which records were improperly acquired "were related to criminal investigations or domestic terrorism investigations for which NSLs are not an authorized technique under the ECPA NSL statute, the Attorney General's NSI Guidelines, or FBI policy."[136]

When the OIG interviewed the personnel responsible for these practices, it found that "no one could satisfactorily explain their actions," instead offering only "a variety of unpersuasive excuses."[137] Supervisors had, at one point, attempted to implement a database to track requests to telecommunications providers, but agents refused to use the new system "because they did not want the responsibility for inputting the data."[138] While it is conceivable that this reluctance stemmed from an extreme aversion to clerical work, it may also indicate that at least some of them may have had doubts about the legality of the prevailing practices. It is similarly telling that when information obtained by these extralegal means was later cited in the small sample of warrant applications to the secret Foreign Intelligence Surveillance Court reviewed by OIG, "FBI personnel filed inaccurate sworn declarations with the FISA Court to the effect that the subscriber or calling activity information was obtained in response to NSLs or a grand jury subpoena, when in fact the information was obtained by other means, such as exigent letters."[139] Again, while it is possible to ascribe these false statements to innocent error, they are also consistent with a desire to avoid FISC scrutiny of the use of exigent letters and informal requests.

The Nature of Intelligence Abuses

While the use of exigent letters was finally formally barred in 2007, it seems clear that the broad and discretionary nature of NSL authority was a key factor in allowing the practice to continue for several years—well after supervisors and Department of Justice attorneys became aware of it. While presumably *this particular form* of abuse is not now likely to continue, its scale and persistence confirms the general tendency for admirably dedicated investigators, precisely as a function of their dedication, to stretch the limits of their authority when unchecked by a neutral and detached magistrate. It demands too much to expect agents properly focused on what is expedient in a specific investigation to simultaneously balance their needs against the aggregate interest in preserving a general system of liberties and privacy protections.

Indeed, from a systemic perspective, excessive focus on particular "abuses" may be something of a red herring. It would, after

It would be troubling if the authority to acquire records were simply broadened so far that almost nothing counted as an abuse.

National Security Letters permit the collection and retention of an enormous amount of sensitive information about innocent Americans for the most part innocent.

all, be far more troubling if the authority to acquire records were simply broadened so far that almost nothing counted as an abuse. The real issue is that even if used precisely as intended, NSLs permit the collection and retention of an enormous amount of sensitive information about innocent Americans for the most part.

The history of intelligence abuses in the United States suggests that the existence of such large databases in itself increases the risk of abuse, even if the initial collection itself is consistent with the letter of the law. While our system of checks and balances is designed to exclude improperly obtained information at trial, historical abuses of intelligence surveillance have more often involved the extralegal use of information to intimidate or harass political dissidents, journalists, and even judges and legislators.[140] As the Senate committee headed by Sen. Frank Church summarized the results of its intensive investigation in the 1970s:

> Too many people have been spied upon by too many Government agencies and too much information has been collected. The Government has often undertaken the secret surveillance of citizens on the basis of their political beliefs, even when those beliefs posed no threat of violence or illegal acts on behalf of a hostile foreign power. The Government, operating primarily through secret informants, but also using other intrusive techniques such as wiretaps, microphone "bugs," surreptitious mail opening, and break-ins, has swept in vast amounts of information about the personal lives, views, and associations of American citizens. Investigations of groups deemed potentially dangerous—and even of groups suspected of associating with potentially dangerous organizations—have continued for decades, despite the fact that those groups did not engage in unlawful activity.
>
> Groups and individuals have been harassed and disrupted because of their political views and their lifestyles. Investigations have been based upon vague standards whose breadth made excessive collection inevitable. Unsavory and vicious tactics have been employed—including anonymous attempts to break up marriages, disrupt meetings, ostracize persons from their professions, and provoke target groups into rivalries that might result in dearths. Intelligence agencies have served the political and personal objectives of presidents and other high officials. While the agencies often committed excesses in response to pressure from high officials in the Executive branch and Congress, they also occasionally initiated improper activities and then concealed them from officials whom they had a duty to inform.[141]

In many cases—although not all—the initial monitoring of domestic targets was itself improper, and there has been an understandable tendency to see this as the sine qua non of abuse. But in a 21st-century technological context, an enormous quantity of information about group political activities, which previously would have been obtainable only via targeted direct surveillance, may be derivable by means of sophisticated analysis of telecommunications metadata swept up in the course of facially legitimate investigations. Under rules that permit the sweeping collection of such data—especially if dead-end leads are both numerous and disproportionately concern unpopular (but nonviolent) political and religious groups—the potential for inappropriate future use of information will not necessarily be linked with improper intent at the acquisition stage. Minimization rules limiting retention and dissemination of data—which should be strengthened—can mitigate this risk to some extent. But harms of this type are inherently difficult to detect, and the mere existence of such massive databases has the potential to chill protected political activity.

Just Another Subpoena?

Like Section 215 orders, National Security Letters are routinely defended on the grounds that they only grant intelligence investigators "the same" authority that is available to criminal investigators via such mechanisms as administrative or grand-jury subpoenas.[142] Even in the criminal context, it bears noting that the routine investigative use of third-party document subpoenas is a late 20th-century development that has occasioned fierce criticism from Fourth Amendment scholars.[143] But these analogies also typically elide a number of important and fundamental differences between NSLs and the subpoenas typically used in criminal investigations.

While the grand jury, as it exists today, is often subordinate to prosecutors in practice, the "theory of its function," as Justice Antonin Scalia has written, "is that it belongs to no branch of the institutional Government, serving as a kind of buffer or referee between the Government and the people."[144] This "unique role in our criminal justice system" is intimately related to its broad investigatory powers, which may be exercised in service of "determining whether or not a crime has been committed."[145] This function bears the greatest resemblance to the most frequent use of National Security Letters—as a tool for exhaustively following-up leads, typically in order to close off unpromising avenues of investigation—except that recipients of grand-jury subpoenas are generally not subject to indefinite gag orders barring disclosure of their own testimony. Trial subpoenas issued at the discretion of federal prosecutors, by contrast, are bound by more stringent procedural restrictions: they are typically tied to a particular criminal offense that there are grounds for believing has been or will be committed, and they are meant to be relatively narrowly calculated to produce admissible evidence of that offense.[146]

Perhaps the most important practical difference, however, is that National Security Letters are fundamentally secret tools whose recipients are, in most cases, indefinitely bound from disclosing even their existence to the general public. The details of their use typically remain shrouded, not merely for the duration of a specific investigation, but effectively forever. This not only removes one important kind of check on the agents using the authority, but also importantly alters the incentives facing the recipients of demands for information.

A comparison with the recent case of *Gonzales v. Google* is instructive here.[147] The Internet search-giant Google moved to quash a subpoena seeking a sample of user search queries, which the government hoped would be relevant to its defense of the controversial Child Online Protection Act against a challenge by the American Civil Liberties Union. The company made clear that a primary basis for its challenge was the fear of losing users' trust, and that "even a perception that Google is acquiescing to the Government's demands to release its query log would harm Google's business."[148] Though relatively unmoved by this "business goodwill" argument, the court *sua sponte* raised its independent concerns about the implications of the request on the privacy of Google's users, and ultimately rejected the demand for even anonymized query logs. While Google's reputational interest did not prove decisive in blocking the demand for information, it did provide an important motive for the judicial review that allowed user privacy interests to be weighed against the government's need for information.

Contrast the track record of National Security Letters, where in many cases employees from major telecommunications firms not only failed to object to improper requests, but were to a substantial degree the *instigators* of the abusive practices.[149] In the sample of reported violations surveyed by the Electronic Frontier Foundation, more than *half* of those related to NSLs occurred because "the private entity receiving the NSL either provided more information than requested or turned over information without receiving a valid legal justification from the FBI."[150] In one particularly egregious

The potential for inappropriate future use of collected telecommunications metadata will not necessarily be linked with improper intent at the acquisition stage.

case, a provider responded to a request for e-mail "header information" with "two CDs containing the full content of all e-mails in the accounts."[151] As EFF concluded:

> Companies were all too willing to comply with the FBI's requests, and —in many cases—the Bureau readily incorporated the over-produced information into its investigatory databases.[152]

This presents a potentially serious problem, because even where the Fourth Amendment does not protect data against disclosure, government searches of telecommunications records, in particular, may implicate distinct First Amendment interests. The permanent secrecy surrounding National Security Letters—which, again, appear to be used primarily to obtain information about people who are not ultimately found to be engaged in wrongdoing—means that the recipients will typically lack both the information that would be necessary to determine when a challenge on First Amendment grounds might be appropriate and, as importantly, the incentive to do so.

In many cases employees from major telecommunications firms not only failed to object to improper requests, but were the *instigators* of the abusive practices.

Where the Fourth Amendment Meets the First Amendment

As Justice Powell observed in his majority opinion in the *Keith* case, national security investigations "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."[153] These concerns are far from hypothetical: in at least one case noted by the Inspector General, the FBI initially sought a Section 215 order for records, which the FISA court denied on the basis of First Amendment concerns. The Bureau then proceeded to obtain the very same records using National Security Letters, even though the NSL statutes are nominally subject to the same First Amendment constraints as Section 215 orders.[154]

One obvious interest implicated by NSLs seeking information about Internet activities is that of anonymous speech. The Supreme Court has held that "an author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment."[155] The Constitution itself, after all, owes its existence in no small part to the pseudonymously-published pamphlets we now know as *The Federalist Papers*.

For this reason, a growing number of courts have found it appropriate to apply heightened standards to civil subpoenas whose purpose is to uncover the identity of an anonymous online speaker.[156] While the precise standards employed vary from court to court, common features include a requirement of notice (via an intermediary) to the defendant before his identity is disclosed to the plaintiff, some prima facie showing to establish the strength of the plaintiff's case, and a judicial balancing of the plaintiff's interest against the burden on speech entailed by disclosure.[157]

The First Amendment protects not only the right to speak, but also a corollary "right to receive information and ideas."[158] Thus, some legal scholars have argued for a parallel right to read anonymously, which could similarly be burdened by NSLs targeting websites hosting controversial content.[159] Here, too, courts have suggested that subpoenas seeking to reveal the reading habits of a target would be subject to heightened scrutiny.[160] The Supreme Court of Colorado has extended this logic to impose heightened standards, even upon probable-cause search warrants "directed to bookstores, demanding information about the reading history of customers," on the grounds that they "intrude upon the First Amendment rights of customers and bookstores because compelled disclosure of book-buying records threatens to destroy the anonymity upon which many customers depend."[161]

There is no obvious reason to think this logic any less applicable to the Internet than

to bookstores—and, indeed, substantial circumstantial evidence that users rely, if anything, *more* heavily on the sense of anonymity the Web provides. For example, 40 percent of Internet users, by one estimate, visit pornographic websites each month.[152] More than a third have visited sites related to sensitive personal issues, such as online support groups or sites providing information about medical conditions.[153] The willingness of users to seek information on such sensitive topics will often depend on the belief that they remain anonymous in doing so.

Finally, the Supreme Court has recognized a First Amendment interest in "expressive association," holding in *NAACP v. Alabama* that "immunity from state scrutiny of membership lists" may be necessary to preserve the "right of the members to pursue their lawful private interests privately and to associate freely with others in so doing."[154] This is, necessarily, an interest that does not turn on whether a third party entity has access to the data in question. It is also an interest especially likely to be implicated as government agencies use NSL-derived data for link analysis aimed precisely at inferring group structures from patterns of communication. In the context of the War on Terror, there is ample evidence that the practice of using NSLs to "follow every lead" is particularly likely to sweep in data about members of controversial (but peaceful) political and religious groups, even if only for the purpose of establishing the *absence* of a connection with more dangerous groups that may hold superficially similar radical views.[155]

Obviously, as organizations make use of e-mail and the Internet to communicate with and coordinate their membership, requests for telecommunications metadata will often tend to reveal such group associations—and when the organization itself is targeted, will be tantamount to straightforward acquisition of a membership roster. Suppose, for example, an NSL "community of interest" request takes as its starting point a member of a group mailing list devoted to political advocacy. The acquisition of the "second degree" transactional records for the list's e-mail address will not only, in effect, reveal the full membership list of the group, but is also likely to provide fairly detailed information about which are the most active participants. This is true not only with respect to traditional, formally incorporated political entities, but self-organizing ad-hoc groups, which legal scholar Katherine Strandburg has dubbed "emergent associations."[156] These kinds of informal, bottom-up associations may be especially sensitive to chilling effects, precisely because they will often lack the institutional resources to protect themselves possessed by more formal, traditional activist entities such as the NAACP.

National Security Letters, then, give us an unfortunate confluence of features. Confirming Justice Powell's warning, they seem especially likely to intrude on protected domains of religious or political speech and association, as they are used in a sweeping effort to preemptively identify the miniscule number of dangerous needles in a largely benign haystack. The extreme secrecy surrounding them, meanwhile, effectively eliminates the practical mechanism by which judicial scrutiny is often brought to bear when those interests are implicated by (intrinsically narrower) criminal investigations. All of this coincides with massively increased capabilities to process, share, and indefinitely store whatever data is obtained, exacerbating the risk that the aggregate information contained in government databases may be subject to pernicious uses unforeseen—and perhaps unforeseeable—at the time any particular piece of data is acquired.

National Security Letters seem especially likely to intrude on protected domains of religious or political speech and association.

Recommendations

There is little doubt investigators find NSLs useful and convenient. But given the risk to core civil-liberties interests posed by such sweeping and discretionary tools, convenience is an inadequate justification. The secret acquisition, without judicial approval, of sensitive records pertaining to presumptively innocent Americans should not be

The secret acquisition of sensitive records pertaining to presumptively innocent Americans should not be countenanced without clear evidence that it is necessary to the prevention of serious harm to national security.

countenanced without clear evidence that it is necessary to the prevention of serious harm to national security, and that any more limited authority would be insufficient to accomplish this goal. Nothing in the public record suggests that this burden can be met.

Of the five types of National Security Letters, ECPA NSLs for communications records present the most serious threat to protected privacy interests and civil-liberties interests. The Patriot Act's expansion of ECPA NSL authority to investigations designed to protect against international terrorism should be retained, along with the delegation of issuing authority to field offices, assuming ongoing centralized review. Its scope should otherwise be returned to its pre-Patriot limits. ECPA NSLs for "toll records" or their Internet equivalent should be limited to persons believed, on the basis of specific facts, to be agents of some foreign power. Any effort to expand their scope from toll records to electronic communications transaction records generally should be especially resisted, since the practical implications for privacy interests of such broad authority are effectively impossible to predict given the speed of technological change. More restricted NSLs, seeking basic subscriber information, should be available for persons in direct communication with those suspected agents.

This structure properly balances the need for investigative flexibility with the privacy interests of largely innocent parties. It allows analysts to determine the identities of persons with whom actual investigative subjects are in contact, but does not permit the exposure of potentially sensitive patterns of communication and association on the basis of any casual link to a single suspect. In combination with evidence obtained by other investigative means, this should enable agents to establish which persons require further scrutiny.

If there is some reason to think the records of particular parties in contact with a target are relevant to the investigation, but there are insufficient grounds for concluding that those parties are themselves agents of a foreign power, the information obtained at that stage can be employed to make the requisite showing to the FISA court for a Section 215 order seeking more-detailed records. This structure *still* grants enormous flexibility to investigators, permitting access to records pursuant to a relatively permissive standard, but ensures that records implicating core speech and association interests are not routinely obtained about innocent persons without the approval of an independent magistrate. While it may be tempting to insist that a court order be obtained for *all* records, this could have the perverse consequence of yielding greater intrusion, as agents would have an incentive to sweep as broadly as possible in a single order—obviating the need for multiple applications—even when more-limited records would suffice.

A similar process should obtain for financial-record NSLs. That is, they should permit investigators to obtain detailed records only for persons believed, on the basis of specific facts, to be agents of foreign powers. They may also permit identification of other parties to those transactions—such as the recipient of a wire transfer. Records of *those* parties, however, should be acquired pursuant to a Section 215 order following a judicial determination that the records are relevant. Because full credit reports generally contain less-sensitive and detailed information, and are attended by lesser expectations of privacy, the current standard for credit report NSLs may be adequate, provided future audits confirm they are being used in an appropriately narrow fashion.

As with Section 215 orders, the gag provisions of the NSL statutes should be modified to conform to the ruling in *Doe v. Mukasey*.[167] The oversight and minimization procedures which the Justice Department has already agreed to implement on a voluntary basis should similarly be codified in statute to ensure they are not quietly eroded by the decisions of future administrations.[168] In particular, when an investigation is closed without further legal or intelligence action

being taken, records obtained in the course of that investigation should be purged from FBI databases, by default, after some fixed period of time. There is no legitimate reason to indefinitely retain detailed information about tens of thousands of Americans who are not suspected of involvement in terror or espionage. Notwithstanding any changes, the myriad problems already identified with the use of National Security Letters, and the incredible scale of their use, suggests that this expanded authority should be subject to a sunset and regular auditing by the Inspector General to ensure that they are subject to continuing review.

Conclusion

It has become commonplace over the last decade to speak of the need to balance privacy and security interests. While it is certainly true that trade-offs between these values are sometimes inevitable, we should not allow the metaphor to mislead us into viewing them as inherently conflicting. Often we can have both.

The reforms proposed in this paper are guided by that principle: they seek to limit the government's ability to invade the privacy of innocent Americans without compromising the effectiveness of tools the intelligence community truly requires to detect and apprehend terrorists. In the climate of panic and uncertainty following the attacks of 9/11—with no clear understanding of how the attackers had gone undetected, how many more might be waiting to strike again, or what methods might prove necessary to detect them—it should not be surprising that we erred on the side of granting government more power with fewer restrictions. Now, with the benefit of a decade's experience, we have an opportunity to do better.

Notes

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

2. Editorial, "Stampeded in the House," *Washington Post*, October 16, 2001.

3. Pub. L. No. 108-458 and 118 Stat. 3638 §6001. References throughout this paper to "Patriot provisions" or "Patriot authorities" should be understood as shorthand encompassing Lone Wolf and other changes to surveillance powers made by subsequent legislation.

4. USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. 109-177, 120 Stat. 192–277 (2006). For further background on the three sunsetting provisions, see Anna C. Henning and Edward C. Liu, "Amendments to the Foreign Intelligence Surveillance Act Set to Expire in 2009," CRS Report R40138, December 23, 2009.

5. For a more detailed account, see Brian T. Yeh and Charles Doyle, "USA PATRIOT Improvement and Reauthorization Act of 2005: A Legal Analysis," CRS Report RL33332, December 21, 2006.

6. See, for example, House Judicary Committee, "Hearing on the USA PATRIOT Act," September 22, 2009, http://judiciary.house.gov/hearingshear_090922.html; and Senate Judiciary Committee "Reauthorizing the USA PATRIOT Act: Ensuring Liberty and Security," September 23, 2009, http://judiciary.senate.gov/hearings/hearing.cfm?id=4062.

7. The most serious abuses are documented in Office of the Inspector General, "A Review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records," January 2010, http://www.justice.gov/oig/special/s1001r.pdf. For a summary of earlier findings of improprieties, see David Stout, "F.B.I. Head Admits Mistakes in Use of Security Act," *New York Times*, March 10, 2007, http://www.nytimes.com/2007/03/10/washington/10fbi.html.

8. Hearing on the Report by the Office of the Inspector General of the Department of Justice on the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records, April 14, 2010, http://judiciary.house.gov/hearings/hear_100414.html. See also the earlier Hearing on: H.R. 3189, the "National Security Letters Reform Act of 2007," April 10, 2008, http://judiciary.house.gov/hearings/hear_041508.html.

9. See, for example, Charlie Savage, "Battle Looms Over the Patriot Act," *New York Times*, September 20, 2009, http://www.nytimes.com/2009/09/20/us/politics/20patriot.html.

10. For a summary of the main proposals and how they would have differed from current law, see the comparison chart produced by the American Civil Liberties Union, "Comparison Chart," September 30, 2009, http://www.aclu.org/images/general/asset_upload_file577_41249.pdf; and "A Breakdown of the H.R. 3845, The USA PATRIOT Amendments Act of 2009," October 27, 2009, http://www.aclu.org/national-security/breakdown-hr-3845-usa-patriot-amendments-act-2009. The American Association of Law Libraries' Issue Brief "USA PATRIOT ACT and PATRIOT Reauthorization: Section 215," June 2010, http://www.aallnet.org/aallwash/ib082009.pdf, includes a detailed timeline of reform proposals and legislative action.

11. Michael B. Farrell, "Obama signs Patriot Act extension without reforms," *Christian Science Monitor*, March 1, 2010, http://www.csmonitor.com/USA/Politics/2010/0301/Obama-signs-Patriot-Act-extension-without-reforms.

12. David Kravetz, "House Fails to Extend Patriot Act Spy Powers," *Wired*, February 8, 2011, http://www.wired.com/threatlevel/2011/02/patriot-act-notextended/.

13. Thomas Ferraro and Phillip Barbara, "Congress votes to renew anti-terrorism powers," *Reuters*, February 17, 2011, http://www.reuters.com/article/2011/02/17/us-usa-security-congress-idUSTRE71G47T20110217.

14. S. 149, "To extend expiring provisions of the USA PATRIOT Improvement and Reauthorization Act of 2005, the Intelligence Reform and Terrorism Prevention Act of 2004, and the FISA Amendments Act of 2008 until December 31, 2013, and for other purposes," http://www.govtrack.us/congress/billtext.xpd?bill=s112-149.

15. Fahima Haque, "GOP Senators Back Permanent Extension of Patriot Act," February 4, 2011, http://www.mainjustice.com/2011/02/04/gop-senators-back-permanent-extension-of-patriot-act/

16. Press Release, "Leahy Renews Effort To Extend Expiring PATRIOT Act Authorities, Increase Oversight," January 26, 2011, http://leahy.senate.gov/press/press_releases/release/?id=16e3e765-00e7-48eb-add7-a64f415e9c1d. For a more detailed overview of proposals, see Edward C. Liu, "Amendments to the Foreign Intelligence Surveillance Act (FISA) Set to Expire February 28, 2011," CRS Report R40138 (February 10, 2011), http://www.fas.org/sgp/crs/intel/R40138.pdf; and Charles Doyle, *National Security Letters: Proposals in the 112th Congress*, CRS Report R41619, February 1, 2011.

17. P.L. 107-56, § 224(b); P.L. 108-458, § 6001(b).

18. See "Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities," S. REP. NO. 94-755 (1976) [hereinafter "Church Committee Report"].

19. The letter is available at http://www.wired.com/threatlevel/2009/09/obama-backs-expiring-patriot-act-spy-provisions/.

20. See, for example, Amy Zegart, *Spying Blind: The CIA, the FBI, and the Origins of 9/11* (Princeton: Princeton University Press, 2007).

21. Liu and Henning, above at note 4.

22. Patrick Leahy, Charles Grassley, and Arlen Specter: "Interim Report on FBI Oversight in the 107th Congress by the Senate Judiciary Committee: FISA Implementation Failures," February 2003, http://www.fas.org/irp/congress/2003_rpt/fisa.html.

23. Ibid. §III(C)(1).

24. *United States v. U.S. District Court*, 407 U.S. 297 (1972). Although FISA wiretaps—unlike those at issue in the Keith case—do involve advance judicial approval, the Foreign Intelligence Surveillance Court has acknowledged that because surveillance orders under FISA and Title III "diverge in constitutionally relevant areas—in particular, in their probable cause and particularity showings—a FISA order may not be a 'warrant' contemplated by the Fourth Amendment." In re: Sealed Case, 310 F.3d 717 (2002).

25. *Id.*, majority opinion of Justice Powell at 309. See also *United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980), holding that the foreign intelligence exception to the conventional Fourth Amendment warrant requirement applies "only when the object of the search or the surveillance is a foreign power, its agent or collaborators" because of the enhanced "need for speed, stealth, and secrecy" as well as "difficult and subtle judgments about foreign and military affairs."

26. See Peter P. Swire, "The System of Foreign Intelligence Surveillance Law," 72 *Geo. Wash. L. Rev.* 1306 (2004), section II.

27. See letter from Roland Weich, above at note 17.

28. See H.R. Rep. No. 1283, Pt. I, 95th Cong., 2d Sess. 1978 U.S.C.C.A.N. 4048 (June 8, 1978) at 43.

29. See David S. Kris and J. Douglas Wilson, *National Security Investigations & Prosecutions* (Eagan,

MN: Thomson/West, 2007) §8 [hereinafter "Kris and Wilson"].

30. Transactional Records Access Clearinghouse, "Who is a Terrorist," September 28, 2009, http://trac.syr.edu/tracreports/terrorism/215/.

31. Named for the Omnibus Crime Control and Safe Streets Act of 1968, Title III, Pub. L. 90-351, 82 Stat. 212 (June 19, 1968) (codified as amended at 18 U.S.C. §§2510-22) [hereinafter "Title III"].

32. In re *All Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F. Supp. 2d 611 (2002).

33. Kris and Wilson, §9:4.

34. *U.S. v. Sattar*, 2003 WL 22510435 (S.D. N.Y. 2003).

35. See notes 50–52, below, and accompanying text.

36. Carrie Johnson, "Director of FBI Urges Renewal of Patriot Act," *Washington Post*, March 26, 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/03/25/AR2009032501862.html.

37. Electronic Communications Privacy Act of 1986, Pub. L. 99-508, §106(d)(3), codified at 18 U.S.C. §2581(11). For a more detailed history, see Peter M. Thompson, "White Paper on The USA PATRIOT Act's 'Roving' Electronic Surveillance Amendment to the Foreign Intelligence Surveillance Act" (Washington: The Federalist Society, April 2004), http://www.fed-soc.org/publications/pubID.130/pub_detail.asp.

38. See, for example, James X. Dempsey, "Why Section 206 Should Be Modified" in *Patriot Debates: Experts Debate the USA PATRIOT Act*, ed. Stewart A. Baker and John Kavanaugh (Chicago: ABA Publishing, 2005), http://www.abanet.org/natsecurity/patriotdebates/section-206, which raises many of the concerns outlined here while agreeing that "It makes perfect sense that the FBI should have roving tap authority in intelligence investigations of terrorists."

39. The "particularity" requirement is meant to limit the discretion of officers executing a warrant. See *Maryland v. Garrison*, 480 U.S. 79, 84, 107 S. Ct. 1013, 94 L. Ed. 2d 72 (1987).

40. See Kris and Wilson §6:12.

41. Administrative Office of the United States Courts, "Wiretap Report 2009," April 2010, http://www.uscourts.gov/Statistics/WiretapReports/WiretapReport2009.aspx.

42. *United States v. Bianco*, 998 F.2d 1112 (2d Cir. 1993), cert. denied, 114 S. Ct. 1644 (1994).

43. *United States. v. Petti*, 973 F.2d 1441 (9th Cir. 1992), cert. denied, 113 S. Ct 1859 (1993).

44. See Mark Rumold, "Documents Obtained by EFF Reveal FBI Patriot Act Abuses," *Deeplinks Blog*, March 31, 2011, https://www.eff.org/deeplinks/2011/03/documents-obtained-eff-reveal-fbi-patriot-act.

45. See note 31.

46. "FBI Typo Triggers Errant E-Mail Search," *The Smoking Gun*, December 3, 2010, http://www.thesmokinggun.com/documents/fail/fbi-typo-triggers-errant-e-mail-search.

47. Remarks of Joel M. Margolis at the ISS World Americas Conference on the panel "Regulatory and CALEA Issues Facing Telecom Operators Deploying DPI Infrastructure," October 13, 2009. A link to a recording of the panel by security researcher Chris Soghoian is at http://paranoia.dubfire.net/2010/01/who-is-neustar.html.

48. For an introduction to DPI technology and analysis of its interaction with surveillance law, see Paul Ohm ,"The Rise and Fall of Invasive ISP Surveillance" *University of Illinois Law Review* 1417 (2009), http://ssrn.com/abstract=1261344.

49. See note 42.

50. See Yeh and Doyle, above at note 5, pp. 16–18.

51. Office of the Inspector General, "The Federal Bureau of Investigation's Foreign Language Translation Program (Redacted for Public Release)," Audit Report 10-02, October 2009, http://www.justice.gov/oig/reports/FBI/a1002 redacted.pdf.

52. 18 U.S.C. §2518(8)(d).

53. See Kris and Wilson §22:1.

54. *Id.* §27–§30.

55. The orders could be served on "a common carrier, public accommodation facility, physical storage facility, or vehicle rental facility." Pub. L. 105-282, Title II, §215, 112 Stat. 2411 (October 20, 1998); 50 U.S.C. §1672(a) (1998).

56. Office of the Inspector General, "A Review of the Federal Bureau of Investigation's Use of Section 215 Orders for Business Records," March, 2007, http://www.usdoj.gov/oig/special/s0703a/final.pdf [hereinafter OIG 215 Report I].

57. *John Doe, Inc. v. Mukasey*, 549 F.3d 861 (2d Cir. 2008).

58. 50 U.S.C. §1861(f)(2)(ii).

59. 50 U.S.C. §1861(b)(2)(a).

60. Kris and Wilson §18:3.

61. See Yeh and Doyle, above at note 5, and OIG 215 Report I, pp. ii v.

62. *Id.* note 59.

63. See *United States v. Miller*, 425 U.S. 435 (1976); *Smith v. Maryland*, 442 U.S. 735 (1979).

64. 147 Cong. Rec. S10993 (October 25, 2001).

65. See, for example, "USA PATRIOT Act Debate," *PBS NewsHour*, PBS, December 13, 2005, http://www.pbs.org/newshour/bb/congress/july-dec05/patriot_12-13.html. For a more detailed discussion of differences between these authorities, see notes 140–150 below and accompanying text.

66. For a very partial sample, see Daniel Solove, "The Fourth Amendment, Records, and Privacy," in *The Digital Person: Technology and Privacy in the Information Age* (New York: NYU Press, 2004); Christopher Slobogin, *Privacy at Risk: The New Government Surveillance and the Fourth Amendment* (Chicago: University of Chicago Press, 2007) pp. 151–64; Gerald G. Ashdown, "The Fourth Amendment and the 'Legitimate Expectation of Privacy,'" *Vand. L. Rev.* 34 (1981): 1289, 1315; Patricia Bellia, "Surveillance Law Through Cyberlaw's Lens," *Geo. Wash. L. Rev.* 72 (2004): 1375, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=556467; Jack M. Balkin, "The Constitution in the National Surveillance State," *Minn. L. Rev.* 93 (2008): 1, 19; Stephen E. Henderson, "Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too," *Pepp. L. Rev.* 34 (2007): 975–76; Susan Freiwald, "First Principles of Communications Privacy," *Stan. Tech. L. Rev.* 3 (2007): 46–49, http://stlr.stanford.edu/pdf/freiwald-first-principles.pdf; Jim Harper, "Reforming Fourth Amendment Privacy Doctrine," *American University Law Review* 58 (June 2008): 5, http://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1045; Matthew Tokson, "Automation and the Fourth Amendment," *Iowa L. Review* 96 (2010) 581–647, http://www.uiowa.edu/~ilr/issues/ILR_96-2_Tokson.pdf.

67. Orin S. Kerr, "The Case for the Third-Party Doctrine," 107 *Mich. L. Rev.* (2009), http://ssrn.com/abstract=1138128.

68. See Stephen E. Henderson, "Learning from All Fifty States: How To Apply the Fourth Amendment and Its State Analogs To Protect Third Party Information from Unreasonable Search," *Cath. U. L. Rev.* 55 (2006): 373.

69. See *Murdock v. State*, 664 P.2d 589, 598 (Alaska Ct. App. 1983) ("[The petitioner] had a reasonable expectation of privacy in the property stored [in a rented locker] at the YMCA."); *Ferris v. State*, 640 S.W.2d 636, 638 (Tex. App. 1982) ("Under proper circumstances, a storage locker is a place entitled to Fourth Amendment . . . protection.")

70. *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

71. In re Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F. 3d 304, 319 (3d Cir. 2010) at 317.

72. See, for example, Kashmir Hill, "History Sniffing: How YouPorn Checks What Other Porn Sites You've Visited and Ad Networks Test The Quality of Their Data," *Forbes*, November 30, 2010, http://blogs.forbes.com/kashmirhill/2010/11/30/history-sniffing-how-youporn-checks-what-other-porn-sites-youve-visited-and-ad-networks-test-the-quality-of-their-data/.

73. See notes 151–64 below and accompanying text.

74. 50 U.S.C. 1861(c).

75. See OIG 215 Report I at viii. Ironically, the Justice Department appears to have been more conservative than Congress: the OIG report explains that the Office of Legal Counsel initially concluded that Section 215 did not override separate statutory protections for sensitive educational and medical records. Only when Congress explicitly established heightened standards for acquisition of such records—apparently believing itself to be *raising* the level of protection afforded them—did OLC authorize their acquisition pursuant to this authority. Language in a subsequent Inspector General's report suggests that Justice Department attorneys remain reluctant to process requests that do not fall within the traditional definition of business records, however. See Office of the Inspector General, "A Review of the FBI's Use of Section 215 Orders for Business Records in 2006," March 2008, http://www.justice.gov/oig/special/s0803a/final.pdf [hereafter OIG 215 Report II] at 48.

76. In 2005, 141 "combination" orders under Section 215 were issued in tandem with "pen register" orders, which permit monitoring of numbers dialed from a target phone, in order to

obtain subscriber information about persons in communication with the primary target. Following the 2006 reauthorization, this information can be obtained automatically under the pen register order alone.

77. See Ronald Weich, "FISA Annual Report to Congress 2009," April 30, 2010, http://www.fas.org/irp/agency/doj/fisa/2009repc.pdf.

78. In 2006, the average processing time for approved Section 215 orders was 147 days and even longer for applications ultimately withdrawn. Tellingly, no agents interviewed by the Inspector General could identify any harm to national security as a result of these delays. OIG 215 Report II at 43.

79. *Id.* at 55.

80. OIG 215 Report I at 54.

81. See American Library Association, "Resolution on the USA PATRIOT Act and Libraries," June 29, 2005, http://www.ala.org/ala/aboutala/offices/oif/statementspols/ifresolutions/usapatriotactlibraries.cfm.

82. OIG 215 Report I at 28.

83. Testimony of Todd Hinnen, House Judiciary Committee Hearing, above at note 6.

84. Statement of Sen. Russ Feingold, Senate Judiciary Committee Hearing, above at note 6, http://judiciary.senate.gov/hearings/testimony.cfm?id=4062&wit_id=4083.

85. Remarks of Sen. Richard Durbin, Senate Judiciary Committee "Executive Business Meeting," October 1, 2009) http://judiciary.senate.gov/resources/webcasts/index.cfm?changedate=09-28-09&p-all.

86. Remarks of Sen. Russ Feingold, *ibid.*

87. See Tokson, above at note 64. Note that the government has argued successfully and plausibly—that purely automated filtering of electronic communications for the purpose of isolating those belonging to a surveillance target does not constitute "interception" of all filtered communications. This argument seems difficult to square with the premise that persons normally waive their expectation of privacy in data similarly processed by private entities. See testimony of Donald M. Kerr Assistant Director, Laboratory Division, FBI, Before the U.S. Senate Committee on the Judiciary (September 6, 2000), http://www.loc.gov/law/find/hearings/pdf/00089583263.pdf.

88. See Leahy press release, above at note 16.

89. This tripartite scheme is based on the proposal previously approved unanimously by the Senate, and reintroduced in 2009 by Sen. Russ Feingold as part of the Judiciously Using Surveillance Tools In Counterterrorism Efforts (JUSTICE) Act, http://www.eff.org/files/HEN09874.pdf.

90. *Doe v. Mukasey*, note 56, above.

91. 50 U.S.C. §1862(f)(2)(C).

92. *Doe v. Mukasey* at 47, above at note 56.

93. A search by Prof. Peter Swire turned up only two brief mentions of NSLs in newspaper stories written prior to 2002. See testimony of Peter P. Swire before the U.S. Senate Judiciary Committee's Subcommittee on the Constitution, "Responding to the Inspector General's Findings of Improper Use of National Security Letters by the FBI," April 11, 2007, http://judiciary.senate.gov/hearings/hearing.cfm?id-2679.

94. Barton Gellman, "The FBI's Secret Scrutiny; In Hunt for Terrorists, Bureau Examines Records of Ordinary Americans," *Washington Post*, November 6, 2005, http://www.washingtonpost.com/wp-dyn/content/article/2005/11/05/AR2005110501366.html.

95. Statement of Glenn A. Fine Inspector General, U.S. Department of Justice, House Judiciary Committee Hearing "Misuse of Patriot Act Powers: The Inspector General's Findings of Improper Use of National Security Letters by the FBI," March 21, 2007, http://judiciary.senate.gov/hearings/hearing.cfm?id-2616.

96. For detailed background see Kris and Wilson §19:2; Charles Doyle, *National Security Letters in Foreign Intelligence Investigations: Legal Background and Recent Amendments*, CRS Report RL33320, September 8, 2009, www.fas.org/sgp/crs/intel/RL33320.pdf; Swire above at note 25.

97. 12 U.S.C. §3414.

98. Kris and Wilson §19:2 note 16; see note 105 below and accompanying text for examples.

99. 18 U.S.C. §2709.

100. See U.S. Department of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence* (2009) §3(B), http://www.cybercrime.gov/ssmanual/03ssma.html#B.1; *Kaufman v. Nest Seekers*, LLC, 2006 WL 2807177, at note 5 (S.D.N.Y. Sept. 26, 2006); Becker v. Toca, 2008 WL 4443050, at note 4 (E.D. La. September 26, 2008).

101. See Ellen Nakashima, "White House pro-

posal would ease FBI access to records of Internet activity," *Washington Post*, July 29, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/07/28/AR2010072806141.html.

102. Statement of Glenn A. Fine.

103. U.S. Department of Justice, "FY 2006 Performance and Accountability Report," http://www.justice.gov/ag/annualreports/pr2006/2006par.pdf.

104. See Swire, above at note 92.

105. See Testimony of Lisa Graves, Senate Judiciary Committee hearing, above at note 6.

106. U.S. Department of Justice, Office of the Inspector General, "A Review of the Federal Bureau of Investigation's Use of National Security Letters," March 2007, [hereinafter OIG NSL Report I].

107. Kris and Wilson §19:5, summarizing 31 U.S.C. §§5312(a)(2) & (c)(1).

108. *Id.*

109. See OIG NSL Report I; "A Review of the FBI's Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006," March 2008 [hereinafter OIG NSL Report II]; "A Review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records," January 2010 [hereinafter OIG NSL Report III], http://www.usdoj.gov/oig/special/index.htm.

110. OIG NSL Report II at 9. NSL *requests* are counted rather than simply NSLs because a single physical letter may contain multiple discrete demands for information and in a few cases, hundreds.

111. See OIG NSL Report I at xlv. ("Overall, we found approximately 17 percent more national security *letters* and 22 percent more national security letter *requests* in the case files we examined in four field offices than were recorded in the OGC database. As a result, we believe that the total number of NSL requests issued by the FBI is significantly higher than the FBI reported.")

112. *Id.* note 108.

113. *Id.* note 76.

114. Remarks of David Kris, Senate Judiciary Committee Hearing, above at note 6, http://www.fas.org/irp/congress/2009_hr/patriot2.html.

115. See OIG NSL Report I at 109; OIG NSL Report III at 54–64.

116. OIG NSL Report III at 57.

117. *Id.* at 60.

118. OIG NSL Report II at 114.

119. Eric Lichtblau, *Bush's Law: The Remaking of American Justice* (New York: Pantheon, 2008) p. 92.

120. See Zegart, above note 20, chap. 1; James Bamford, *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America* (New York: Doubleday, 2008), Book I.

121. See Jeff Jonas and Jim Harper, "Effective Counterterrorism and the Limited Role of Predictive Data Mining," Cato Institute Policy Analysis no. 584, December 11, 2006, http://www.cato.org/pub_display.php?pub_id=6784.

122. See National Research Council, *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment* (Washington: National Academies Press, 2008).

123. Transactional Records Access Clearinghouse, "As Terrorism Prosecutions Decline, Extent of Threat Remains Unclear," May 18, 2010, http://trac.syr.edu/tracreports/terrorism/231/.

124. Transactional Records Access Clearinghouse, "National Profile and Enforcement: Trends Over Time," 2006, http://trac.syr.edu/tracfbi/newfindings/current/.

125. See American Civil Liberties Union, "Internet Archive's NSL Challenge," April 29, 2008, http://www.aclu.org/national-security/internet-archives-nsl-challenge.

126. OIG NSL Report I at 110.

127. Ellen Nakashima, "FBI Shows Off Counterterrorism Database," *Washington Post*, August 30, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/08/29/AR2006082901520.html.

128. See Thom Shanker, "Loophole May Have Aided Theft of Classified Data," *New York Times*, July 9, 2010, https://www.nytimes.com/2010/07/09/world/09breach.html.

129. Electronic Frontier Foundation, "Patterns of Misconduct: FBI Intelligence Violations from 2001–2008" (January 2011), http://www.eff.org/pages/patterns-misconduct-fbi-intelligence-violations.

130. OIG NSL Report I at xxxiii.

131. See OIG NSL Report III at 25–44.

132. *Id.*, table 4.3 at 198.

133. *Id.* at 89–122.

134. *Id.* at 45.

135. *Id.* at 137–212.

136. *Id.* at 208.

137. *Id.* at 66.

138. *Id.* at 151.

139. *Id.* at 122..

140. See generally Ivan Greenberg, *The Dangers of Dissent: The FBI and Civil Liberties Since 1965* (Lanham, MD: Lexington Books, 2010); Athan Theoharis, *The FBI and American Democracy: A Brief Critical History* (Lawrence, KS: University of Kansas Press, 2004).

141. Church Committee Report, Book II.

142. See notes 63–64 above and accompanying text.

143. Christopher Slobogin, "Subpoenas and Privacy," 54 *DePaul L. Rev.* 805, 813–14 (2005).

144. *United States v. Williams*, 504 U.S. 36 at 48 (1992).

145. *United States v. R. Enterprises*, 498 U.S. 292 (1991).

146. See, for example, *United States v. Nixon*, 418 U.S. 683 (1974).

147. *Gonzales v. Google*, Inc., No. 5:06-mc-80006-W (N.D. Cal. Mar. 17, 2006).

148. *Id.*

149. See OIG NSL Report III, at 14–25.

150. "Patterns of Misconduct," note 26, above, at 8.

151. *Id.*

152. *Id.*

153. *United States v. U.S. District Court*, note 23, above.

154. OIG 215 Report II at 65–74.

155. *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995).

156. See *Doe v. 2TheMart.com Inc.*, 140 F. Supp. 2d 1088 (W.D. Wash. 2001); *Columbia Ins. Co. v. Seescandy.com*, 185 F.R.D. 573 (N.D. Cal. 1999); *Mobilisa, Inc. v. Doe 1*, 170 P.3d 712 (Ariz. Ct. App. 2007); *Krinsky v. Doe 6*, 72 Cal. Rptr. 3d 231 (Ct. App. 2008); *Doe No. 1 v. Cahill*, 884 A.2d 451 (Del. 2005); *Dendrite Int'l, Inc. v. Doe*, No. 3, 775 A.2d 756 (N.J. Super. Ct. App. Div. 2001); In re *Subpoena Duces Tecum to Am. Online, Inc.* (In re *AOL*), 52 Va. Cir. 26 (Cir. Ct. 2000), *rev'd on other grounds sub nom., Am. Online, Inc. v. Anonymous Publicly Traded Co.*, 542 S.E.2d 377 (Va. 2001).

157. Nathaniel Gleicher, "John Doe Subpoenas: Toward a Consistent Legal Standard," *Yale L.J.* 118 (2008): 320, http://www.yalelawjournal.org/the-yale-law-journal/content-pages/john-doe-subpoenas:-toward-a-consistent-legal-standard/.

158. *Stanley v. Georgia* 394 U.S. 557 (1969).

159. Julie E. Cohen, "A Right to Read Anonymously: A Closer Look at 'Copyright Management' in Cyberspace," *Conn. L. Rev.* 28 (1996): 981, http://ssrn.com/abstract=17990.

160. In re *Grand Jury Subpoena to Kramerbooks & Afterwords Inc., Med. L. Rptr.* 26 (D.D.C. 1998): 1599.

161. *Tattered Cover, Inc. v. City of Thornton*, 44 P.3d 1044, 1054. (Colo. 2002).

162. See David Crary, "Battle Brews as Porn Moves into Mainstream," *Breitbart.com*, April 1, 2006, http://www.breitbart.com/article.php?id=D8GNH P902&show_article=1.

163. Press Release, Pew Internet & Am. Life Project, Pew Research Ctr., "86% of Internet Users Want to Prohibit Online Companies from Disclosing Their Personal Information Without Permission," August 21, 2000, http://www.pewinternet.org/Press-Releases/2000/86-of-Internet-Users-Want-to-Prohibit-Online-Companies-From-Disclosing-Their-Personal-Inf.aspx.

164. *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449, 460–63 (1958).

165. See Linda E. Fisher, "Guilt by Expressive Association: Political Profiling, Surveillance and the Privacy of Groups," *Ariz. L. Rev.* 46 (2004): 621, 625, 662 n.224.

166. Katherine J. Strandburg, "Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance," *Boston College L. Rev.* 49 (2008): 741, http://works.bepress.com/katherine_strandburg/15.

167. See notes 89–90 and accompanying text.

168 See Press Release, "DOJ To Implement Provisions Of Leahy-Authored Patriot Act Re-authorization Proposal," December 9, 2010, http://leahy.senate.gov/press/press_releases/release/?id=355bb191-f539-4f78-a6f2-8a49e85c7c0b.

STUDIES IN THE POLICY ANALYSIS SERIES

674. **Fannie Mae, Freddie Mac, and the Future of Federal Housing Finance Policy: A Study of Regulatory Privilege** by David Reiss (April 18, 2011)

673. **Bankrupt: Entitlements and the Federal Budget** by Michael D. Tanner (March 28, 2011)

672. **The Case for Gridlock** by Marcus E. Ethridge (January 27, 2011)

671. **Marriage against the State: Toward a New View of Civil Marriage** by Jason Kuznicki (January 12, 2011)

670. **Fixing Transit: The Case for Privatization** by Randal O'Toole (November 10, 2010)

669. **Congress Should Account for the Excess Burden of Taxation** by Christopher J. Conover (October 13, 2010)

668. **Fiscal Policy Report Card on America's Governors: 2010** by Chris Edwards (September 30, 2010)

667. **Budgetary Savings from Military Restraint** by Benjamin H. Friedman and Christopher Preble (September 23, 2010)

666. **Reforming Indigent Defense: How Free Market Principles Can Help to Fix a Broken System** by Stephen J. Schulhofer and David D. Friedman (September 1, 2010)

665. **The Inefficiency of Clearing Mandates** by Craig Pirrong (July 21, 2010)

664. **The DISCLOSE Act, Deliberation, and the First Amendment** by John Samples (June 28, 2010)

663. **Defining Success: The Case against Rail Transit** by Randal O'Toole (March 24, 2010)

662. **They Spend WHAT? The Real Cost of Public Schools** by Adam Schaeffer (March 10, 2010)

Published by the Cato Institute, Policy Analysis is a regular series evaluating government policies and offering proposals for reform. Nothing in Policy Analysis should be construed as necessarily reflecting the views of the Cato Institute or as an attempt to aid or hinder the passage of any bill before Congress. Contact the Cato Institute for reprint permission. Additional copies of Policy Analysis are $6.00 each ($3.00 each for five or more). To order, or for a complete listing of available studies, write the Cato Institute, 1000 Massachusetts Ave., N.W., Washington, D.C. 20001 or call toll free 1-800-767-1241 (8:30-4:30 eastern time). Fax (202) 842-3490 • www.cato.org

CATO INSTITUTE

Association of State Criminal Investigative Agencies

SHARING IDEAS FOR BETTER LAW ENFORCEMENT

May 12, 2011

The Honorable Lamar Smith
Chairman
Committee on the Judiciary
U.S. House of Representatives
Washington, DC 20515

The Honorable John Conyers
Ranking Member
Committee on the Judiciary
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Smith and Ranking Member Conyers,

The Association of State Criminal Investigative Agencies (ASCIA) supports the reauthorization of the key provisions of the PATRIOT ACT, specifically the "Lone Wolf", "Third-Party Business Records" and "Roving Wire Tap" provisions.

ASCIA members are very cognizant of their responsibility to protect the civil liberties of our citizens and believe our record as agencies has demonstrated this. We would not support any legislation that we believe would infringe upon our citizens' civil rights or civil liberties.

As the association that represents the chief executives of the state criminal investigative agencies we must be sure that our investigators comply not only with the letter of the law but also with the intent of the law in all of our investigations. We also must support the use of every reasonable lawful investigative technique in our efforts to uncover any plot to do harm to this nation by terrorists.

Our belief is that these three provisions are responsible and needed tools to help law enforcement agencies in their investigation of counter-terrorism cases. We do not believe these provisions represent undue intrusions into the privacy of American citizens nor in the past has their use created a pattern of abuse by investigators.

Therefore, we urge Congress to reauthorize these three important provisions.

Sincerely,

John Quinn
President of ASCIA
Director
Division of Criminal Investigation
State of Iowa

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, OIG
& NOAA Fisheries Law Enforcement
DEFENSE
Air Force - OIG
Army - CID
Defense Criminal Investigative Service
Naval Criminal Investigative Service
OIG
EDUCATION - OIG
ENERGY -OIG
ENVIRONMENTAL PROTECTION AGENCY - CID & OIG
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
Federal Air Marshal
Federal Emergency Management Agency
Federal Protective Service
U.S. 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
U.S Marshals Service
OIG
U.S. Attorney's Office-CI
LABOR- OIG & Racketeering
NATIONAL AERONAUTICS & SPACE ADMIN. - OIG
NUCLEAR REGULATORY COMMISSION - OIG
POSTAL SERVICE-OIG & Inspection
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. COURTS (JUDICIAL)
Probation, Parole & Pretrial Services
VETERANS AFFAIRS -OIG

NATIONAL OFFICERS
President
JON ADLER
Executive Vice-President
NADHAN CATURA
Vice President - Operations
LAZARO COSME
Vice President – Agency Affairs
CHRIS SCHOPPMEYER
Vice President – Membership Benefits
JOHN RAMSEY
Vice President - Legislative Affairs
DUNCAN THRIPLETON
Secretary
MARIA COSCIA
Treasurer
JAMES O'TOOLE JR
National Chapters Director
RASHEED TAHIR
National Awards Director
SHANON MASI-SCHERRSON
Public Affairs
Jennifer Mattingly
Legislative Counsel
Sill & Associates, 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

SERGEANTS BENEVOLENT ASSOCIATION
POLICE DEPARTMENT, CITY OF NEW YORK
35 WORTH STREET, NEW YORK, NY 10013
212.226.2180 FAX 212.431.4280
www.sbanyc.org

OFFICE OF THE PRESIDENT
EDWARD D. MULLINS

May 5, 2011

Lamar Smith
Chairman
United States House of Representatives
Committee on the Judiciary
2138 Rayburn House Office Building
Washington, DC 20515-6216

John Conyers, Jr.
Ranking Member
United States House of Representatives
Committee on the Judiciary
2138 Rayburn House Office Building
Washington, DC 20515-6216

Dear Mr. Chairman and Ranking Member Conyers:

The Sergeants Benevolent Association of New York City is a labor organization that represents the 11,000 active and retired Sergeants of the NYPD. This letter is to advise you of our union's views regarding the reauthorization of the expiring provisions of the USA PATRIOT Act. We respectfully request your support in ensuring that the three provisions due to expire on May 28th concerning law enforcement access to business records, "roving wiretaps", and "lone wolf" surveillance are reauthorized, and that the reauthorization is permanent and without legislative modification. The SBA stands with the FBI Agents Association, the Society of Former Special Agents of the FBI, and the Federal Law Enforcement Officers Association in the belief that the expiring Patriot Act provisions are simply too important to our security to allow them to sunset or to be constrained with new limitations on their use until our elected representatives can declare that America has won the war against terrorism.

The USA PATRIOT Act was enacted in direct response to the terrorist attacks of September 11, 2001. These murderous attacks devastated New York City and the ranks of its Police and Fire Departments. More than 70 law enforcement officers lost their lives when the World Trade Center Towers collapsed. Moreover, members of our union and other law enforcement officers, firefighters, and an array of other citizens who helped respond to the attacks are continuing to die and suffer debilitating illnesses as a result of inhaling the toxins released by the collapse of the Twin Towers. The SBA takes time to remember the price of 9-11 each year when we hold our annual Heroism Awards to honor the memory of the NYPD Sergeants killed by the terrorists. As we do so, we recommit ourselves to doing all we can to ensure such an attack never happens again.

The powers the Patriot Act provided to our federal counterparts after 9-11 are an important tool for ensuring there is not another 9-11. The welcome success in eliminating Osama Bin-Laden makes reauthorization of the expiring Patriot Act authorities more, not less, important. Bin-Laden's death has enraged groups and individuals attracted to his hateful and

murderous ideology. The Pakistani Taliban has vowed revenge and bragged "[w]e already have our people in America, and we are sending more there." We agree with CIA Director Panetta's recent statements in an interview with Brian Williams of NBC Nightly News that we should not "kid ourselves that killing Osama bin Laden kills al Qaeda. . . . They're still going to try to attack our country. . . . We've damaged them, but we still have to defeat them." Given this, we are dismayed that some Members of the United States House of Representatives may be hesitant to support reauthorization of the expiring Patriot Act authorities.

We find that the concerns expressed about reauthorization reflect confusion about the nature of the expiring authorities and their importance in safeguarding America from future attacks. Section 215 of the Patriot Act has allowed federal law enforcement to seek orders requiring the production of business records that relate to foreign intelligence operations or international terrorism. Under Section 206 of the Act, law enforcement can obtain wiretap orders only upon a showing of probable cause for those who attempt to evade surveillance by using multiple communications devices. Finally, the "lone wolf" provision of the Intelligence Reform and Terrorism Prevention Act of 2004 allows the FISA Court to issue surveillance orders for those non-U.S. persons engaged in international terrorism or activities in preparation of terrorism. Over the last decade, our federal law enforcement counterparts have developed a record of using these specific information gathering powers responsibly for their intended purpose of safeguarding America from another 9-11.

We also find misguided arguments that we must protect civil liberties by fixing in statute various internal procedures law enforcement agencies may follow to ensure the responsible use of the expiring Patriot Act authorities. Fixing an agency's current internal procedures into actual legislative constraints is a bad idea because it ties the hands of our federal counterparts. This is especially dangerous to do right now because law enforcement needs more flexibility than ever in the wake of our recent success. As Al-Qaeda and its sympathizers seek to avenge Bin-Laden's death and reassert their continued relevance and efficacy, we are likely to see significant changes in how they operate. These changes may necessitate subtle alterations in how law enforcement utilizes the expiring Patriot Act authorities. Fixing current procedures in legislative mandates could preclude such adjustments.

The terrorist organizations that declared war on America even before 9-11 are wounded and desperate, but still dangerous. They are an enemy that on 9-11 killed more Americans than the surprise attack on Pearl Harbor that launched World War II. And they would love now, more than ever, to carry out another such atrocity on American soil. Therefore, we ask that before House Members decline to reauthorize or decide to curtail authorities created to stop such attacks that they consider that law enforcement needs these powers now more than ever to prevent another 9-11 or something even worse. Our union appreciates your historical support of law enforcement. We appreciate your attention to our serious concerns on this matter. Please do not allow America's recent success and the security from additional attacks that our armed forces, our intelligence community, and federal, state, and local law enforcement have provided over the almost ten years since 9-11 to lull you into believing that it is now safe to put away or curtail the use of tools created after 9-11 to prevent another terrorist act on American soil.

Sincerely,

Ed Mullins

Ed Mullins
President
Sergeants Benevolent Association
of New York City

CC: Members, Committee on the Judiciary, U.S. House of Representatives
Hon. John Boehner, Speaker, U.S. House of Representatives
Hon. Nancy Pelosi, Minority Leader, U.S. House of Representatives

SOCIETY OF FORMER SPECIAL AGENTS
OF THE FEDERAL BUREAU OF INVESTIGATION, INC.

3717 FETTLER PARK DRIVE • DUMFRIES, VIRGINIA 22025-2048
(800) 527-7372 • (703) 445-0026 • FAX (703) 445-0039

May 5, 2011

The Honorable Lamar S. Smith
Chairman
U.S. House of Representatives
Committee on the Judiciary
2138 Rayburn House Office Building
Washington, D.C. 20515

Dear Congressman Smith:

On behalf of the 8000 members of the Society of Former Special Agents of the Federal Bureau of Investigation, Inc. (Society), I am writing to inform you of our views on the importance of permanently reauthorizing the three provisions of the USA Patriot Act that are going to expire on May 28, 2011.

The Society was established in 1937 as a fraternal, educational, and community-minded organization to preserve the FBI heritage in a spirit of friendship, loyalty, and goodwill. As former and current Special Agents of the FBI, our members are experienced in conducting sensitive criminal and terrorism investigations and are concerned that any changes to the Patriot Act that would make it more difficult for the FBI to fulfill its vital mission of protecting our great country.

In addition, the Society is concerned with the introduction of new issues that could impede progress in reauthorizing these important national security provisions. In view of the bipartisan consensus for the reauthorization of these provisions, we hope that their expiration can be avoided.

Since the September 11, 2001 terrorist attacks, Federal law enforcement agencies have effectively utilized three sections of the Patriot Act, namely: the business records provision, the roving wiretap provision and the lone wolf surveillance provision. These sections of the Patriot Act were adopted in direct response to the September 11th attacks and to place new restrictions and requirements on these sections of the Act would be detrimental to Federal law enforcement efforts to detect and prevent future terrorist attacks.

The business records provision, Section 215 of the Patriot Act, allows investigators to apply to the U.S. Foreign Intelligence Surveillance Court (FISA Court) for an order requiring the production of business records related to foreign intelligence operations or investigations of international terrorism. This provision is utilized in specific and rare circumstances. However, despite the infrequent use of the provision, the ability to access important records early in an investigation is critical. The Society strongly encourages Congress to reauthorize this provision on a permanent basis without limitations

The roving wiretap provision, Section 206 of the Patriot Act, allows the FISA Court to issue wiretap authorizations that are not linked to specific telephones or computers if the subject of the surveillance demonstrates an intent to evade the surveillance. It is absolutely essential to provide this ability to investigators due to the advanced technology employed by criminal and terrorism networks and conspirators. The failure to reauthorize this provision of the Patriot Act or encumber the provision with restrictions would jeopardize the importance of this valuable investigative tool.

The lone wolf provision, Section 6001 of the Intelligence Reform and Terrorism Prevention Act of 2004, provides the FISA Court with the authority to approve surveillance of non-U.S. persons acting alone or not linked to a foreign entity who are engaged in international terrorism or activities in preparation of terrorist acts. The lone wolf provision provides law enforcement with an important tool to obtain necessary information to prevent dangerous terrorist acts from occurring. The Society strongly encourages Congress not to allow this provision to expire or place restrictions on the provision that would weaken this vital investigative tool.

The Society respects and appreciates your leadership on these important issues. As former and current Special Agents of the FBI, our members are very concerned with any changes to the Patriot Act that would make it more difficult for the FBI and other Federal law enforcement agencies to investigate terrorists and their threats to our nation. We urge Congress to reauthorize the expiring provisions of the Patriot Act permanently and without restrictions as the three expiring provisions are essential to the security of our country.

Sincerely,

Lester A. Davis
President

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

Konrad Motyka, President

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

NATIONAL
FRATERNAL ORDER OF POLICE®

328 MASSACHUSETTS AVE., N.E.
WASHINGTON, DC 20002
PHONE 202-547-8189 • FAX 202-547-8190

CHUCK CANTERBURY
NATIONAL PRESIDENT

JAMES O. PASCO, JR.
EXECUTIVE DIRECTOR

The Honorable F. James Sensenbrenner
Chairman
Subcommittee on Crime, Terrorism and Homeland Security
Committee on the Judiciary
U.S. House of Representatives
Washington, D.C. 20515

11 May 2011

Dear Mr. Chairman,

I am writing on behalf of the members of the Fraternal Order of Police to advise you of our support for H.R. 1800, the "FISA Sunsets Reauthorization Act," which will be marked up this week.

This legislation would reauthorize, until 31 December 2017, two key provisions of the USA PATRIOT Act--authorizations for roving wiretaps and orders for tangible things (commonly referred to as "Section 215")--which are set to expire in May of this year. The bill would also make permanent a third provision which allows law enforcement to seek warrants against "lone wolf" terrorists.

These provisions enable law enforcement officers to use the same investigative tools used in criminal cases against suspected terrorists seeking to attack our nation and its people. Without it, the intelligence and law enforcement communities will be unable to share information about the ongoing threats our nation faces and the ability of law enforcement to prevent future attacks will be considerably lessened. Ensuring these vital tools remain available to law enforcement is a priority for the FOP, and we are prepared to work with the Administration and Congress to make other improvements to the statute that may be needed. Terrorists and terrorist organizations are not a static threat–they adapt and evolve, and the tactics and statutes we adopt to counter them must be equally flexible.

We recognize that, in popular and media culture, the USA PATRIOT Act is portrayed as controversial. This is an unjust and inaccurate portrayal. The law is one which has been carefully considered and judiciously used and there is no record that any of the authorities granted by the Act have been abused. It is a tool to catch terrorists and prevent terrorism, nothing more. While the United States won a significant victory by eliminating Osama bin Laden, we did not eliminate the danger posed by al Qaeda and others seeking to do harm to the United States and her citizens.

It is our hope that the Subcommittee will act quickly on the legislation before we get any closer to the expiration of these important provisions. As always, on behalf of the more than 335,000 members of the Fraternal Order of Police, thank you for your leadership on this and so many other issues important to law enforcement. If I can provide any further information about the importance of this issue, please do not hesitate to contact me or Executive Director Jim Pasco in my Washington office.

Sincerely,

Chuck Canterbury
National President

—BUILDING ON A PROUD TRADITION—

Major County Sheriffs' Association

1450 Duke Street, Suite 207, Alexandria, Virginia 22314

President
Sheriff Douglas C. Gillespie
Las Vegas Metropolitan Police Department
400 Stewart Ave.
Las Vegas, NV 89101-2984
(702) 229-4201
(702) 382-2964 (fax)
dgillespie@lvmpd.com

Vice President
Sheriff Richard Stanek
Hennepin County Sheriff's Office
350 S. 5th St. Room 6 Courthouse
Minneapolis, MN 55415-1316
612-348-2347
612-348-2205 (fax)
rstanek@hennepin.com

Vice President – Government Affairs
Sheriff Michael J. Bouchard
Oakland County Sheriff's Office
1200 North Telegraph – Building 38 East
Pontiac, MI 48341
248-858-5001
248-858-1800 (fax)
mbouchard@oakgov.com

Treasurer
Sheriff John Aubrey
Jefferson County Sheriff's Office
514 Court Place Ste 604
Louisville, Kentucky 40202
(502)574-5400
(502)574-5185 (fax)
aubrey@jcsoheriff.com

Secretary
Sheriff Al Lamberti
Broward County Sheriff's Office
2601 West Broward Boulevard
Fort Lauderdale, FL 33312
954-831-8901
954-797-6050 (fax)
alamberti@sheriff.org

Executive Director
Joseph R. Wolfinger
402 Parkway Drive
Tappahannock, VA 22560
(804) 445-9303
(804) 445-9323 (fax)
jwolfinger@sheriffs.org

Associate Executive Director
Michael Ferrucci Jr.
Leadership Associates
701 A Carolina Street
Fredericksburg, VA 22401-5901
540-899-2978
540-899-2998 (fax)
mferrucci@sheriffs.org

May 11, 2011

The Honorable Lamar Smith
Chairman
Committee on the Judiciary
U.S. House of Representatives
Washington, DC 20515

The Honorable John Conyers
Ranking Member
Committee on the Judiciary
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Smith and Ranking Member Conyers,

The Major County Sheriffs' Association (MCSA) supports the extension of key provisions of the PATRIOT Act to ensure that federal law enforcement agencies have the tools they need to investigate possible terror plots and to protect American citizens. Specifically, the MCSA believes that "lone wolf," "third-party business records," and "roving wire tap" provisions should be extended.

Protecting the civil rights, civil liberties, and privacy of our citizens is at the top of our minds daily in law enforcement. MCSA members hold themselves to high standards and constantly balance their core responsibility to preserve public safety with the imperative to protect citizens' liberties. We take very seriously our mission to ensure that those who would do harm to our communities are denied that opportunity at every turn. That is why we have significantly improved the way we collaborate with our law enforcement and intelligence partners at every level of government since September 11, 2001.

MCSA members collectively represent over 100 million Americans. The tens of thousands of brave men and women who work in our agencies have a tough job: they must be prepared to respond to any crime or act of terror, even as they do everything within their power to prevent those events and investigate possible threats. It is our people at the local level that have to pick up the pieces when the worst happens. As their leaders, we owe it to them – and to our communities – to ensure that every tool of government is used effectively to prevent attacks from happening.
Critical among those tools are the three expiring provisions of the PATRIOT Act mentioned above. A few facts are clear:

- these three provisions do not represent undue intrusions into the privacy of American citizens;
- these authorities have not resulted in any pattern of abuse by agents entrusted with them;
- these authorities ensure that investigative tools which are so effective in the enforcement of laws against organized crime, gangs, and drug traffickers are available for use against aspiring terrorists;
- if these provisions are not reauthorized, America will be less secure.

It is a tough reality that law enforcement agencies at every level are facing significant operational challenges due to the tight budget environment. And yet our enemies are not shrinking in number, the threats are not diminishing, and the sophistication of terrorists' planning and communications methods is not lessening. We are already doing more with less. Taking away investigative authorities will only make matters worse.

We must not let the fact that we have gone nearly 10 years without a major terrorist attack on U.S. soil lull us into complacency. We must redouble our efforts to detect and prevent acts of terrorism.
The MCSA urges Congress to reauthorize these three important provisions.

Sincerely,

Sheriff Doug Gillespie
President, MCSA

National District Attorneys Association
44 Canal Center Plaza, Suite 110, Alexandria, Virginia 22314
703.549.9222/703.836.3195Fax
www.ndaa.org

May 11, 2011

Chairman Lamar Smith
House Committee on the Judiciary
2138 Rayburn House Office Building
Washington, DC 20515

Ranking Member John Conyers
House Committee on the Judiciary
B351 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Smith and Ranking Member Conyers:

On behalf of the National District Attorneys Association, the oldest and largest organization representing the interests of over 39,000 state and local prosecutors, we offer our full support towards the reauthorization of several expiring provisions of the USA PATRIOT Act. Specifically, NDAA fully supports making the "lone wolf" definition in the existing statute permanent, extending the roving wiretap provision for an additional six years and extending the provision allowing law enforcement access to business records for an additional six years.

Since the USA PATRIOT Act was passed by Congress and signed into law shortly after the September 11, 2001 attacks on America, the three provisions listed above have been used effectively and judiciously by federal, state and local law enforcement to prevent another 9/11-like attack from happening on American soil for nearly a decade. If any of these provisions were allowed to expire, both domestic and international terrorists and terrorist organizations would be able to use substantial loopholes in the United States Code to put America's communities at risk. It is also important to note that all branches of our government – Legislative, Executive and Judicial – have performed routine oversight over each provision since their implementation in 2001 and none of the provisions have been deemed unconstitutional or have been found to be abused by the government at any time.

With the recent apprehension and death of Osama Bin Laden at the hands of American forces, many may feel that these provisions are no longer applicable which, in our view, couldn't be further from the truth. Osama Bin Laden was but one of thousands of terrorists in the world who want to bring America harm by any means necessary. With the radical advances with internet and cell phone technology since 9/11, terrorists are more independent and mobile than they have ever been before. By extending each of these provisions you will help maintain America's ability to protect our homeland by providing law enforcement the necessary tools to perform their jobs safely and successfully.

The National District Attorneys Association urges you and your colleagues on the House Judiciary Committee to extend each of the three provisions mentioned above when you meet to mark-up the USA PATRIOT Act Reauthorization. Thank you for all that you do for America's state and local prosecutors.

Respectfully,

James Reams
President

To Be the Voice of America's Prosecutors and to Support Their Efforts to Protect the Rights and Safety of the People

National Association of Assistant United States Attorneys
12427 Hedges Run Dr. • Ste 104 • Lake Ridge, VA 22192-1715
Tel: (800) 455-5661 • Fax: (800) 528-3492
Web: www.naausa.org

May 11, 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:

I write on behalf of the National Association of Assistant United States Attorneys (NAAUSA) to express our support for the reauthorization of the provisions of the PATRIOT Act and related laws that will expire on May 27, 2011. We support H.R. 1800 and urge its prompt approval by the Congress. The legislation would extend expiring provisions of the USA PATRIOT Improvement and Reauthorization Act of 2005 relating to access to business records and roving wiretaps and to permanently extend expiring provisions of the Intelligence Reform and Terrorism Prevention Act of 2004 relating to individual terrorists as agents of foreign powers.

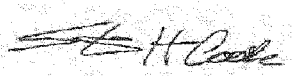
NAAUSA represents the interests of the 5,600 career Assistant United States Attorneys employed by the Department of Justice. We believe that the PATRIOT Act has demonstrated its value as an essential law enforcement tool in defending America and preserving public safety. As we noted in a 2005 letter to the House Judiciary Committee in support of the PATRIOT ACT's reauthorization at that time, "It certainly is not coincidental that the United States has not been attacked by terrorist forces since September 11." More than five years later that observation still rings true.

Recent developments involving the death of Osama Bin Laden make it doubly critical that Congress take the actions necessary to assure that law enforcement authorities have the necessary tools to root out terrorism at home and abroad. Law enforcement and intelligence agencies need the investigative and security-related authority to find and bring to justice those that plot terror aimed at Americans. That authority is embodied in the three provisions -- the business records, roving wiretap, and lone wolf surveillance provisions -- extended by H.R. 1800. These provisions have aided in the discovery and thwarting of numerous terror plots and the saving of untold American lives.

President: Steven H. Cook, ED of Tennessee
Vice President for Policy: Robert E. Mydans, District of Colorado
Vice President for Operations and Membership: John E. Nordin II, CD of California
Treasurer: Robert Gay Guthrie, ED of Oklahoma
Secretary: Rita R. Valdrini, ND of West Virginia

It is vital that the PATRIOT Act be renewed and that none of its provisions be allowed to sunset. Thank you for your consideration of our comments.

Sincerely,



Steven H. Cook
President