AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

# PERMANENT PROVISIONS OF THE PATRIOT ACT

## HEARING

BEFORE THE

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

MARCH 30, 2011

**Serial No. 112–15**

Printed for the use of the Committee on the Judiciary

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

U.S. GOVERNMENT PRINTING OFFICE

65–486 PDF WASHINGTON : 2011

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

## COMMITTEE ON THE JUDICIARY

LAMAR SMITH, Texas, *Chairman*

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

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

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

---

## SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

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

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

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

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

# CONTENTS

MARCH 30, 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 ..... 4

WITNESSES

Todd M. Hinnen, Acting Assistant Attorney General for National Security, Department of Justice
Oral Testimony ..... 6
Prepared Statement ..... 9
Kenneth L. Wainstein, Partner, O'Melveny & Myers LLP
Oral Testimony ..... 22
Prepared Statement ..... 25
Michael German, Senior Policy Counsel, American Civil Liberties Union
Oral Testimony ..... 31
Prepared Statement ..... 33

# PERMANENT PROVISIONS OF THE PATRIOT ACT

**WEDNESDAY, MARCH 30, 2011**

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

The Subcommittee met, pursuant to call, at 10:01 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, Poe, Griffin, Gowdy, Quayle, Scott, Conyers, Johnson, Deutch, Jackson Lee, and Quigley.

Staff present: (Majority) Caroline Lynch, Subcommittee Chief Counsel; Sam Ramer, Counsel; Saran Allen, Counsel; Arthur Radford Baker, Counsel; Anthony Angeli, Counsel; Lindsay Hamilton, Clerk; (Minority) Bobby Vassar, Subcommittee Chief Counsel; Joe Graupensberger, Counsel; Ron LeGrand, Counsel; Liliana Coranado, Counsel; Sam Sokol, Counsel; and Veronica Eligan, Professional Staff Member.

Mr. SENSENBRENNER. The Subcommittee on Crime will be in order.

Today's hearing is on the permanent provisions of the PATRIOT Act which are the 14 provisions that were made permanent in the 2006 authorization.

And I would like to especially thank our witness for coming and thank you for joining us today.

I am joined today by my colleague from Virginia, the Ranking Member of the Subcommittee, Bobby Scott, and the junior Chairman emeritus, John Conyers of Michigan.

I recognize myself for 5 minutes.

Today's hearing will examine the permanent provisions of the PATRIOT Act. As Chairman of the Judiciary Committee in 2005, I spearheaded the reauthorization of the Act which made permanent 14 of the 16 temporary provisions. These 14 provisions provide a variety of law enforcement and intelligence gathering tools to identify and prevent terrorist threats of the 21st century.

Perhaps the most significant of those provisions is designed to remove the information sharing wall that existed prior to the 9/11 terrorist attacks. The 9/11 Commission report provided a detailed description of the evolution of the wall which prevented information sharing between law enforcement and intelligence agencies. As

the report notes, the wall was not erected by a single act of Congress, court ruling, or administrative order. Rather, it was built slowly over time based upon the interpretation and often misinterpretation of Federal law and Justice Department procedural memos.

Sections 203 and 208 of the Act helped tear down the wall by implementing important changes to FISA and the Federal Criminal Procedures. As the Department noted in 2005, the new ability to share critical information has significantly altered the entire manner in which terrorism investigations are conducted, allowing for a much more coordinated and effective approach than was possible prior to the passage of the USA PATRIOT Act.

The need for information sharing is perhaps even more critical today as America continues to encounter isolated plots carried out by individual terrorists. The preemption of these plots is often dependent upon the timely ability of our intelligence and law enforcement agencies to work together to connect those dots.

The 2005 reauthorization also made permanent laws that designate terrorism-related offenses wiretap predicates, authorize emergency disclosure of electronic surveillance, modernize search warrant authorities, and authorize law enforcement assistance to victims of cyber attacks.

Many will agree that these provisions are common sense and largely noncontroversial, including civil liberties organizations such as the Center for Democracy and Technology. Their permanence has neither diminished Congress' ability to oversee their use nor increased the potential for misuse by the Government.

The other investigative tools, including National Security Letters and delayed notice search warrants, are often thought to be products of the 2001 PATRIOT Act. That is not true. National security letters were first authorized by Congress 15 years before the PATRIOT Act in legislation sponsored by Senator Leahy and former Wisconsin Congressman Robert Kastenmeier. NSL's are similar to administrative or grand jury subpoenas but can only be used to acquire specific categories of third party records such as telephone toll records, credit reports, and bank records. The 2001 PATRIOT Act confirmed the NSL standard to bring it in line with the over 300 other Federal administrative subpoena authorities. The 2005 reauthorization added several additional NSL procedures, including the express authorization for NSL recipients to consult their attorneys and judicial review of NSL's and nondisclosure orders.

Current legislation in the Senate would revert the NSL's back to the original Leahy-Kastenmeier pre-9/11 standard. 2 weeks ago, the FBI Director Mueller testified before the Committee that he opposes this change, explaining that National Security Letters are the building blocks which enable the FBI to collect information. Changing the standard or sunsetting NSL's would undercut the FBI's authority to undertake the kinds of investigations that led to the disruptions in the last 9 years.

Delayed notice search authority also predates the PATRIOT Act. In 1979, the Supreme Court found that the Fourth Amendment does not require law enforcement to give immediate notice of the execution of a search warrant. Three Federal courts of appeals have considered and upheld the constitutionality of delayed notice

search warrants since 1979. Section 213 of the PATRIOT Act codified the courts' ability to delay notice to a target of a search under a certain set of circumstances. The notice may not be delayed indefinitely. Initial delay may extend for up to 30 days and the delay may only be extended by the court for an additional 90 days based upon a showing of good cause.

The Senate proposal would reduce the 30-day time frame to 7 days and Director Mueller testified against this change, notifying that the 30-day time frame works well and he sees no advantage to drawing it back to 7 days.

Congress must be careful not to undermine the tools we have in place that have helped the FBI and other agencies prevent another 9/11 attack and preempt the increasing number of smaller individualized terrorist plots.

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

Mr. SCOTT. Thank you, Mr. Chairman, and thank you for holding this hearing following on the Subcommittee's recent hearing about the three expiring provisions of the U.S. PATRIOT Act. So I am glad that now we are examining the rest of the law and we will have additional hearings.

In the wake of the attacks on September 11th, we rushed to enlarge the power of Government with respect to privacy and other fundamental rights. Whatever we say about the PATRIOT Act, I do not think that we are any more free today because of it. In my mind a major cause of concern is that these extensions of Government powers created greater incentives for Government to use them even in contexts most of us would agree were not appropriate.

A good example of this is the documented abuse of the National Security Letters. The PATRIOT Act significantly loosened the standards for the FBI to issue those demands for certain types of personal information, and two Inspector General reports found significant abuses of NSL's. While the Justice Department and FBI have taken steps to address the abuses, the abuses themselves underscore the danger in hastily expanding such powers that do not involve oversight by an individual magistrate or judge.

Also, the PATRIOT Act allows greater use in criminal cases of information gathered in intelligence investigations. We generally allow intelligence information to be obtained under different rules and standards than those applied to criminal law. Once again, we need to be concerned about the incentives we give to Government when we loosen these restrictions. The use of intelligence gathering tools to avoid otherwise applicable constitutional constraints on law enforcement poses a grave threat to the fundamental protections our Founders established. We saw this from the abuses in COINTELPRO and other abuses exposed by the Church Commission hearings led by then Senator Frank Church. While we should provide for appropriate sharing of information between the CIA and the FBI in instances such as preventing terrorism, I believe that the PATRIOT Act went too far in authorizing information gathering and sharing of intelligence by law enforcement.

Finally, I mentioned the PATRIOT Act's relaxation of standards by which FISA orders may be obtained. Previously the requirement was that the primary purpose of such order was to gather foreign intelligence. That was exchanged to now the Government must only show a significant purpose, not the primary purpose of the order is to gain intelligence information. This, of course, gives law enforcement not only the authority but incentive to seek FISA orders in what are largely criminal investigations rather than having to meet the higher standards required for criminal warrants.

To make matters worse, targets of an inappropriate FISA order may never find out that their privacy was breached and may never have an opportunity to challenge it. It is difficult to uncover abuses in such cases, and it makes it hard for us to conduct appropriate oversight.

Ultimately I don't believe we need to choose between being safe and being free. We can reasonably achieve both and we should constantly strive to assure both. But there is good reason to provide the probable cause and other things for criminal warrants. They may not be appropriate for intel, but the information sharing gives the incentive to get the warrants through the intelligence approach with the lesser standard.

Ben Franklin famously said to those who would give up essential liberty to purchase a little temporary safety, deserve neither liberty nor safety. And that is why I am pleased that we are having this hearing today to further examine the USA PATRIOT Act and look forward to the testimony of our witnesses.

And I yield back.

Mr. SENSENBRENNER. I thank the gentleman from Virginia.

Now, would the junior Chairman emeritus want an opening statement?

Mr. CONYERS. Well, after considerable deliberation, my answer is yes, Mr. Senior Chairman Emeritus.

Mr. SENSENBRENNER. This is just like the Senate with senior and junior Senators. The gentleman is recognized for 5 minutes.

Mr. CONYERS. I want to begin by commending you, Chairman Sensenbrenner, in terms of the work that you have done on this Committee that starts with the Voting Rights Act of 1981, the amendments of 2006, the Americans with Disabilities legislation that you have championed throughout your career, and the original PATRIOT Act that came out of this Committee unanimously in 2001.

Because of that, we come here today to request of you that we have another meeting on this subject without the distinguished witnesses that are here where we can discuss some of the unclassified and classified materials that would be the subject of such a meeting. I am fully aware that the month after next we are going to have to dispose of this matter, and I think that this would be a very important meeting in terms of reaching some kind of consensus about where we are.

Now, I guess the problem that bothers me most is the fact that we have now allowed the Government to legally secretly enter anybody's home in the United States to search and to keep secret that they broke into someone's home for the purposes of any criminal investigation. And it can be kept secret for longer than 90 days by

merely getting an extension. I would like this discussed here today, of course, but I would like us to meet with the Committee in a nonpublic hearing on that issue.

In addition, we have National Security Letters which first started off outside of the PATRIOT Act and now have been included and extended inside of the PATRIOT Act. The FBI issues tens of thousands of such letters every year. It has been determined by the Inspector General that there is widespread abuse of this power, and to me this is not acceptable. We need to decide what we are going to do on this or this whole bill is going to be, I can predict, in some serious difficulty.

Frequently national security powers are brought to ordinary cases. Section 218 of this act allows the executive to use full national security powers in ordinary criminal investigations so long as it claims a significant purpose of gathering foreign intelligence.

And so I look forward to our discussion this morning. I thank you for the extension of time.

Mr. SENSENBRENNER. I thank the gentleman from Michigan.

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

Todd Hinnen is the Acting Assistant Attorney General for National Security at the Department of Justice. Prior to assuming this position, Mr. Hinnen was the Deputy Assistant Attorney General for Law and Policy at the National Security Division of DOJ. He also previously served as chief counsel to then Senator Joseph R. Biden, Jr., as a director in the National Security Council's Combating Terrorism Directorate and as a trial attorney in the Department of Justice's Computer Crime and Intellectual Property Section. He clerked for Judge Richard Tallman of the Ninth Circuit Court of Appeals and is a graduate of Amherst College and Harvard Law School.

Ken Wainstein is a partner at O'Melveny & Myers in Washington, D.C. and a member of the white collar defense and corporate investigations practice. Prior to his work at O'Melveny, Mr. Wainstein spent 19 years with the Department of Justice. From 1989 to 2001, he served as an assistant U.S. Attorney both in New York and Washington. In 2001, he was appointed Director of the Executive Office of U.S. Attorneys where he provided oversight and support to the 94 U.S. attorneys offices. The next year he joined the FBI to serve first as general counsel and then as chief of staff to Director Robert S. Mueller. In 2004, Mr. Wainstein was appointed and later confirmed as the U.S. Attorney for Washington, D.C. He was confirmed again by the Senate in 2006 after being nominated as the first Assistant Attorney General for National Security in the Justice Department. He established and led the new division which consolidated DOJ's law enforcement and intelligence activities on counterterrorism and counterintelligence matters. In 2008, he was named Homeland Security Advisor to then President Bush. In that position he advised the President and oversaw the interagency coordination process for our homeland security and counterterrorism programs. He received his bachelor of arts in government and international relations from the University of Virginia and his juris doctor from the University of California-Berkeley in 1988.

Mike German is the Policy Counsel for National Security and Privacy for the American Civil Liberties Union, Washington Legislative Office. Prior to his work at the ACLU, he served as a special agent for the FBI for 16 years. Mr. German's final assignment with the FBI was as a counterterrorism instructor at the FBI National Academy. There he taught courses on extremism in democratic societies and developed a graduate level training program for State, local, and international law enforcement officers. He left the FBI in 2004 and joined the ACLU in 2006. He received his bachelor of arts in philosophy from Wake Forest University and his juris doctor from Northwestern University Law School.

Without objection, all Members' opening statements will appear in the record in their entirety.

Without objection, the witnesses' statements will appear in the record in their entirety.

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

And without objection, the Chair will be authorized to declare recesses during roll call votes in the House if they happen.

The Chair now recognizes Mr. Hinnen for 5 minutes.

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

Mr. HINNEN. Mr. Chairman, Ranking Member Scott, Ranking Member Conyers, and Members of the Subcommittee, thank you for inviting me to testify again on behalf of the Department of Justice as you consider reauthorization of the USA PATRIOT Act. 3 weeks ago, I addressed the three FISA provisions that are due to expire in May. Today you have asked me to discuss other PATRIOT Act provisions.

As you know, the PATRIOT Act contained provisions amending a wide variety of laws, including those affecting immigration, border protection, victim's rights, criminal investigations and prosecutions, and foreign intelligence. I understand that the Subcommittee would like us to focus today on the criminal and intelligence investigative authorities affected by the PATRIOT Act.

The PATRIOT Act amendments to these authorities achieved several objectives. First, the Act provided national security officers with tools similar to those commonly used in routine criminal investigations. It permitted the Government to apply for roving FISA surveillance orders and business records orders, each of which has a well established criminal analog as we discussed 3 weeks ago.

It also amended existing National Security Letter authorities so that they operated more like grand jury subpoenas. In particular, it allowed NSL's to be issued out of field offices, not just FBI headquarters, and it permitted the FBI to issue an NSL if the records sought were relevant to an authorized national security investigation, a standard similar to but still more demanding than that for grand jury subpoenas.

Second, the Act modernized a number of criminal investigative authorities. For instance, it permitted the Government to use the criminal pen trap statute to intercept email data in addition to phone numbers.

Third, the Act streamlined the use of investigative authorities, reducing administrative burdens so that the Government could focus its finite resources on identifying and disrupting terrorist plots and bringing the perpetrators to justice. For instance, it extended the duration of FISA surveillance orders against non-Americans so that agents, attorneys, and judges do not have to undertake the labor-intensive process of renewing them as often. It also allowed the Government in criminal investigations to obtain pen register and stored communications orders from any court that had jurisdiction over the crime rather than forcing investigators in one State to go before a court in another State just because that is where the Internet service provider happened to be.

Fourth, the Act permitted intelligence and law enforcement officers to share information and work together to protect Americans from national security threats. It removed the so-called "FISA wall," clarifying that intelligence collected through FISA surveillance could be shared with criminal investigators and support criminal prosecutions. It also permitted information obtained through criminal wiretaps and grand jury investigations to be shared with intelligence officials.

Many of these changes proved uncontroversial. Those that were set to expire were renewed, some with amendments. They are now a permanent part of the authorities we use to protect the country against terrorism and other national security threats.

I understand that the Subcommittee would also like me to address the authorities governing National Security Letters. Like grand jury subpoenas in routine criminal investigations, NSL's allow the FBI during predicated national security investigations to obtain certain basic information that forms the building blocks of most investigations. For example, NSL's are used to obtain telephone calling records and email transaction records. These records can help the FBI identify co-conspirators. NSL's can also be used to obtain information regarding bank accounts being used to fund terrorist activities. NSL's were used to obtain substantial information regarding the 11 Russian deep-cover spies caught last year, including information about payments they received in financial accounts. In short, NSL's are a critical tool in the national security toolbox and their absence would significantly hamstring the FBI in its ability to protect the country.

Although NSL's are used in much the same way as grand jury subpoenas, they are subject to far greater statutory constraints and much more rigorous oversight. Additionally, NSL's are subject to congressional reporting requirements.

As the Subcommittee is no doubt aware, in 2007 DOJ's Inspector General issued a report that was critical of how the FBI had used NSL's from 2003 to 2005. As he testified before the House Judiciary Committee, the IG did not—and I quote—"find evidence of deliberate or intentional violations of the NSL statutes, Attorney General guidelines, or FBI policy." The Department and the FBI worked hard to address the issues raised in the 2007 IG report, and in 2008, the IG issued a follow-on report praising the substantial progress the FBI had made in tightening the internal controls and processes involved in the issuance of NSL's. That progress has continued.

As many of your staffers have seen, the FBI now issues NSL's using a centralized computer system that minimizes errors. The system ensures that before an NSL can be issued, the agent must articulate how the information sought is relevant to an authorized national security investigation, an FBI attorney must review the request, and a high level signatory must approve it.

Mr. Chairman, I see I am out of time. I can address some additional safeguards during the question and answer period. Thank you. I look forward to your questions.

[The prepared statement of Mr. Hinnen follows:]

# Department of Justice

**STATEMENT OF**
**TODD M. HINNEN**
**ACTING ASSISTANT ATTORNEY GENERAL FOR NATIONAL SECURITY**
**DEPARTMENT OF JUSTICE**

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

**AT A HEARING ENTITLED**
**"THE PERMANENT PROVISIONS OF THE PATRIOT ACT"**

**PRESENTED ON**
**MARCH 30, 2011**

**Statement of**
**Todd M. Hinnen**
**Acting Assistant Attorney General for National Security**
**Department of Justice**

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

**At a Hearing Entitled**
**"The Permanent Provisions of the PATRIOT Act"**

**Presented on**
**March 30, 2011**

Chairman Sensenbrenner, Ranking Member Scott, and members of the Subcommittee, thank you for inviting me to testify today. Three weeks ago, I testified before this Subcommittee on the three provisions of the Foreign Intelligence Surveillance Act ("FISA") that were recently reauthorized by Congress but are scheduled to sunset again in May: the "roving" surveillance provision, the "lone wolf" definition, and the "business records" provision. Today I will address other national security investigative authorities enacted or amended as part of the USA PATRIOT Act, focusing in particular on the legal authorities relating to national security letters ("NSLs"). These authorities are not currently scheduled to expire, but I understand the Committee would like me to discuss their use, oversight, and importance to national security. Before I do that, I'd like to provide a brief overview of the investigative tools Congress enacted in the USA PATRIOT Act and why they remain important today.

**Investigative Authorities in the USA PATRIOT Act**

Nearly ten years ago, shortly after the September 11 attacks, Congress enacted the USA PATRIOT Act, a key purpose of which was "to enhance law enforcement investigatory tools" to protect the country from terrorism. *See* United 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, 272 (2001). Title II of the original PATRIOT Act, entitled "enhanced surveillance procedures," contains a number of important amendments to FISA and other laws to make national security investigations more effective and efficient. Of these Title II provisions, 16 were scheduled to expire in 2005, but Congress made 14 of them permanent in the USA PATRIOT Improvement and Reauthorization Act of 2005 while extending the sunsets on the roving surveillance and business records provisions. *See* USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, §§ 102-03, 120 Stat. 192, 194-95 (2006).

The enhancements that were made to our investigative tools in the PATRIOT Act are now fundamental to how we conduct national security investigations. For example, provisions in the PATRIOT Act helped us tear down the so-called FISA "wall" between law enforcement and intelligence. *See* USA PATRIOT Act, sections 203, 218 and 504. The wall had two aspects:

there were limits on intelligence agents' ability to share information they collected using intelligence tools with criminal investigators; and there were limits on the ability of criminal investigators to share information they collected using criminal tools with their colleagues on the intelligence side.

On the intelligence side, the wall was built on the proposition that because FISA required *the* purpose of surveillance to be collection of foreign intelligence,, which was widely interpreted to mean "the primary purpose," the statute itself regulated the nature and scope of interactions between intelligence and law enforcement officials. The PATRIOT Act eliminated the perceived statutory bar on such information sharing, and the FISA Court of Review issued an important decision upholding the Act's clarification that so long as a "significant purpose" of the FISA surveillance is to obtain foreign intelligence, the statute permits a greater degree of interaction between intelligence and law enforcement officials than was previously thought permissible. Other provisions adopted in the PATRIOT Act addressed the other side of the wall. For example, section 203 revised the Wiretap Act and Federal Rule of Criminal Procedure 6(e) to facilitate sharing of Title III and grand jury material involving foreign intelligence or counterintelligence with any Federal law enforcement, intelligence, or national security official to assist them in performing their duties. These were commonsense measures that greatly facilitated our ability to implement broad-based information sharing in the national security arena.

The cumulative result of the elimination of the wall is better cooperation than ever before between the intelligence and law enforcement communities. The National Security Division that I currently head embodies this fundamental change, as criminal prosecutors and intelligence lawyers responsible for implementing FISA are integrated in a single organizational division. The result is not only more effective investigations in which law enforcement and intelligence officials work together to protect Americans, but also more efficient use of these sensitive authorities. National Security Division lawyers work closely with investigators virtually from the outset of an investigation, providing legal advice and oversight as it progresses. The FBI has also reorganized itself to integrate intelligence and law enforcement functions. The results of these changes are seen in cases such as the investigation and arrest in September 2009 of Najibullah Zazi, who plotted to attack the New York City subway system. Intelligence and law enforcement tools were both used and prosecutors and agents worked together to prevent a terrorist attack and then effectively prosecute the case.

Some provisions of the PATRIOT Act were designed to modernize investigative authorities to take account of evolving technologies. For example, section 216 clarified that district courts may authorize pen register and trap and trace devices to be used in criminal investigations to obtain dialing, routing, addressing, or signaling information for electronic communications (*e.g.*, e-mail) in addition to telephonic communications (while prohibiting

collection of content). 18 U.S.C. §§ 3123(a)(1), 3127(3) & (4). Use of pen/trap authority for electronic communications is now routine and a vital part of the investigative tool-kit in criminal cases. The showing that the government must make to obtain a pen/trap order under FISA was also changed in section 214 to bring it into line with the standard applicable in ordinary criminal cases, which requires only that the information sought be relevant to an ongoing criminal investigation. *See* 18 U.S.C. § 3122(b)(2). Before the PATRIOT Act, the government had to show that the facility in question was in communication with a foreign power or agent of a foreign power or an individual engaged in international terrorism or clandestine intelligence activities; now it is sufficient that the information likely to be obtained is "relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities" or is "foreign intelligence information not concerning a United States person." 50 U.S.C. § 1842(c)(2). At the same time, the law precludes an investigation of a United States person based solely upon activities protected by the First Amendment. As revised, the FISA pen register/trap and trace authority is an effective tool that allows investigators operating in the national security arena to gather basic information using the same tools that ordinary criminal investigators have used effectively and without controversy for decades.

Other provisions of the PATRIOT Act were designed to streamline our national security investigations and make them more efficient. For example, section 207, as expanded in 2005 by section 105 of the USA PATRIOT Improvement and Reauthorization Act , extended the time periods for which electronic surveillance and physical searches targeting non-United States persons are authorized under a FISA Court order before a renewal order must be obtained (this time period was later adjusted again by the FISA Amendments Act of 2008). 50 U.S.C. §§ 1805(d)(1), 1824(d)(1). This has allowed the FBI and the National Security Division to focus more of our limited resources on new investigative activity where it is most needed rather than on repeated renewals of FISA applications. Section 216 granted district courts nationwide jurisdiction to authorize pen register and trap and trace devices. 18 U.S.C. § 3123(a)(1). This allows criminal investigators to serve pen register/trap and trace orders on providers anywhere in the country, rather than requiring them to waste valuable time and resources obtaining each order from the district court in the district in which the provider happens to be located.

While I have not catalogued today all of its important reforms, I hope the examples I have provided demonstrate that the tools that are part of the USA PATRIOT Act are critical for national security investigations. The authorities obtained have allowed the Department of Justice and the FBI to more effectively and efficiently achieve their mission of protecting the country from international terrorism and national security threats. We work hard to use these authorities responsibly and in a manner that is consistent with the civil liberties that Americans hold dear, complying with the many safeguards required by statute and developing additional safeguards as a matter of policy and practice. With that brief introduction, I'll address in detail one type of investigative tool that was improved by the PATRIOT Act, although the authority existed long

before the enactment of that statute, and that remains critical to our ability to keep the country safe: national security letters.

**The NSL Statutes**

A national security letter is effectively an administrative subpoena, issued by a federal agency, requiring the production of certain limited types of information held by third-party custodians. NSLs are used during national security investigations in much the same way as grand jury subpoenas are used during routine criminal investigations. NSLs and grand jury subpoenas allow investigators to acquire the sort of very basic information that can be used as building blocks of an investigation; documents like telephone toll records, and banking and credit records. Unlike grand jury subpoenas, however, NSL authorities are limited to only certain types of records and are found in several distinct statutes, each of which has specific rules governing its use, the types of records that can be obtained, and the nature of the certification that must be provided. And, unlike most grand jury subpoenas, the NSL statutes all contain nondisclosure provisions, which, upon certification from a specified government official, restrict the recipient's right to disclose the NSL. Finally, also unlike grand jury subpoenas, the government must report to Congress specific information regarding its use of NSLs.

It is important to note that the USA PATRIOT Act did not create NSLs; it did, however, change the standard of proof required to issue NSLs. Whereas before the USA PATRIOT Act there had to be specific and articulable facts demonstrating that the information sought pertained to a foreign power or an agent of a foreign power, it is now sufficient that the material sought by an NSL be relevant to a national security investigation. In addition, the USA PATRIOT Act allowed the delegation of NSL approval authority, which, for FBI, had previously been reserved to FBI Headquarters and the three largest field offices, to all FBI field offices, provided that the NSL is approved by an official at the level of Special Agent in Charge ("SAC") or higher. Most of the NSL statutes also expressly require that, if the subject of the investigation is a United States person, it not be based solely on activities protected by the First Amendment. In addition, the Attorney General's Guidelines for Domestic FBI Operations — which also apply to the issuance of NSLs — prohibit the collection, investigation, or maintenance of information on United States persons solely for purposes of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution, and this requirement has been incorporated into FBI policy.

There are five statutes that authorize the issuance of NSLs: the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2709; the Right to Financial Privacy Act ("RFPA"), 12 U.S.C. § 3414; two provisions of the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. §§ 1681u and v; and the National Security Act ("NSA"), 50 U.S.C. § 436. Three of these authorities may be used only by the FBI, and the other two may be used by the FBI and other

agencies (although other agencies collectively issue only a very small number of NSLs). Because the overwhelming majority of NSLs are issued by the FBI, my testimony focuses on the FBI's use of NSLs.

Under ECPA, the FBI may obtain subscriber information, toll billing records, and electronic communication transactional records from a wire or electronic communications service provider, such as a telephone company or an Internet service provider. This is the NSL authority that is used most frequently by the FBI, and each ECPA NSL must include a certification by an authorized FBI employee at the SAC level or above that the records are being sought for an authorized national security investigation. Examples of "electronic communication transactional records" ("ECTRs") that may be obtained by an ECPA NSL are account numbers, physical addresses, subscriber telephone numbers, IP addresses, and other non-content information that is analogous to subscriber information or toll billing records for telephones. Significantly, the FBI *cannot* obtain the content of communications through an ECPA NSL.

The Department is preparing a proposed amendment to the ECPA NSL statute to clarify the obligation of providers to produce ECTRs and has had discussions with staff on both the House and Senate sides related to that issue. Although this term is included in subsection 2709(a) (which describes the provider's duty to produce records), it is absent from subsection 2709(b) (which requires FBI to make a certification in connection with a request for records). This omission has led a small number of providers to conclude that the FBI is not entitled to obtain ECTRs. In contrast, it has led one court to acknowledge the possibility of the opposite extreme, recognizing in dicta that providers may have an obligation to provide the FBI with ECTRs even if there were no certification of relevance. *See Doe v. Gonzales*, 500 F. Supp. 2d 379, 387 n.6 (S.D.N.Y. 2007) ("Section 2709(b) does not make clear whether any certification by the FBI is required with respect to a request for 'electronic communication transactional records.'"). While we believe the current law requires the production of ECTRs, and that the certification requirement in subsection 2709(b) applies as well, we expect to propose an amendment to eliminate this source of confusion in the statutory text.

Under RFPA, the FBI has the authority to issue NSLs for the financial records of a person or entity from various types of financial institutions, such as banks, credit unions, and credit card companies. RFPA NSLs are commonly used in connection with investigations of potential terrorist financing. Again, each RFPA NSL must include a certification by an authorized FBI employee at the SAC level or above that the records are being sought for an authorized national security investigation. RFPA also allows other agencies to issue NSLs.

Under provisions of FCRA, the FBI has the authority to issue three different, but related, types of NSLs to credit reporting agencies: an NSL pursuant to 15 U.S.C. § 1681u(a) for the names of financial institutions with which the subject has or has had an account; an NSL

pursuant to 15 U.S.C. § 1681u(b) for consumer identifying information (name, address, former addresses, employment, and former employment); and an NSL pursuant to 15 U.S.C. § 1681v for a full credit report. This last one may be used only in international terrorism cases, as opposed to any national security investigation.

Finally, any authorized investigative agency has the authority to issue NSLs pursuant to the National Security Act ("NSA") in the course of investigations of improper disclosure of classified information by government employees. 50 U.S.C. § 436(a)(1)-(2). The standards for issuance of National Security Act NSLs are significantly different than the others. The records sought must pertain to a person who is or was an Executive Branch employee and who provided consent to the government to access his financial records, consumer reports, and travel information as a condition of his access to classified information. Moreover, there must be reasonable grounds to believe that the person is or may be disclosing classified information in an unauthorized manner, has incurred excessive indebtedness or acquired unexplained affluence, or had the capability and opportunity to disclose classified information known to have been lost or compromised. National Security Act NSLs may be issued to financial institutions, consumer credit agencies, and commercial entities with travel information, but must be approved at the Assistant Secretary or Assistant Director level or above. The FBI has not used this authority to date.

As a matter of procedure under FBI policy, an FBI employee seeking an NSL must prepare a document (an electronic communication, or "EC") in which the employee lays out the factual predicate for the request. The factual recitation must be sufficiently detailed so that the approving official can determine that the material sought is relevant to an authorized national security investigation. Additionally, it needs to provide enough information concerning the underlying investigation that reviewing officials can confirm that the investigation is adequately predicated and, if concerning a United States person, is not based solely on the exercise of First Amendment rights.

I believe the current standards for issuance of an NSL are appropriate. In a traditional criminal case, a grand jury subpoena may be issued "merely on suspicion that the law is being violated, or even just because [the grand jury] wants assurance that it is not" being violated. *United States v. R. Enterprises*, 498 U.S. 292, 297 (1991). Imposing a higher evidentiary standard on NSLs, as was the case before the reforms of the USA PATRIOT Act, would significantly impair the effectiveness of this important investigative tool. This is true particularly because NSLs are often used at the outset of an investigation when additional facts concerning the subject of the investigation may not be available and when basic information is needed in order to be able to move an investigation forward.

**Challenging NSL Nondisclosure**

As noted above, all of the NSL statutes contain provisions barring the recipients from disclosing the NSL (except to an attorney or other person whose assistance is required to comply) based upon a certification that nondisclosure is necessary. The FBI (as well as other agencies issuing NSLs) must make an individualized determination for every NSL it issues whether there is a need for secrecy based on a danger to national security or interference with an investigation that might result from disclosure. Generally the need for secrecy derives from a desire not to reveal prematurely the existence of the investigation to its targets. If the need for secrecy is certified, the NSL may forbid the recipient from disclosing it unless and until the recipient obtains a judicial order for relief.

In *Doe v. Mukasey*, 549 F.3d 861 (2d Cir. 2008), the recipient of an ECPA NSL challenged the constitutionality of the nondisclosure requirement in court. The United States Court of Appeals for the Second Circuit found the statute unconstitutional under the First Amendment because it imposes a burden on the recipient to initiate litigation in order to protect his free speech interests, but observed that the government could cure this problem with a "reciprocal notice" approach: "The Government could inform each NSL recipient that it should give the Government prompt notice, perhaps within ten days, in the event that the recipient wishes to contest the nondisclosure requirement. Upon receipt of such notice, the Government could be accorded a limited time, perhaps 30 days, to initiate a judicial review proceeding to maintain the nondisclosure requirement, and the proceeding would have to be concluded within a prescribed time, perhaps 60 days." *Id.* at 879. Thus the court struck down the nondisclosure provisions "only to the extent that they fail to provide for Government-initiated judicial review," and stated that the government "can respond to this partial invalidation ruling by using the suggested reciprocal notice procedure," which if implemented would allow the nondisclosure provisions to "survive First Amendment challenge." *Id.* at 884. The FBI promptly implemented the reciprocal notice procedure as suggested by the court for all types of NSLs. The *Doe* court also struck down a separate statutory requirement that the government's certification, which triggers the nondisclosure requirement, must be treated as "conclusive" absent a finding of bad faith; the court required "some demonstration" from the government to allow for meaningful judicial review on the merits. *Id.* at 882.

Legislation now pending in the Senate to reauthorize the three expiring FISA authorities would essentially codify the reciprocal notice practice for NSL nondisclosure challenges and eliminate the conclusive presumption, thus rendering the non-disclosure provisions of the NSL statutes facially constitutional. *See* S.193, "USA PATRIOT Act Sunset Extension Act of 2011." In place of the conclusive presumption afforded the government's determination on the need for secrecy, under the Senate bill, the court would be required to give "substantial weight" to the government's determination that disclosure of the NSL would endanger national security or harm

an investigation. The bill would also require the government to notify the recipient of an order who has objected to nondisclosure if and when the need for government secrecy no longer exists. We believe these procedures are constitutionally and operationally sound and give the government and the recipient a fair chance to litigate the nondisclosure requirements.

Since shortly after the *Doe* decision, the FBI has given all NSL recipients the option of notifying the FBI if they wish to be released from their secrecy obligation. Only one recipient of an NSL has objected to nondisclosure; the issue was resolved without the necessity of litigation.

**The NSL Subsystem**

In 2007, the Department of Justice Office of the Inspector General ("OIG") issued a report that was critical of the FBI's use of NSL authorities. For example, the report found that NSLs had been issued when the investigative authority to conduct the underlying investigation had lapsed; that telephone billing and e-mail subscriber records had been obtained concerning the wrong individuals; that NSLs were issued citing the wrong statutory authorities; that full credit reports had been obtained in counterintelligence investigations, which the relevant NSL statute does not permit; and that NSLs were issued out of "control files" rather than from "investigative files" in violation of FBI policy. *See* Department of Justice Office of Inspector General Report, "A Review of the Federal Bureau of Investigation's Use of National Security Letters," at 66-67 (March 2007). However, as the Inspector General testified in 2007, "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 adequate guidance, and lack of adequate oversight." *Id.*

In the wake of this report, the FBI developed an automated system – the NSL subsystem – under which NSLs would be issued in order to control for and prevent most non-substantive errors. The NSL subsystem was created to be a part of the existing, highly successful FISA Management System; it functions as a workflow tool that automates much of the work in preparing NSLs and their associated paperwork. It is designed to require the user to enter certain data before the workflow can proceed and requires specific reviews and approvals before the request for the NSL can proceed. Through this process, the FBI can electronically ensure that applicable legal and administrative requirements are met and that required reporting data are accurately collected.

For example, by requiring the user to identify the investigative file from which the NSL is to be issued, the system ensures that NSLs are not requested out of administrative or control files. In addition, the subsystem automatically verifies the status of the case to ensure that the investigation is still open at the time the NSL is drafted. It also automatically populates the NSL with appropriate statutory language, validates the case file through the FBI's case file system to ensure that the case is open and a proper sub-file has been identified, and ensures that the underlying investigation has not lapsed. Thus, for instance, the system would prevent a user from relying on the FCRA NSL provision, 15 U.S.C. 1681v – which applies only in terrorism investigations – to issue an NSL in a counterintelligence investigation. The system requires the user to identify separately the target of the investigative file and, if it is a different person, the identity of the person about whom records are being obtained through the requested NSL. This allows the FBI to tabulate more accurately the number of different persons about whom data is gathered using NSLs – one of the data points on which the government is required to report to Congress. The system also requires that specific data elements be entered before the process can continue, such as requiring that the target's status as a United States Person ("USPER") or non-USPER be entered, or requiring that an FBI lawyer approve the legal sufficiency of the grounds for which the NSL is sought. The system does not permit requests containing logically inconsistent answers to proceed.

The NSL subsystem was designed so that the FBI employee requesting an NSL need enter data once and the subsystem automatically populates all subsequent places where those data are needed. Among other things, this eliminated one particular type of transcription error that gave rise in the past to unauthorized collections (*e.g.*, the relevant telephone number on which records were requested in the authorizing EC was 202-333-1234, but due to a typographical error in the NSL served on the telephone company, the FBI asked for records relating to 202-333-1243). In addition, requesters are required to provide a narrative statement explaining the factual basis for the determination that the information being sought is relevant to an appropriately predicated national security investigation, and the basis for a determination that the NSL should include a non-disclosure provision, if such a provision is included.

The NSL subsystem also ensures that both the NSL and the EC supporting issuance of the NSL are reviewed and approved in accordance with FBI policy, which now mandates review and approval by an FBI attorney. (Prior to the 2007 OIG report, legal review of NSLs had been recommended but not required; in addition, the exact scope of the lawyer's review obligation had not been defined). In addition, only an FBI employee who is statutorily authorized to do so can authorize issuance of the NSL in the subsystem. Once approved in the subsystem, the various documents are automatically uploaded into the FBI's Automated Case Support System ("ACS").

Finally, this subsystem has a comprehensive Congressional reporting capability. Since its deployment, FBI policy has required all NSLs to be created using the NSL subsystem, with

only a few very narrow exceptions (*e.g.*, very sensitive investigations such as espionage investigations). The system has increased the accuracy of NSL reporting, reduced drafting errors, and has ensured all required levels of approval have been obtained. By FBI policy, NSLs that are created outside of the NSL subsystem must be reported to the Office of the General Counsel ("OGC") and the information required for Congressional reporting is manually entered into the system.

Based on several audits of the subsystem by the FBI's Inspection Division, the Department has concluded that the subsystem has significantly improved the FBI's compliance with the NSL statute and has reduced errors in the production of NSLs to a very low rate. It also has increased the accuracy of NSL reporting.

**FBI/DOJ Oversight of NSLs**

Following the 2007 OIG Report regarding NSLs, the FBI also took a hard look at all of its policies regarding NSLs and the communication of those policies to FBI employees. In addition to developing and deploying the NSL subsystem, the FBI tightened policies and procedures that existed and ensured that they were all put into a single comprehensive document that was disseminated to the field. That document required legal reviews of all NSLs, required retention of signed copies of NSLs and ECs supporting the NSLs in the investigative file, and required a review of information received in response to an NSL to ensure there had been no "overproduction" of information. Since December 2008, all of those rules have been available in the FBI's Domestic Investigations and Operations Guide ("DIOG"), of which employees have copies and which also is available to all employees on their FBI computers.

In addition, since 2008, the FBI's Inspection Division has conducted a number of NSL audits. The Inspection Division audit is a focused review of the use of NSLs in an effort to assess the FBI's compliance with all applicable policies, statutes, and guidelines with respect to the issuance of NSLs and the handling of NSL results, to determine the efficacy of corrective actions taken subsequent to their prior audits, and to propose additional corrective action as appropriate. The Inspection Division audit reviews every NSL that is created outside of the NSL subsystem. For NSLs prepared within the subsystem, the Inspection Division audits a sample. Each Inspection Division audit thus far has shown minimal non-compliance, with the most recent audits for 2008 and 2009 showing only about 0.7% of reviewed NSLs having any compliance issues.

Also following the OIG's 2007 NSL review, the FBI established a compliance office, modeled on those established by publicly-traded companies, to look critically at areas of legal risk to ensure that policies, procedures, and training were designed and executed in a way that

would maximize the likelihood of full legal compliance. That office, the Office of Integrity and Compliance ("OIC"), is focused on NSLs, as well as other areas of legal risk to the FBI.

The FBI's OGC has conducted extensive NSL training both at FBI Headquarters and in field offices. In addition, an online training course is required for all employees involved in drafting, reviewing, and approving NSLs.

Finally, the Department of Justice, National Security Division, and the FBI's OGC conduct oversight of FBI field offices each year through National Security Reviews ("NSRs"). The NSR teams typically review between 15-20 field offices per year. During those reviews, among other compliance issues, attorneys conduct comprehensive reviews of the field office's use of NSLs, including compliance with the applicable laws and policies.

For each national security investigation reviewed, the NSR teams examine all aspects of NSL use in the investigation. For each NSL selected, the NSR teams examine the authorizing EC, the NSL itself, and the subsequent results. For example, among the items considered during the review, the teams analyze the NSL's authorizing EC to ensure that there is a sufficient nexus between the records sought and the investigation. In so doing, the teams can verify not only that the FBI has established the relevancy of the request to the investigation, as required by the authorizing NSL statutes, but also documented that nexus so that the approving officials have enough information to make an informed decision regarding authorization of the NSL.

The NSR teams also examine the NSL to determine the scope of the request and carefully review the results supplied in response. In this manner, the NSR teams are able to verify whether the FBI is properly handling those instances when material is provided that exceeds the scope of an NSL. Although over-productions are the result of third-party action, it is the FBI's responsibility to manage correctly the disposition of such information. This includes promptly identifying the over-production, as well as ensuring that over-produced material is not used in furtherance of an investigation or uploaded into FBI databases.

It is noteworthy that, even as of 2008, the Office of Inspector General concluded that "since the issuance of our March 2007 report, the FBI and the Department have made significant progress in implementing the recommendations from that report and in adopting other corrective actions to address serious problems we identified in the use of national security letters." *See* 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). Since that time, the FBI and DOJ reviews described above have found that NSLs are being properly issued in the overwhelming majority of cases. At the conclusion of each NSR, the field office receives an oral out-briefing detailing the results of the review, including its handling of NSLs, and providing

recommendations regarding any areas found to be deficient. This is followed up by a formal written report.

**NSL Procedures**

Last year, the Attorney General approved new procedures for FBI's collection, use, and storage of information obtained from NSLs. The purpose of these procedures is to improve adherence to the NSL statutes and provide additional privacy safeguards for NSL-obtained information without impeding the FBI's operational and technical mission requirements. These procedures are designed to interrelate with the DIOG mentioned above, which in turn implements the Attorney General's Guidelines for Domestic FBI Operations, also mentioned above. Department officials have briefed Congress, including the House and Senate Judiciary Committees, on these new procedures.

As set forth in the new procedures, FBI employees must review all information produced in response to NSLs seeking financial records to ensure that information that (a) is not responsive to the NSL or (b) has no investigative value is not entered into the electronic case file. If the information is responsive to the NSL *and* has potential investigative value, it may be uploaded into the Automated Case Support System ("ACS") or other FBI databases. NSL-derived information may, however, be entered temporarily into local electronic files on desktop computers for initial analysis to determine whether it is responsive and has investigative value. Any non-responsive information must be sequestered with the chief division counsel ("CDC") or the National Security Law Branch ("NSLB") for proper handling (*i.e.*, either destruction or return to the party from which they were requested), and the NSLB must be notified of the over-production, in accordance with established procedures.

As the FBI develops technology to assist in the analysis of financial data, so that the FBI can draw important investigative links between disparate data, all data that are responsive to NSLs (regardless of whether it is assessed to have immediate investigative value) may be entered into a separate, secure database with effective access controls, an established access policy, and an effective audit capability to monitor compliance. The access policy must ensure that NSL data in the separate data base (*i.e.*, data that were responsive to NSL requests but did not have apparent investigative value at the time they were received) are not retrieved and uploaded into ACS unless and until their investigative value is established through an authorized search of the separate database. Information that is not responsive to the NSL request may not be uploaded into any FBI database and must either be destroyed or returned to the provider.

**UNCLASSIFIED**

**The Value of NSLs**

I would like to conclude my remarks by emphasizing how important NSLs are to our national security. NSLs are an indispensable investigative tool, and have often been described as the "building blocks" of national security investigations. NSLs contribute significantly to the FBI's ability to carry out its national security responsibilities by directly supporting its counterterrorism, counterintelligence, and intelligence missions.

As reported in the Department's last annual report on NSL usage, excluding requests for subscriber information (*i.e.*, an NSL issued to ascertain the subscriber associated with a particular telephone or email address), in 2009, the FBI made 14,788 NSL requests for information concerning 6,114 different United States persons. In 2008, the FBI made 24,744 NSL requests (excluding requests for subscriber information) pertaining to 7,225 United States persons. These numbers reflect the importance of these tools to the FBI, but also reflect the fact that the FBI uses NSLs to obtain information regarding a very small portion of the American population.

NSLs are issued by the FBI in national security cases for a variety of investigative reasons. They are used in counterintelligence cases in which individuals are suspected of attempting to steal our nation's secrets, including espionage cases. They are used extensively in terrorism cases to help correctly identify international terrorists and thwart future attacks in the United States. As an investigative tool, NSLs are integral to determining whether, how, and by whom our nation is being put at risk. So, while I cannot discuss specific investigative techniques that were used in specific investigations, NSLs were used in most cases, if not every major case, in which the FBI has disrupted terrorist plots against the homeland or identified spies working to obtain classified United States Government information. These tools have helped keep our nation safe, while safeguarding the civil liberties of all Americans.



---

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

## TESTIMONY OF KENNETH L. WAINSTEIN, PARTNER, O'MELVENY & MYERS LLP

Mr. WAINSTEIN. Thank you, Mr. Chairman, Ranking Member Scott, Members of the Subcommittee. Thank you for inviting me to this important hearing. I am honored to join my two distinguished

co-panelists in the continued national dialogue about the PATRIOT Act.

In assessing the PATRIOT Act, it is important that we first recognize the historical context in which it was passed. Before the morning of September 11th, 2001, the Nation had not fully awakened to the deadly threat that we faced from international terrorists. That all changed with the attacks of September 11th. Our Nation immediately put itself on a war footing, a war that the Government is vigorously pursuing to this day, and undertook to mobilize the Nation's resources toward the goal of preventing another 9/11 attack.

A crucial part of that mobilization took place up here on Capitol Hill when Congress took stock of our national security authorities, found them inadequate, and acted quickly passing the original PATRIOT Act on October 25th, 2001. The passage of this legislation marked a sea change in our approach to international terrorism in a number of ways.

For one, it gave our national security professionals a number of important tools that had long been available to criminal investigators, tools like the roving surveillance authority.

Second, the PATRIOT Act enhanced the Government's ability to anticipate and prevent terrorism by, for example, reducing the evidentiary threshold for issuance of Section 215 orders and National Security Letters for third party records about a person, allowing agents to use these tools to investigate leads and connect the dots at the first indication that that person might somehow be relevant to a national security investigation.

Third, the PATRIOT Act reduced a number of administrative burdens that had previously complicated and slowed the pace of our national security investigations.

And finally and arguably most significantly, the PATRIOT Act lowered the perceived wall between our law enforcement and intelligence community personnel—that set of procedures that had grown out of the rules of practice in the FISA Court and that prevented our law enforcement officers and our intelligence agents from coordinating operations and sharing information about terrorist suspects, thereby bifurcating our counterterrorism operations just when we needed them to be fully integrated to meet the growing threat from international terrorism.

Congress lowered this procedural wall in the PATRIOT Act, and with these changes we now have the ability to deploy all of our national counterterrorism personnel and assets in a coordinated, worldwide campaign against what the President has aptly described as al Qaeda's far-reaching network of violence and hatred.

It is worth noting that all of these significant legislative improvements were drafted, considered, and enacted within a mere 45 days of the 9/11 attacks. Congress is to be commended for moving with such urgency but also for taking the hurried enactment into account and building into the law the sunset provisions that required a future examination of these authorities and their implementation.

In 2005, Congress went through a lengthy process of carefully scrutinizing each and every provision and identifying those where additional limitations or oversight could provide valuable protec-

tion against misuse without reducing their operational effectiveness. This process resulted in the 2006 reauthorization act which added significant new safeguards for many of the PATRIOT Act authorities.

In addition to these new safeguards, the executive branch has substantially increased its own internal national security oversight in the years since 9/11. That effort can be seen in a number of initiatives that have been pursued by the FBI and the National Security Division at main Justice, especially in the aftermath of the Inspector General's 2007 report finding serious flaws in the FBI's use of the NSL authority.

In 2007, the FBI established its Office of Integrity and Compliance which is tasked with establishing and implementing compliance policy throughout the bureau, and that same year, the National Security Division in main Justice established a new section devoted to oversight of the FBI's national security operations. This was actually an historic development. While DOJ attorneys had previously had a role in conducting oversight into certain areas of national security operations, that role was limited. It was only upon the stand-up of the Oversight Section that Justice Department attorneys were given the complete mandate to examine all aspects of the FBI's national security program. These two new offices reflect the Justice Department's commitment to compliance and have gone a long way toward institutionalizing and embedding effective oversight within the operations of our national security program.

Over this past decade, the executive branch and Congress have succeeded in building investigative infrastructure and capabilities that are necessary to protect our national security. Thanks to the determined efforts of our law enforcement and intelligence leadership and personnel, we now have a formidable counterterrorism program that has succeeded in preventing another 9/11 attack and keeping al Qaeda off balance. And thanks to Congress' forceful but careful effort to bring our national security authorities into line with today's threat from international terrorism, we now have a well balanced legislative framework governing our counterterrorism operations. In light of this history, we have every reason to approach the 10-year anniversary of the PATRIOT Act with confidence that its authorities and safeguards will continue to contribute both to the defense of our national security and to the protection of our civil liberties.

Thank you, Mr. Chairman. I would be happy to answer any questions you may have.

[The prepared statement of Mr. Wainstein follows:]

**STATEMENT OF**

**KENNETH L. WAINSTEIN**
**PARTNER, O'MELVENY & MYERS LLP**

**BEFORE THE**

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

**CONCERNING**

**THE PATRIOT ACT**

**PRESENTED ON**

**MARCH 30, 2011**

Chairman Sensenbrenner, Ranking Member Scott, and Members of the Subcommittee, thank you for inviting me to this important hearing. My name is Ken Wainstein, and I am a partner at the law firm of O'Melveny & Myers. Prior to my leaving the government in January, 2009, I served in a variety of capacities, including Homeland Security Advisor to the President, Assistant Attorney General for National Security, United States Attorney, General Counsel and Chief of Staff of the FBI, and career federal prosecutor.

During that time, I was honored to work alongside the men and women who devote themselves to protecting our national security, and to participate -- along with my two distinguished co-panelists -- in what has been a very constructive national discussion over the past decade about the intersection of national security operations and the protection of privacy and civil liberties. I commend the Subcommittee for continuing this important dialogue about the appropriate parameters of the government's investigative capabilities in our country's fight against international terrorism.

We will soon mark the ten-year anniversary of the PATRIOT Act, the legislation that significantly boosted our counterterrorism capabilities in the aftermath of the 9/11 attacks. It is fitting that the Subcommittee takes this occasion to reflect on the utility of that statute over the past decade and its impact on privacy and civil liberties.

1. Passage of the PATRIOT Act

In assessing the PATRIOT Act, it is important that we first recognize the historical context in which it was passed. Before the morning of September 11, 2001, the Nation had not fully awakened to the deadly threat we faced from international terrorists. As a result, we had not developed the national counterterrorism apparatus to meet the threat from organizations like al Qaeda. Our counterterrorism operations were limited in size and scope, and there were impediments to effective coordination among the agencies running those operations.

That all changed with the attacks of September 11, 2001. Our Nation immediately put itself on a war footing against al Qaeda -- a war that the government is vigorously pursuing to this day -- and undertook to mobilize the Nation's resources toward the goal of preventing another 9/11 attack. That effort has resulted in comprehensive changes across the government -- from the commitment of significant new counterterrorism resources to the wholesale reorganization of the government's intelligence apparatus.

A crucial part of that mobilization effort also took place up here on Capitol Hill, where Congress undertook the important task of evaluating and enhancing the investigative tools available to our counterterrorism personnel. Immediately after the 9/11 attacks, Congress took stock of our national security authorities and found them inadequate for several reasons: (1) they were designed more for the traditional adversaries of the Cold War and less for the asymmetrical terrorist threat we face today; (2) they did not permit sufficient coordination and information sharing between law enforcement and intelligence personnel; and (3) they did not provide to national security professionals many of the basic investigative tools that had long been available to law enforcement investigators. The upshot was that agents on the front lines of our

counterterrorism program lacked the tools they needed to identify, investigate and neutralize plots before they matured into terrorist attacks.

Congress recognized that this situation was unacceptable and acted quickly, drawing up an omnibus package of authorities and passing the original PATRIOT Act on October 25, 2001. The passage of this legislation marked a sea change in our approach to international terrorism, and its effect could immediately be felt throughout our counterterrorism operations in a variety of ways.

For one, it gave our national security professionals a number of important tools that had long been available only to criminal investigators. For example, Section 206 of the PATRIOT Act allowed the FISA Court to authorize "roving" surveillance, an authority that permits the government to maintain surveillance coverage on a target as he or she moves from one communication device to another. While law enforcement personnel investigating crimes like drug offenses and racketeering have been using roving wiretaps since 1986, national security agents trying to prevent terrorist attacks only received this authority with the passage of the PATRIOT Act. Similarly, Section 215 of the PATRIOT Act gave national security personnel the authority to compel production of business records and other tangible things, a tool that is comparable to the criminal prosecutor's longstanding ability to acquire such items with a grand jury subpoena.

Second, the PATRIOT Act enhanced the government's ability to anticipate and prevent terrorism by refining certain existing tools to make them more useful in identifying suspects and plots in the early stages of investigation. For instance, the statute reduced the evidentiary threshold for issuance of Section 215 orders and National Security Letters ("NSLs") for third-party records about a person, allowing agents to use these tools to investigate leads and connect the dots at the first indication that that person might somehow be relevant to a national security investigation.

Third, the PATRIOT Act reduced a number of the administrative burdens that had complicated and slowed the pace of our national security investigations by, for example, extending the duration of FISA wiretap orders, delegating the authority to issue NSLs down to the field office level, and permitting agents to obtain search warrants for electronic communications information that can be served in any judicial district around the country.

Fourth, the PATRIOT Act greatly facilitated the sharing of certain types of national security information between criminal investigators and intelligence agents. It removed the previous prohibition on sharing information from a criminal wiretap with intelligence agents, and it expressly authorized criminal investigators to share any foreign intelligence information that they come upon in their investigations with interested national security personnel.

Finally -- and arguably most significantly -- the PATRIOT Act lowered the perceived "wall" between our law enforcement and Intelligence Community personnel -- a set of rules and procedures that prevented those two groups from coordinating operations and sharing information about terrorist suspects.

This wall grew out of the requirement in the Foreign Intelligence Surveillance Act ("FISA") that the collection of foreign intelligence had to be "*the* purpose" of a wiretap or search authorized by the FISA Court. Over the decades after the 1978 passage of FISA, that statutory provision became interpreted to require that intelligence agents could obtain a FISA surveillance or search order only if they showed the FISA Court that collecting foreign intelligence was "the *primary* purpose" of the surveillance or search authority they sought. In order to make that showing, it became necessary for intelligence agents to limit coordination with criminal investigators so as to avoid the risk that the FISA Court might suspect that criminal investigation and prosecution was actually their primary purpose.

This led to the situation where intelligence agents who were tracking a terrorist target felt they could not share information or coordinate operations with law enforcement agents who were pursuing a criminal investigation against the very same target -- thereby bifurcating our counterterrorism operations just when we needed them to be fully integrated to meet the growing threat of international terrorism. This situation prevailed as al Qaeda was expanding its reach and attacking our interests around the world, and the wall was still firmly in place when the terrorists struck on 9/11.

Congress rectified this situation in the PATRIOT Act by eliminating the "primary purpose" test and providing that a FISA order was appropriate so long as the collection of foreign intelligence was a "significant" purpose of the surveillance or search. It also expressly permitted agents using intelligence tools like FISA to consult and coordinate activities with their law enforcement counterparts who were pursuing the same terrorists, spies and other national security targets.

The lowering of the wall and the new information-sharing authorities in the PATRIOT Act led to fundamental changes in the conduct of our Nation's counterterrorism program. Our analysts can now gather, synthesize, and disseminate terrorist threat information around the law enforcement and intelligence communities without jeopardizing the ability to secure FISA orders; our FBI and Intelligence Community leaders can freely share information and coordinate operations on a daily basis; and our federal government can fully partner with the 700,000-odd law enforcement officers who are the eyes and ears of our counterterrorism effort within the United States.

With these changes, we now have the ability to deploy all of our national counterterrorism personnel and assets in a coordinated, worldwide campaign against what the President has described as al Qaeda's "far-reaching network of violence and hatred."

2. The Reauthorization Act of 2006

It is worth noting that all of these significant legislative improvements were drafted, considered and enacted within a mere 45 days of the 9/11 attacks. Congress is to be commended for moving with urgency and speed and producing such a well-considered piece of legislation. Congress was also wise to take the hurried enactment into account and to build into the law the sunset provisions that required a future examination of these authorities and their implementation.

Starting in 2005, Congress undertook the process of re-examining each of these authorities and engaged in a vigorous debate over their reauthorization. To its credit, Congress went through a lengthy process of carefully scrutinizing each provision and identifying those where additional limitations or oversight could provide valuable protection against misuse without reducing their operational effectiveness. This process resulted in the 2006 Reauthorization Act, which added significant new safeguards for many of the primary authorities in the original PATRIOT Act. Examples include:

- Revising the NSL authorities to provide that NSL recipients can challenge the NSLs and their nondisclosure provisions and to require the Justice Department Inspector General to review the Department's use of the NSL authority for potential misuse; and

- Addressing concerns raised about Section 215 orders by providing a means for challenging the legality of a Section 215 order and its nondisclosure provision and by requiring high-level approval within the FBI before such an order could be sought for sensitive records like library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, or certain medical records.

3. Oversight within the Justice Department

In addition to these new safeguards and the various provisions for legislative and judicial oversight built into the PATRIOT Act authorities, the Executive Branch has substantially increased its own internal national security oversight. That effort can be seen in a number of initiatives that have been pursued by the FBI and the National Security Division in Main Justice. Besides generally enhancing the coverage and frequency of oversight efforts -- especially in the aftermath of the Inspector General's 2007 report finding serious flaws in the FBI's use of the NSL authority -- both components established strong offices devoted to monitoring the FBI's compliance with all regulations and laws governing its national security program.

In 2007, the FBI established its Office of Integrity and Compliance, an office reporting to the Deputy Director that is tasked with establishing and implementing compliance policy throughout the Bureau, monitoring and ensuring compliance audits within the Bureau's operational programs, and instilling a set of procedures and a culture of constant respect for compliance within the Bureau.

That same year, the National Security Division -- my old division in the Justice Department -- established a new section devoted to oversight of the FBI's national security operations. While DOJ attorneys previously had a role in conducting oversight into certain areas of those operations, that role was limited. It was only upon the stand-up of the Oversight Section that Justice Department attorneys were given the complete mandate to examine all aspects of the FBI's national security program. Since then, the Oversight Section has worked closely with the FBI's Office of the General Counsel to conduct field office compliance reviews, in which FBI and DOJ attorneys travel to an FBI field office and conduct a thorough file review to ensure that agents in that office are following all applicable laws, regulations, and policies in their use of national security investigative authorities.

These two new offices reflect a genuine commitment to compliance, and have gone a long way toward institutionalizing and embedding effective oversight within the operations of our national security program.

4. Conclusion

Over this past decade, the Executive Branch and Congress have succeeded in building the investigative infrastructure and capabilities that are necessary to protect our national security. Thanks to the determined efforts of our law enforcement and intelligence leadership and personnel, we now have a formidable counterterrorism program that has succeeded in preventing another 9/11 attack and keeping al Qaeda off balance. And thanks to Congress' forceful -- but careful -- effort to bring our national security authorities in line with today's threat from international terrorism, we now have a well-balanced legislative framework governing our counterterrorism operations. In light of this history, we have every reason to approach the ten-year anniversary of the PATRIOT Act with confidence that its authorities and safeguards will continue to contribute both to the defense of our national security and to the protection of our civil liberties.



---

Mr. SENSENBRENNER. Thank you very much.
The Chair recognizes Mr. German for 5 minutes.

**TESTIMONY OF MICHAEL GERMAN, SENIOR POLICY COUNSEL, AMERICAN CIVIL LIBERTIES UNION**

Mr. GERMAN. Good morning, Chairman Sensenbrenner, Ranking Member Scott, and Members of the Subcommittee. Thank you for the opportunity to testify on behalf of the American Civil Liberties Union as Congress revisits the USA PATRIOT Act.

The PATRIOT Act vastly and unconstitutionally expanded the Government's authority to pry into people's private lives with little or no evidence of wrongdoing, violating Fourth Amendment protections against unreasonable searches and seizures and First Amendment protections of free speech and association.

Worse, it allows this expanded spying to take place in secret with few protections to ensure these powers are not abused and little opportunity for Congress to determine whether these authorities are actually making America safer.

There has not been a full public accounting about how all the powerful tools of the PATRIOT Act have been used against Americans. But the little information that has been made public points to repeated abuse. Inspector General audits ordered in the PATRIOT Act reauthorization revealed significant abuse of National Security Letters, and courts have found several PATRIOT Act provisions unconstitutional, including the NSL gag orders, certain material support provisions, ideological exclusion provisions, and the FISA "significant purpose" standard.

One of the most abused provisions of the PATRIOT Act is the National Security Letter authority. These requests for communication, financial and credit information are issued by the FBI without review by a court or Department of Justice attorney. And because of the PATRIOT Act provisions to the NSL statutes, they may be used to gather records about anyone the FBI deems relevant to an investigation, even if they are not suspected of wrongdoing.

The Department of Justice Inspector General confirmed that the FBI issues upwards of 50,000 NSL's a year, often against people two and three times removed from the suspected terrorist or agent of foreign power under investigation. The majority of NSL's are used against U.S. persons. The FBI reported that it has addressed a number of mismanagement issues identified in the Inspector General report, but the NSL's fundamental flaw, its use to collect sensitive information on people who are not suspected of doing anything wrong, and the indefinite retention and use of that information, must be addressed by Congress.

The ACLU has endorsed a number of proposals to amend the NSL statute short of repealing the PATRIOT Act NSL provision, including Ranking Member Conyers' reauthorization bill from last year and the Justice Act that was introduced in the House and Senate in the 111th Congress. Those bills would limit the use of NSL's to the collection of information that pertains to a foreign power, an agent of a foreign power's activities, or someone in contact with an agent of a foreign power. Requiring such a nexus would permit the Government to collect information, pertinent information, while protecting wholly innocent information from being caught in a massive Government dragnet. The NSL gag provisions, which have been deemed unconstitutional, should also be remedied by statute.

Congress should also amend the material support statute. While the statute has been in existence for some time, the PATRIOT Act and subsequent reauthorization legislation has expanded and redefined what material support means. We all acknowledge the Government's legitimate and compelling interest in protecting the Nation from terrorism and in stemming material support that furthers the unlawful violent acts of terrorist groups. But this overbroad statute does not make an exception for associational or humanitarian activity that does not in fact further an organization's illegal activities, and it therefore chills charitable efforts that the Government should be encouraging. The generosity of the American people toward those in need around the world is an asset to U.S. counterterrorism efforts, and Congress should remedy this unintended chill on legitimate humanitarian efforts by revising the statute.

In addition to these sections, there are other permanent provisions of the PATRIOT Act that violate the Constitution and civil liberties and they are addressed in my written testimony. For example, the so-called "sneak and peek" authority, ideological exclusion provisions, and amendments to the Foreign Intelligence Surveillance Act. Surveillance authorities outside the PATRIOT Act should be reviewed as well so Congress can get a comprehensive picture of how these authorities work together.

Despite some claims to the contrary, much of the PATRIOT Act was not controversial and the provisions that do not infringe on privacy need not necessarily be repealed. Overwhelmingly common sense amendments can be adopted to protect privacy while permitting the Government to gather information about those it actually suspects are probable terrorists or spies. We urge the Committee to include such protections in any legislation it reports.

Thank you very much.

[The prepared statement of Mr. German follows:]

Written Statement of
Michael German, Senior Policy Counsel

American Civil Liberties Union
Washington Legislative Office

On

"The Permanent Provisions of the PATRIOT Act"

Before the

Subcommittee on Crime, Terrorism and Homeland Security

House Committee on the Judiciary

March 30, 2011

**WASHINGTON LEGISLATIVE OFFICE**
915 15th Street, NW Washington, D.C. 20005
(202) 544-1681 Fax (202) 546-0738

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

More than nine years after its implementation there is little evidence that the Patriot Act has been effective in making America more secure from terrorists. However, there are many unfortunate examples that the government abused these authorities in ways that both violate the rights of innocent people and squander precious security resources. Three Patriot Act-related surveillance provisions are scheduled to expire in May 2011, which will give the 112th Congress an opportunity to review and thoroughly evaluate all Patriot Act authorities – as well as all other post-9/11 domestic intelligence programs – and rescind, repeal or modify provisions that are unused, ineffective or prone to abuse. The American Civil Liberties Union encourages Congress to exercise its oversight powers fully, to restore effective checks on executive branch surveillance powers and to prohibit unreasonable searches and seizures of private information without probable cause based on particularized suspicion.

In a September 14, 2009 letter to the Senate Judiciary Committee, the Department of Justice (DOJ) called for "a careful examination" of the expiring Patriot Act authorities and stated its willingness to consider modifications that would "provide additional protection for the privacy of law abiding Americans."[2] Congress should accept this invitation and conduct a thorough evaluation of all government surveillance authorities. The DOJ letter went on to argue for reauthorization of all three provisions without amendment but we believe that the "careful examination" it calls for will reveal that these and many other surveillance authorities are unnecessary and unconstitutionally broad.

**OUR FOUNDING FATHERS FOUGHT FOR THE RIGHT TO BE FREE FROM GOVERNMENT INTRUSION**

The Fourth Amendment to the U. S. Constitution protects individuals against 'unreasonable searches and seizures.' In1886, Supreme Court Justice Joseph P. Bradley suggested that the meaning of this phrase could not be understood without reference to the historic controversy over general warrants in England and her colonies.[3] General warrants were broad orders that allowed the search or seizure of unspecified places or persons, without probable cause or individualized suspicion. For centuries, English authorities had used these broad general warrants to enforce "seditious libel" laws designed to stifle the press and suppress political dissent. This history is particularly informative to an analysis of the Patriot Act because the purpose of the Fourth Amendment was not just to protect personal property, but "to curb the exercise of discretionary authority by [government] officers."[4]

To the American colonists, nothing demonstrated the British government's illegitimate use of authority more than "writs of assistance" – general warrants that granted revenue agents of the Crown blanket authority to search private property at their own discretion.[5] In 1761, in an event that John Adams later described as "the first act of opposition" to British rule, Boston lawyer James Otis condemned general warrants as "the worst instrument of arbitrary power, the most destructive of English liberty and the fundamental principles of law, that ever was found in an English law book."[6] Otis declared such discretionary warrants illegal, despite their official government sanction, because they "placed the liberty of every man in the hands of every petty officer."[7] The resistance to writs of assistance provided an ideological foundation for the American Revolution – the concept that the right of the people to be free from unwarranted government intrusion into their private affairs was the essence of liberty. American patriots carried a declaration of this foundational idea on their flag as they marched into battle: "Don't tread on me."

Proponents of the Patriot Act suggest that reducing individual liberties during a time of increased threat to our national security is both reasonable and necessary, and that allowing fear to drive the government's decisions in a time of emergency is "not a bad thing."[8] In effect, these modern-day patriots are willing to exchange our forbearers' "don't tread on me" banner for a less inspiring, one reading "if you aren't doing anything wrong you have nothing to worry about."

Colonial-era patriots were cut from different cloth. They saw liberty not as something to trade for temporary comfort or security, but rather as a cause worth fighting for even when the odds of success, not to mention survival, were slight. Our forbearers' commitment to personal liberty did not waver when Great Britain sent troops to quell their rebellion, nor did it waver during the tumultuous and uncertain period following the war as they struggled to establish a government that could secure the blessings of the liberty they fought so hard to win.

The framers of the Constitution recognized that giving the government unchecked authority to pry into our private lives risked more than just individual property rights, as the Supreme Court later recounted: "The Bill of Rights was fashioned against the background of knowledge that unrestricted power of search and seizure could also be an instrument for stifling liberty of expression."[9] These patriots understood from their own experience that political rights could not be secured without procedural protections. The Fourth Amendment requirements of prior judicial review and warrants issued only upon probable cause were determined to be the necessary remedies to the arbitrary and unreasonable assaults on free expression that were characterized by the government's use of general warrants. "The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another."[10] The Supreme Court has long acknowledged the important interplay between First Amendment and Fourth Amendment freedoms. As it reflected in 1965, "what this history indispensably teaches is that the constitutional requirement that warrants must particularly describe the 'things to be seized' is to be accorded the most scrupulous exactitude when the 'things' are books, and the basis for their seizure is the ideas which they contain."[11]

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

> National security cases, moreover, often reflect a convergence of First and Fourth Amendment values not present in cases of "ordinary" crime. Though the investigative duty of the executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech.[12]

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

Stifling dissent does not enhance security. The framers created our constitutional system of checks and balances to curb government abuse, and ultimately to make the government more responsive to the needs of the people – which is where all government

power ultimately lies. The Patriot Act gave the executive branch broad and unprecedented discretion to monitor electronic communications and seize private records, placing individual liberty, as John Otis warned, "in the hands of every petty officer." Limiting the government's power to intrude into private affairs, and checking that power with independent oversight, reduces the error and abuse that conspire to undermine public confidence. As the original patriots knew, adhering to the Constitution and the Bill of Rights makes our government stronger, not weaker.

**EXCESSIVE SECRECY THWARTS CONGRESSIONAL OVERSIGHT**

Just 45 days after the worst terrorist attack in history Congress passed the Patriot Act, a 342-page bill amending more than a dozen federal statutes, with virtually no debate. The Patriot Act was not crafted with careful deliberation, or narrowly tailored to address specific gaps in intelligence gathering authorities that were found to have harmed the government's ability to protect the nation from terrorism. In fact, the government hesitated for months before authorizing an official inquiry, and it took over a year before Congress published a report detailing the many significant pieces of intelligence the government lawfully collected before 9/11 but failed to properly analyze, disseminate or exploit to prevent the attacks.[13] Instead of first determining what led to the intelligence breakdowns and then legislating, Congress quickly cobbled together a bill in ignorance, and while under intense pressure, to give the president all the authorities he claimed he needed to protect the nation against future attacks.

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

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

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

**NEW SUNSET DATES CREATE OVERSIGHT AND AMENDMENT OPPORTUNITY**

When Congress reauthorized the Patriot Act in 2006, it established new expiration dates for two Patriot Act provisions and for a related provision of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA).[18] After a series of reauthorizations these three provisions, **section 206** and **section 215** of the Patriot Act and **section 6001** of the IRTPA, are all set to expire on May 27, 2011. The 112th Congress will revisit these provisions this year, which creates an opportunity for Congress to examine and evaluate the government's use and abuse of all Patriot Act authorities, as well as any other post-9/11 surveillance or security programs.

**Section 206** of the Patriot Act authorizes the government to obtain "roving wiretap" orders from the Foreign Intelligence Surveillance Court (FISC) whenever a subject of a wiretap request uses multiple communications devices. The FISC is a secret court established under the Foreign Intelligence Surveillance Act (FISA) that issues classified orders for the FBI to conduct electronic surveillance or physical searches in intelligence investigations against foreign agents and international terrorists. Unlike roving wiretaps authorized for criminal investigations,[19] section 206 does not require the order to identify either the communications device to be tapped nor the individual against whom the surveillance is directed, which is what gives section 206 the Kafkaesque moniker, the "John Doe roving wiretap provision." The reauthorized provision requires the target to be described "with particularity," and the FBI to file an after-the-fact report to the FISC to explain why the government believed the target was using the phones it was tapping. However, it does not require the government to name the target, or to make sure its roving wiretaps are intercepting only the target's communications. The power to intercept a roving series of unidentified devices of an unidentified target provides government agents with an inappropriate level of discretion reminiscent of the general warrants that so angered the American colonists. There is very little public information available regarding how the government uses section 206, though FBI Director Robert Mueller recently revealed in March 25, 2009 testimony before the Senate Judiciary Committee that the FBI obtained roving wiretaps under this authority 147 times.[20] The DOJ's September 14, 2009 letter to the Senate Judiciary Committee offers no explanation for why the roving wiretap authorities the FBI has used in criminal cases since 1986, which better protect the rights of completely innocent persons, are insufficient. This provision should be narrowed to bring it in line with criminal wiretap authorities, or be allowed to expire.

The DOJ letter revealed that the FBI has never used the surveillance authorities granted under **section 6001** of the IRTPA, which is known as the "lone wolf" provision. Section 6001 authorizes government agencies to obtain secret FISA surveillance orders against individuals who are not connected to any international terrorist group or foreign nation. The government justified this provision by imagining a hypothetical "lone wolf," an international terrorist operating independently of any terrorist organization, but there is little evidence to suggest this imaginary construct had any basis in reality. The failure to use this authority seems to substantiate this claim. Moreover, since terrorism is a crime,

there is no reason to believe that the government could not obtain a Title III surveillance order from a criminal court if the government had probable cause to believe an individual was planning an act of terrorism.[21] Quite simply, this provision allows the government to avoid the more exacting standards for obtaining electronic surveillance orders from criminal courts. The constitutionality of a provision that allows the government to circumvent the warrant requirement of the Fourth Amendment where there is no connection to a foreign power or international terrorist group remains dubious. Congress should not provide the government an unconstitutionally broad power; especially where the problem it resolves only exists in hypothetical. This provision should be allowed to expire.

**Section 215** of the Patriot Act provides a sweeping grant of authority for the government to obtain secret FISC orders demanding "any tangible thing" it claims is relevant to an authorized investigation regarding international terrorism or espionage. Known as the "library provision," section 215 significantly expands the types of items the government can demand under FISA and lowers the standard of proof necessary to obtain an order. Prior to the Patriot Act, FISA required probable cause to believe the target was an agent of a foreign power. Section 215 only requires the government to claim the items sought are relevant to an authorized investigation. Most significant in this change of standard, however, was the removal of the requirement for the FBI to show that the items sought pertain to a person the FBI is investigating. Under section 215, the government can obtain orders for private records or items belonging to people who are not even under suspicion of involvement with terrorism or espionage, including U.S. citizens and lawful resident aliens, not just foreigners.

Section 215 orders come with compulsory non-disclosure orders, which contributed to the secrecy surrounding how they were being used. To ensure that it would have at least some information upon which to evaluate Patriot Act powers before the next sunset period, Congress included a provision in the 2006 Patriot Act reauthorization that required the Department of Justice Inspector General (IG) to audit the FBI's use of National Security Letters (NSLs) and section 215 orders.[22] These reports provided the first thorough examination of the implementation of the post-9/11 anti-terrorism powers. They also confirmed what our nation's founders already knew: unchecked authority is too easily abused.

## EVIDENCE OF ABUSE: THE INSPECTOR GENERAL AUDITS

### NATIONAL SECURITY LETTERS

NSLs are secret demand letters issued without judicial review to obtain sensitive personal information such as financial records, credit reports, telephone and e-mail communications data and Internet searches. The FBI had authority to issue NSLs through four separate statutes, but these authorities were significantly expanded by **section 505** of the Patriot Act.[23] **Section 505** increased the number of officials who could authorize NSLs and reduced the standard necessary to obtain information with them, requiring only an internal certification that the records sought are "relevant" to an authorized

counterterrorism or counter-intelligence investigation. The Patriot Act reauthorization made the NSL provisions permanent.

The NSL statutes now allow the FBI and other executive branch agencies to obtain records about people who are not known – or even suspected – to have done anything wrong. The NSL statutes also allow the government to prohibit NSL recipients from disclosing that the government sought or obtained information from them. While Congress modified these "gag orders" in the Patriot Act reauthorization to allow NSL recipients to consult a lawyer, under the current state of the law NSLs are still not subject to any meaningful level of judicial review (ACLU challenges to the NSL gag orders are described below).[24]

The first two IG audits, covering NSLs and section 215 orders issued from 2003 through 2005, were released in March of 2007. They confirmed widespread FBI mismanagement, misuse and abuse of these Patriot Act authorities.[25] The NSL audit revealed that the FBI managed its use of NSLs so negligently that it literally did not know how many NSLs it had issued. As a result, the FBI seriously under-reported its use of NSLs in its previous reports to Congress. The IG also found that FBI agents repeatedly ignored or confused the requirements of the NSL authorizing statutes, and used NSLs to collect private information against individuals two or three times removed from the subjects of FBI investigations. Twenty-two percent of the audited files contained unreported legal violations.[26] Most troubling, FBI supervisors used hundreds of illegal "exigent letters" to obtain telephone records without NSLs by falsely claiming emergencies.[27]

On March 13, 2008, the IG released a second pair of audit reports covering 2006 and evaluating the reforms implemented by the DOJ and the FBI after the first audits were released in 2007.[28] Not surprisingly, the new reports identified many of the same problems discovered in the earlier audits. The 2008 NSL report shows that the FBI issued 49,425 NSLs in 2006 (a 4.7 percent increase over 2005), and confirms the FBI is increasingly using NSLs to gather information on U.S. persons (57 percent in 2006, up from 53 percent in 2005).[29]

The 2008 IG audit also revealed that high-ranking FBI officials, including an assistant director, a deputy assistant director, two acting deputy directors and a special agent in charge, improperly issued eleven "blanket NSLs" in 2006 seeking data on 3,860 telephone numbers.[30] None of these "blanket NSLs" complied with FBI policy and eight imposed unlawful non-disclosure requirements on recipients.[31] Moreover, the "blanket NSLs" were written to "cover information already acquired through exigent letters and other informal responses."[32] The IG expressed concern that such high-ranking officials would fail to comply with FBI policies requiring FBI lawyers to review all NSLs, but it seems clear enough that this step was intentionally avoided because the officials knew these NSL requests were illegal.[33] It would be difficult to call this conduct anything but intentional.

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

The FBI's gross mismanagement of its NSL authorities risks security as much as it risks the privacy of innocent persons. The IG reported that the FBI could not locate return information for at least 532 NSL requests issued from the field, and 70 NSL requests issued from FBI headquarters (28 percent of the NSLs sampled).[37] Since the law only allows the FBI to issue NSLs in terrorism and espionage investigations, it cannot be assumed that the loss of these records is inconsequential to our security. Intelligence information continuing to fall through the cracks at the FBI through sheer incompetence is truly a worrisome revelation.

SUGGESTED REFORM OF NSL STATUTES

- Repeal the expanded NSL authorities that allow the FBI to demand information about innocent people who are not the targets of any investigation. Reinstate prior standards limiting NSLs to information about terrorism suspects and other agents of foreign powers.

- Allow gag orders only upon the authority of a court, and only when necessary to protect national security. Limit scope and duration of such gag orders and ensure that their targets and recipients have a meaningful right to challenge them before a fair and neutral arbiter.

- Impose judicial oversight of all Patriot Act authorities. Allowing the FBI to self-certify that it has met the statutory requirements invites further abuse and overuse of NSLs. Contemporaneous and independent oversight of the issuance of NSLs is needed to ensure that they are no longer issued at the drop of a hat to collect information about innocent U.S. persons.

SECTION 215 ORDERS

The IG's **section 215** audits showed the number of FBI requests for section 215 orders were sparse by comparison to the number of NSLs issued. Only 13 section 215 applications were made in 2008.[38]

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

While this portion of the IG report is heavily redacted, it appears that sometime in 2006 the FBI twice asked the FISC for a section 215 order seeking "tangible things" as part of a counterterrorism case. The court denied the request, both times, because "the facts were too 'thin' and [the] request implicated the target's First Amendment rights."[39] Rather than re-evaluating the underlying investigation based on the court's First Amendment concerns, the FBI circumvented the court's oversight and pursued the investigation using three NSLs that were predicated on the same information contained in the section 215 application.[40] The IG questioned the legality of the FBI's use of NSLs based on the same factual predicate contained in the section 215 request the FISC rejected on First Amendment grounds, because the authorizing statutes for NSLs and section 215 orders contain the same First Amendment caveat.[41]

The IG also discovered the FISC was not the first to raise First Amendment concerns over this investigation to FBI officials. Lawyers with the DOJ Office of Intelligence Policy and Review (OIPR) raised the First Amendment issue when the FBI sent the section 215 application for its review.[42] The OIPR is supposed to oversee FBI intelligence investigations, but OIPR officials quoted in the IG report said the OIPR has "not been able to fully serve such an oversight role" and that they were often bullied by FBI agents:

> In addition, the former Acting Counsel for Intelligence Policy stated that there is a history of significant pushback from the FBI when OIPR questions agents about the assertions included in FISA applications. The OIPR attorney assigned to Section 215 requests also told us that she routinely accepts the FBI's assertions regarding the underlying investigations as fact and that the FBI would respond poorly if she questioned their assertions.[43]

When the FISC raised First Amendment concerns about the FBI investigation, the FBI general counsel decided the FBI would continue the investigation anyway, using methods that had less oversight. When asked whether the court's concern caused her to review the underlying investigation for compliance with legal guidelines that prohibit investigations based solely on protected First Amendment activity, the general counsel said she did not because "she disagreed with the court's ruling and nothing in the court's ruling altered her belief that the investigation was appropriate."[44] Astonishingly, she put

her own legal judgment above the decision of the court. She added that the FISC "does not have the authority to close an FBI investigation."[45]

A former OIPR counsel for intelligence policy argued that while investigations based solely on association with subjects of other national security investigations were "weak," they were "not necessarily illegitimate."[46] It is also important to note that this investigation, based on simple association with the subject of another FBI investigation, was apparently not an aberration. The FBI general counsel told the IG the FBI would have to close "numerous investigations" if they could not open cases against individuals who merely have contact with other subjects of FBI investigations.[47] Conducting "numerous investigations" based upon mere contact, and absent facts establishing a reasonable suspicion of wrongdoing, will only result in wasted effort, misspent security resources and unnecessary violations of the rights of innocent Americans.

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

The DOJ's September 14, 2009 letter indicates that no recipient of a section 215 order has ever challenged its validity, and cites this as evidence the authority is not being abused.[48] This argument ignores the fact that section 215 orders are designed to obtain records held in the possession of third parties, as opposed to the subject of the information demand, so the interest in expending the time and expense of fighting such an order is remote. We know the FBI engaged in massive abuse of NSLs, yet out of over two hundred thousand NSL recipients only a handful ever challenged these demands. Moreover, recipients of section 215 orders are gagged from disclosing they received them, so any public debate about the reasonableness of these demands short of a court challenge is effectively thwarted.

Moreover, despite the FBI's infrequent use of section 215, the IG discovered serious deficiencies in the way it managed this authority. The IG found substantial bureaucratic delays at both FBI headquarters and OIPR in bringing section 215 applications to the FISC for approval. While neither the FBI's FISA Management System nor DOJ's OIPR tracking system kept reliable records regarding the length of time section 215 requests remained pending, the IG was able to determine that processing times for section 215 requests ranged from ten days to an incredible 608 days, with an average delay of 169 days for approved orders and 312 days for withdrawn requests.[49] The IG found these delays were the result of unfamiliarity with the proper process, simple misrouting of the section 215 requests and an unnecessarily bureaucratic, self-imposed, multi-layered review process.[50] Most tellingly, the IG's 2008 report found that the process had not improved since the IG identified these problems had been identified in the 2007 audit.[51] DOJ has used long processing times for FISA applications as justification for expanding its surveillance powers and reducing FISC review, but this

evidence shows clearly that ongoing mismanagement at the FBI and OIPR drives these delays, not a lack of authority.[52] Congress should instead compel efficiency at these agencies by increasing its oversight and reining in these expanded authorities.

SUGGESTED REFORMS

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

**UNCONSTITUTIONAL: COURT CHALLENGES TO THE PATRIOT ACT**

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

NATIONAL SECURITY LETTER GAG ORDERS

The ACLU challenged the non-disclosure and confidentiality requirements in NSLs in three cases. The first, *Doe v. Mukasey*, involved an NSL served on an Internet Service Provider (ISP) in 2004 demanding customer records pursuant to the Electronic Communications Privacy Act (ECPA).[53] The letter prohibited the anonymous ISP and its employees and agents "from disclosing to any person that the FBI sought or obtained access to information or records under these provisions." In the midst of a lawsuit over the constitutionality of the NSL provisions in ECPA, the Patriot Act reauthorization was enacted amending the NSL provision but maintaining the government's authority to request sensitive customer information and issue gag orders – albeit in a slightly narrower set of circumstances.[54] In September 2007, the District Court for the Southern District of New York found that even with the reauthorization amendments the gag provision violated the Constitution. The court struck down the amended ECPA NSL statute in its entirety,[55] with Judge Victor Marrero writing that the statute's gag provisions violated the First Amendment and the principle of separation of powers.

In December 2008, the Second U.S. Circuit Court of Appeals upheld the decision in part. The appeals court invalidated parts of the statute that placed the burden on NSL recipients to initiate judicial review of gag orders, holding that the government has the burden to justify silencing NSL recipients. The appeals court also invalidated parts of the statute that narrowly limited judicial review of the gag orders – provisions that required the courts to treat the government's claims about the need for secrecy as conclusive and required the courts to defer entirely to the executive branch.[56] The appeals court then remanded the case back to the lower court and required the government to finally justify the more than four-year long gag on the "John Doe" NSL recipient in the case. In June 2009, the government attempted to satisfy this requirement by filing its justification for the gag entirely in secret documents which not even Doe's lawyers had any access to. The ACLU asked the court to order the government to disclose its secret filings or at least

provide them with an unclassified summary and redacted version of the documents. In August 2009, Judge Marrero ordered the government to partially disclose its secret filing and to release a public summary of its evidence. As a result of a settlement agreement reached in 2010, the ACLU's "John Doe" client, Nicholas Merrill, was finally able to publicly identify himself and his former company as the plaintiffs in the case..

The second case, *Library Connection v. Gonzales*, involved an NSL served on a consortium of libraries in Connecticut.[57] In September 2006, a federal district court ruled that the gag on the librarians violated the First Amendment. The government ultimately withdrew both the gag and its demand for records.

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

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

MATERIAL SUPPORT FOR TERRORISM PROVISIONS

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

The Antiterrorism and Effective Death Penalty Act of 1996 (AEDPA), passed in the wake of the Oklahoma City bombing, criminalized providing material support to

terrorists or terrorist organizations.[63] Title 18 U.S.C. § 2339A makes it a federal crime to knowingly provide material support or resources in preparation for or in carrying out specified crimes of terrorism, and 18 U.S.C. § 2339B outlaws the knowing provision of material support or resources to any group of individuals the secretary of state has designated a foreign terrorist organization (FTO).[64] AEDPA defined "material support or resources" as "currency or other financial securities, financial services, lodging, training, safe-houses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel, transportation, and other physical assets, except medicine or religious materials." AEDPA also amended the Immigration & Nationality Act (INA) to give the secretary of state almost unfettered discretion to designate FTOs.[65]

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

**Section 805** of the Patriot Act expanded the already overbroad definition of "material support and resources" to include "expert advice or assistance," and **section 810** increased penalties for violations of the statute.[66] Through IRTPA, Congress narrowed these provisions in 2004 to require that a person have knowledge that the organization is an FTO, or has engaged or engages in terrorism. However, the statute still does not require the government to prove that the person specifically intended for his or her support to advance the terrorist activities of the designated organization.[67] In fact, the government has argued that those who provide support to designated organizations can run afoul of the law even if they oppose the unlawful activities of the designated group, intend their support to be used only for humanitarian purposes and take precautions to ensure that their support is indeed used for these purposes.[68] This broad interpretation of the material support prohibition effectively prevents humanitarian organizations from providing needed relief in many parts of the world where designated groups control schools, orphanages, medical clinics, hospitals and refugee camps.[69]

In testimony before Congress in 2005, ACLU of Southern California staff attorney Ahilan T. Arulanantham gave a first hand account of the difficulties he experienced while providing humanitarian aid to victims of the 2004 tsunami in Sri Lanka.[70] At the time of the tsunami approximately one-fifth of Sri Lanka was controlled by the Liberation Tigers of Tamil Eelam (LTTE), an armed group fighting against the Sri Lankan government. The U.S. government designated the LTTE as an FTO, but for the 500,000 people living within its territory, the LTTE operates as an authoritarian military government. As a result, providing humanitarian aid to needy people in this part of Sri Lanka almost inevitably requires dealing directly with institutions the LTTE controls.

And because there is no humanitarian exemption from material support laws (only the provision of medicine and religious materials are exempted), aid workers in conflict zones like Sri Lanka are at risk of prosecution by the U.S. government. Arulanantham explained the chilling effect of these laws:

> I have spoken personally with doctors, teachers, and others who want to work with people desperately needing their help in Sri Lanka, but fear liability under the "expert advice," "training," and "personnel" provisions of the law. I also know people who feared to send funds for urgent humanitarian needs, including clothing, tents, and even books, because they thought that doing so might violate the material support laws. I have also consulted with organizations, in my capacity as an ACLU attorney, that seek to send money for humanitarian assistance to areas controlled by designated groups. I have heard those organizations express grave concerns about continuing their work for precisely these reasons. Unfortunately, the fears of these organizations are well-justified. Our Department of Justice has argued that doctors seeking to work in areas under LTTE control are not entitled to an injunction against prosecution under the material support laws, and it has even succeeded in winning deportation orders under the immigration law's definition of material support, for merely giving food and shelter to people who belong to a "terrorist organization" even if that group is not designated.[71]

Tragically, our counterterrorism laws make it more difficult for U.S. charities to operate in parts of the world where their good works could be most effective in winning the battle of hearts and minds. In 2006 Congress passed the Patriot Act reauthorization, making the material support provisions permanent.[72]

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

The material support provisions impermissibly criminalize a broad range of First Amendment-protected activity, both as a result of their sweeping, vague terms and because they do not require the government to show that a defendant *intends* to support the criminal activity of a designated FTO. Courts have held that vague statutes should be invalidated for three reasons: "(1) to avoid punishing people for behavior that they could not have known was illegal; (2) to avoid subjective enforcement of laws…; and (3) to avoid any chilling effect on the exercise of First Amendment freedoms."[73] Material support prohibitions against "training," "services" and "expert advice and assistance" fail each of these three standards.

Any suggestion that the government would not use the material support statutes to prosecute purely First Amendment-protected speech is belied by the fact that it already has. In a most notorious example, the government brought charges against University of Idaho Ph.D. candidate Sami Omar Al-Hussayen, whose volunteer work managing websites for a Muslim charity led to a six-week criminal trial for materially supporting terrorism. The prosecution argued that by running a website that had links to other websites that carried speeches advocating violence, Al Hussayen provided "expert assistance" to terrorists. A jury ultimately acquitted Al-Hussayen of all terrorism-related charges.[74]

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

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

In *Humanitarian Law Project v. Mukasey*, a group of organizations and individuals seeking to support the nonviolent and lawful activities of Kurdish and Tamil humanitarian organizations challenged the constitutionality of the material support provisions on First and Fifth Amendment grounds.[81] They contended that the law violated the Constitution by imposing a criminal penalty for association without requiring

specific intent to further an FTO's unlawful goals, and that the terms included in the definition of "material support or resources" were impermissibly vague. In 2007, the U.S. Court of Appeals for the Ninth Circuit found the terms "training" and "service," and part of the definition of "expert advice and assistance" unconstitutionally vague under the Fifth Amendment.[82] The government appealed this decision and in 2010 the U.S. Supreme Court reversed, upholding the Patriot Act and IRPTA-enhanced material support provisions as constitutional as applied to these plaintiffs.[83]

SUGGESTED REFORM OF MATERIAL SUPPORT STATUTES

- Amend the material support statutes to require specific intent to further an organization's unlawful activities before imposing criminal liability.
- Remove overbroad language, such as "training," "service" and "expert advice and assistance," from the definition of material support.
- Establish an explicit duress exemption to remove obstacles for genuine refugees and asylum-seekers to enter and/or remain in the United States.
- Provide notice, due process and meaningful review requirements in the designation process, and permit defendants charged with material support to challenge the underlying designation in their criminal cases.
- Broaden the humanitarian aid exemption to the material support statute to ensure that charities can provide legitimate humanitarian aid in conflict zones (currently only medicine and religious materials are exempted from the material support prohibition).

IDEOLOGICAL EXCLUSION

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

**Section 411** of the Patriot Act amended the INA to expand the grounds for denying foreign nationals admission into the United States, and for deporting those already here.[84] This section authorizes the exclusion of not only foreign nationals who support domestic or foreign groups the U.S. has designated as "terrorist organizations," but also those who support "a political, social or other similar group whose public endorsement of acts of terrorist activity the secretary of state has determined undermines United States efforts to reduce or eliminate terrorist activities." Moreover, Congress added a provision that authorizes the exclusion of those who have used a "position of prominence within any country to endorse or espouse terrorist activity, or to persuade others to support terrorist activity or a terrorist organization, in a way that the secretary of state has determined undermines United States efforts to reduce or eliminate terrorist activities."[85] Though ostensibly directed at terrorism, the provision focuses on words, not conduct, and its terms are broad and easily manipulated. The State Department's Foreign Affairs Manual takes the sweeping view that the provision applies to foreign nationals who have voiced "irresponsible expressions of opinion." Over the last six years, dozens of foreign scholars, artists and human rights activists have been denied entry to the United States not because of their actions – but because of their political views, their writings and their associations.

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

The ACLU challenged the constitutionality of "ideological exclusion" in *American Academy of Religion v. Napolitano* (previously *American Academy of Religion v. Chertoff*). In July 2004, the Department of Homeland Security (DHS) used the provision to revoke the visa of Tariq Ramadan, a Swiss citizen, one of Europe's leading scholars of Islam and a vocal critic of U.S. policy. Ramadan had accepted a position to teach at the University of Notre Dame. After DHS and the State Department failed to act on a second visa application which would have permitted Ramadan to teach at Notre Dame, he applied for a B Visa to attend and participate in conferences in the U.S. After the government failed to act on *that* application for many months, in January 2006, the American Academy of Religion (AAR), the American Association of University Professors and PEN American Center – organizations that had invited Professor Ramadan to speak in the United States – filed suit. They argued that the government's exclusion of Professor Ramadan, as well as the ideological exclusion provision, violated their First Amendment right to receive information and hear ideas, and compromised their ability to engage in an intellectual exchange with foreign scholars. When challenged in court, the government abandoned its allegation that Professor Ramadan had endorsed terrorism.[86]

The district court held that the government could not exclude Ramadan without providing a legitimate reason and that it could not exclude Ramadan based solely on his speech. It ordered the government to adjudicate Ramadan's pending visa application within 90 days.[87] Thereafter, however, the government found an entirely new basis for barring Ramadan. Invoking the expanded material support provisions of the Real ID Act, the government determined that Professor Ramadan was inadmissible because of small donations he made from 1998 to 2002 to a lawful European charity that provides aid to Palestinians.[88] The plaintiffs continued to challenge the legality of Professor Ramadan's exclusion as well as the constitutionality of the ideological exclusion provision. In July 2007, the district court upheld Professor Ramadan's exclusion but did not rule on the constitutionality of the ideological exclusion provision, finding instead that the plaintiffs lacked standing. The ACLU appealed that decision, and in July of 2009, the U.S. Court of Appeals for the Second Circuit found that the U.S. government had not adequately justified its denial of a visa to Professor Ramadan. The court found that the First Amendment rights of U.S. organizations are at stake when foreign scholars, artists, politicians and others are excluded, and that the organizations have a First Amendment

right to "'hear, speak, and debate with' a visa applicant." The appeals court also found that the government cannot exclude an individual from the U.S. on the basis of "material support" for terrorism without affording him the "opportunity to demonstrate by clear and convincing evidence that he did not know, and reasonably should not have known, that the recipient of his contributions was a terrorist organization." The Second Circuit did not address the constitutionality of the ideological exclusion provision because it agreed with the district court that plaintiffs lacked standing.

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

SUGGESTED REFORM OF IDEOLOGICAL EXCLUSION STATUTES

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

RELAXED FISA STANDARDS

**Section 218** of the Patriot Act amended FISA to eliminate the requirement that the *primary purpose* of a FISA search or surveillance must be to gather foreign intelligence.[89] Under the Patriot Act's amendment, the government needs to show only that a *significant purpose* of the search or surveillance is to gather foreign information in order to obtain authorization from the FISC.[90] This seemingly minor change allows the government to use FISA to circumvent the basic protections of the Fourth Amendment, even where criminal prosecution is the government's primary purpose for conducting the search or surveillance. This amendment allows the government to conduct intrusive investigations to gather evidence for use in criminal trials without establishing probable cause of illegal activity before a neutral and disinterested magistrate, and without providing notice required with ordinary warrants. Instead, the government can obtain authorization for secret searches from a secret and unaccountable court based on an assertion of probable cause that the target is an "agent of a foreign power," a representation the court must accept unless "clearly erroneous." An improperly targeted person has no way of knowing his or her rights have been violated, so the government can never be held accountable.

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

In March 2004, the FBI began to suspect Mayfield of involvement in a series of terrorist bombings in Madrid, Spain, based on an inaccurate fingerprint identification. Although Mayfield had no criminal record and had not left the U.S. in over 10 years, he and his family became subject to months of secret physical searches and electronic surveillance approved by the FISC. In May 2004, Mayfield was arrested and imprisoned for weeks until news reports revealed that the fingerprints had been matched to an Algerian national, Ouhane Daoud. Mayfield was released the following day. In a subsequent lawsuit challenging the Patriot Act amendment to FISA, *Mayfield v. United States*, a federal district court held that the amendment violated the Fourth Amendment by allowing the government to avoid traditional judicial oversight to obtain a surveillance order, retain and use information collected in criminal prosecutions without allowing the targeted individuals a meaningful opportunity to challenge the legality of the surveillance, intercept communications and search a person's home without ever informing the targeted individual and circumvent the Fourth Amendment's particularity requirement.[91] On appeal by the government, the 9th Circuit reversed, holding Mayfield lacked standing because he previously accepted a financial settlement from the FBI.[92]

SUGGESTED REFORM OF FISA STATUTES

- Restore the primary purpose requirement to FISA.

**ONLY ONE PIECE OF THE PUZZLE**

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

Fundamentally, Congress must recognize that overbroad, ineffective or abusive surveillance programs are counterproductive to long-term government interests because they undermine public confidence and support of U.S. anti-terrorism programs. An effort by Congress to account fully for abuses of government surveillance authorities in the recent past is absolutely necessary for several reasons. First, only by holding accountable those who engaged in intentional violations of law can we re-establish the primacy of the law and deter future abuses. Second, only by creating an accurate historical record of the

failure of these abusive programs can government officials learn from these mistakes and properly reform our national security laws and policies. Finally, only by vigorously exercising its oversight responsibility in matters of national security can Congress reassert its critical role as an effective check against abuse of executive authority.

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

**CONCLUSION – IT IS TIME TO AMEND OUR SURVEILLANCE LAWS**

In 2011, Congress must once again revisit the Patriot Act, as three temporary provisions from the 2006 reauthorization are set to expire by the end of the year. This time, however, Congress is not completely in the dark. The IG audits ordered in the Patriot Act reauthorization proved the government lied when it claimed that no Patriot Act powers had been abused. Critics once derided as hysterical librarians were proven prescient in their warnings that these arbitrary and unchecked authorities would be misused. Just like the colonists who fought against writs of assistance, these individuals recognized that true patriotism meant standing up for their rights, even in the face of an oppressive government and an unknowable future. Certainly there are threats to our security, as there always have been, but our nation can and must address those threats without sacrificing our essential values or we will have lost the very freedoms we strive to protect.

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

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

**APPENDIX – THE PATRIOT ACT AT A GLANCE**

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

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

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

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

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

- Section 213: Sneak and Peek Searches. These are delayed notice search warrants. Before the Patriot Act, criminal search warrants required prior notification except in exigent circumstances or for stored communications when notice would "seriously jeopardize an investigation." The Patriot

Act expanded this once narrow loophole – used solely for stored communications – to all searches. Agents might now use this vague catch-all to circumvent longstanding Fourth Amendment protections. These sneak and peek warrants are not limited to terrorism cases – thereby undermining one of the core justifications for the original Patriot Act. In fact, for the 2007 fiscal year, the government reports that out of 690 sneak and peak applications, only seven, or about one percent, were used for terrorism cases.

- Section 214: Pen Register/Trap and Trace Orders Under FISA. Pen register/trap and trace devices pick up communication records in real time and provide the government with a streaming list of phone calls or emails made by a person or account. Before the Patriot Act, this section was limited to tracking the communications of suspected terrorists. Now, it can be used against people who are generally relevant to an investigation, even if they have done nothing wrong.

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

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

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

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

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

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

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

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

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

- Section 6001 of intelligence reform bill: "Lone Wolf" Surveillance and Search Orders. Since its inception, FISA has regulated searches and surveillance on US soil for intelligence purposes. Under FISA, a person would have to belong to a group suspected of terrorism before he or she could be surveilled. The Patriot Act added a new category, allowing

someone wholly unaffiliated with a terrorist organization to be targeted for surveillance. This section is scheduled to expire on December 31, 2009.

---

[1] The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (PATRIOT Act) of 2001, Pub. L. No. 107-56, 115 Stat. 272.
[2] Letter from Ronald Weich, Assistant Attorney General, U.S. Department of Justice, to Senator Patrick Leahy, Chairman, Committee on the Judiciary, (Sept. 14, 2009), *available at* http://judiciary.senate.gov/resources/documents/111thCongress/upload/091409WeichToLeahy.pdf.
[3] *Boyd v. United States*, 116 U.S. 616, 624 (1886).
[4] Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 556 (1999).
[5] *See Boyd*, 116 U.S. 616.
[6] *Id.* at 625.
[7] *Id.*
[8] John Yoo and Eric Posner, *Patriot Act Under Fire*, AMERICAN ENTERPRISE INSTITUTE ONLINE, Dec. 1, 2003, *available at* http://www.aei.org/publications/pubID.19661.filter./pub_detail.asp.
[9] *Marcus v. Search Warrant*, 367 U.S. 717, 729 (1961).
[10] *Marron v. United States*, 275 U.S. 192, 196 (1927).
[11] *Stanford v. Texas*, 379 U.S. 476, 485 (1965).
[12] *United States v. United States District Court (Keith)*, 407 U.S. 297, 313 (1972).
[13] S. REP. NO. 107-351 (Dec. 2002); H.R. REP. NO. 107-792 (Dec. 2002).
[14] Letter from the American Civil Liberties Union to the U.S. House of Representatives (Oct. 23, 2001) (on file with author), *available at* http://www.aclu.org/natsec/emergpowers/14402leg20011023.html; Letter from the American Civil Liberties Union to the U.S. Senate (Oct. 23, 2001) (on file with author), *available at* http://www.aclu.org/natsec/emergpowers/14401leg20011023.html.
[15] Letter from the American Civil Liberties Union to Senator Dianne Feinstein (April 4, 2005) (on file with author), *available at* http://www.aclu.org/safefree/general/17563leg20050404.html.
[16] *USA PATRIOT Act of 2001: Hearing Before the S. Select Comm. on Intelligence*, 109th Cong. 97, 100 (2005) (statement of Alberto R. Gonzales, Att'y Gen. of the United States and Robert S. Mueller, III, Director, Federal Bureau of Investigation). A later report by the Department of Justice Inspector General would reveal that between 2003 and 2005 the FBI had self-reported 19 possible legal violations regarding its use of National Security Letters to the President's Intelligence Oversight Board. Attorney General Gonzales received at least six reports detailing FBI intelligence violations, including misuse of NSLs, three months prior to his Senate testimony. To a certain degree AG Gonzales and FBI Director Mueller were truthful in their testimony because as they well knew, President Bush's Intelligence Oversight Board did not meet to "substantiate" any of the violations reported until the Spring of 2007. *See* DEP'T. OF JUSTICE, OFFICE OF INSPECTOR GENERAL, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF NATIONAL SECURITY LETTERS 69 (Mar. 2007), *available at* http://www.usdoj.gov/oig/special/s0703b/final.pdf; John Solomon, *Gonzales was told of FBI violations*, WASH. POST, Jul. 10, 2007, at A1, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2007/07/09/AR2007070902065.html; John Solomon, *In Intelligence World, a Mute Watchdog*, WASH. POST, Jul. 15, 2007, at A3, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2007/07/14/AR2007071400862.html.
[17] USA PATRIOT Improvement and Reauthorization Act of 2005 (PIRA), Pub. L. No. 109-177, § 119(a), 120 Stat. 192 (2006).
[18] Pub. L. No. 108-458, 118 Stat. 3638 (2004).
[19] 18 U.S.C. § 2518(11), (12).
[20] *Oversight of the Federal Bureau of Investigation: Hearing Before the S. Comm. on the Judiciary*, 111th Cong. (2009) (Testimony of Robert S. Mueller, III, Director, Federal Bureau of Investigation).
[21] Electronic surveillance orders in criminal investigations are governed by the Omnibus Crime Control and Safe Streets Act of 1968. *See* 18 U.S.C. §§ 2510-2520 (2006).
[22] PIRA § 119(a).

[23] The four NSL authorizing statutes include the Electronic Communications Privacy Act, 18 U.S.C. § 2709 (2000), the Right to Financial Privacy Act, 12 U.S.C. § 3401 (2000), the Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq. (2000), and the National Security Act of 1947, 50 U.S.C. § 436(a)(1)(2000).
[24] As amended, the NSL statute authorizes the Director of the FBI or his designee (including a Special Agent in Charge of a Bureau field office) to impose a gag order on any person or entity served with an NSL. *See* 18 U.S.C. § 2709(c). To impose such an order, the Director or his designee must "certify" that, absent the non-disclosure obligation, "there may result a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person." *Id.* at § 2709(c)(1). If the Director of the FBI or his designee so certifies, the recipient of the NSL is prohibited from "disclos[ing] to any person (other than those to whom such disclosure is necessary to comply with the request or an attorney to obtain legal advice or legal assistance with respect to the request) that the [FBI] has sought or obtained access to information or records under [the NSL statute]." *Id.* Gag orders imposed under the NSL statute are imposed by the FBI unilaterally, without prior judicial review. While the statute requires a "certification" that the gag is necessary, the certification is not examined by anyone outside the executive branch. The gag provisions permit the recipient of an NSL to petition a court "for an order modifying or setting aside a nondisclosure requirement." *Id.* at § 3511(b)(1). However, in the case of a petition filed "within one year of the request for records," the reviewing court may modify or set aside the nondisclosure requirement only if it finds that there is "no reason to believe that disclosure may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person." *Id.* at § 3511(b)(2). Moreover, if a designated senior government official "certifies that disclosure may endanger the national security of the United States or interfere with diplomatic relations," the certification must be "treated as conclusive unless the court finds that the certification was made in bad faith." *Id.*
[25] DEP'T OF JUSTICE, OFFICE OF INSPECTOR GENERAL, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF NATIONAL SECURITY LETTERS (Mar. 2007), *available at* http://www.usdoj.gov/oig/special/s0703b/final.pdf [hereinafter 2007 NSL Report]; DEP'T OF JUSTICE, OFFICE OF INSPECTOR GENERAL, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF SECTION 215 ORDERS FOR BUSINESS RECORDS (Mar. 2007), *available at* http://www.usdoj.gov/oig/special/s0703a/final.pdf [hereinafter 2007 Section 215 Report].
[26] 2007 NSL Report, *supra* note 25, at 84.
[27] *Id.*at 86-99.
[28] DEP'T OF JUSTICE, OFFICE OF INSPECTOR GENERAL, A REVIEW OF THE FBI'S USE OF NATIONAL SECURITY LETTERS: ASSESSMENT OF CORRECTIVE ACTIONS AND EXAMINATION OF NSL USAGE IN 2006 (Mar. 2008), *available at* http://www.usdoj.gov/oig/special/s0803b/final.pdf [hereinafter 2008 NSL Report]; DEP'T OF JUSTICE, OFFICE OF INSPECTOR GENERAL, A REVIEW OF THE FBI'S USE OF SECTION 215 ORDERS FOR BUSINESS RECORDS IN 2006 (Mar. 2008), *available at* http://www.usdoj.gov/oig/special/s0803a/final.pdf [hereinafter 2008 Section 215 Report].
[29] 2008 NSL Report, *supra* note 28, at 9.
[30] *Id.* at 127, 129 n.116.
[31] *Id.*at 127.
[32] *Id.*
[33] *Id.*at 130.
[34] *See Doe v. Ashcroft*, 334 F. Supp. 2d 471 (S.D.N.Y 2004); *Doe v. Gonzales*, 500 F.Supp. 2d 379 (S.D.N.Y. 2007); *Doe v. Gonzales*, 386 F. Supp. 2d 66 (D.Conn. 2005); PIRA, Pub. L. No. 109-177, 120 Stat. 195 (2006); USA Patriot Act Additional Reauthorizing Amendments Act of 2006 (ARAA) Pub. L. No.109-178, 120 Stat. 278 (2006). The ACLU is still litigating the constitutionality of the gag order provisions in the USA PATRIOT Improvement and Reauthorization Act of 2005. *See* Press Release, American Civil Liberties Union, ACLU Asks Appeals Court to Affirm Striking Down Patriot Act 'National Security Letter' Provision (Mar. 14, 2008) (on file with author), *available at* http://www.aclu.org/safefree/nationalsecurityletters/34480prs20080314.html.
[35] 2008 NSL Report, *supra* note 28, at 11, 124.
[36] *Id.*at 127.
[37] *Id.*at 81, 88.

[38] Letter from Ronald Weich, Assistant Attorney General, United States Department of Justice, to Harry Reid, Majority Leader, United States Senate (May 14, 2009) (on file with author), *available at* http://www.fas.org/irp/agency/doj/fisa/2008rept.pdf.
[39] 2008 Section 215 Report, *supra* note 28, at 68.
[40] *Id.* at 72.
[41] *Id.* at 73.
[42] *Id.* at 67.
[43] *Id.* at 72.
[44] *Id.*
[45] *Id.* at 71 n.63.
[46] *Id.* at 73.
[47] *Id.* at 72-73.
[48] Letter from Ronald Weich, Assistant Attorney General, U.S. Department of Justice, to Senator Patrick Leahy, Chairman, Committee on the Judiciary, *supra* note 2.
[49] 2008 Section 215 Report, *supra* note 28, at 43.
[50] *Id.* at 45-47.
[51] *Id.* at 47.
[52] *See, Foreign Intelligence Surveillance Act: Closed Hearing Before the H. Permanent Select Comm. on Intelligence,* 110th Cong. (Sept. 6, 2007) (Statement of Kenneth Wainstein, Assistant Att'y Gen., National Security Division, U.S. Dep't of Justice), *available at* http://www.fas.org/irp/congress/2007_hr/090607wainstein.pdf.
[53] *See Doe v. Ashcroft*, 334 F. Supp. 2d 471 (S.D.N.Y 2004); *Doe v. Gonzales*, 500 F. Supp. 2d 379 (S.D.N.Y. 2007); *Doe v. Gonzales*, 386 F. Supp. 2d 66 (D.Conn. 2005). The ACLU is still litigating the constitutionality of the gag order provisions in the USA PATRIOT Improvement and Reauthorization Act of 2005. *See*, Press Release, American Civil Liberties Union, ACLU Asks Appeals Court to Affirm Striking Down Patriot Act 'National Security Letter' Provision (Mar. 14, 2008) (on file with author), *available at* http://www.aclu.org/safefree/nationalsecurityletters/34480prs20080314.html.
[54] PIRA.
[55] *Doe v. Gonzales*, 500 F. Supp. 2d 379, 25 A.L.R. Fed. 2d 775 (S.D.N.Y. 2007).
[56] *Doe v. Mukasey,* No. 07-4943-cv (2nd Cir. Dec. 15, 2008), *available at* http://www.aclu.org/pdfs/safefree/doeymukasey_decision.pdf.
[57] *Library Connection v. Gonzales,* 386 F. Supp. 2d 66, 75 (D. Conn. 2005).
[58] *See* Joint Administrative Motion to Unseal Case, Internet Archive v. Mukasey, No. 07-6346-CW (N.D. Cal. May 1, 2008), *available at* https://www.aclu.org/pdfs/safefree/internetarchive_motiontounseal_20080501.pdf.
[59] *Id.* at 3.
[60] National Security Act of 1947, 50 U.S.C. § 436.
[61] Right to Financial Privacy Act, 12 U.S.C. § 4314.
[62] Fair Credit Reporting Act, 15 U.S.C. § 1681v.
[63] Pub. L. No. 104-132, 110 Stat. 1214 (1996).
[64] § 2339A. Providing material support to terrorists

> (a) Offense. – Whoever provides material support or resources or conceals or disguises the nature, location, source, or ownership of material support or resources, knowing or intending that they are to be used in preparation for, or in carrying out, a violation of section 32, 37, 81, 175, 229, 351, 831, 842(m) or (n), 844(f) or (i), 930(c), 956, 1114, 1116, 1203, 1361, 1362, 1363, 1366, 1751, 1992, 1993, 2155, 2156, 2280, 2281, 2332, 2332a, 2332b, 2332f, or 2340A of this title, section 236 of the Atomic Energy Act of 1954 (42 U.S.C. 2284), or section 46502 or 60123(b) of title 49, or in preparation for, or in carrying out, the concealment of an escape from the commission of any such violation, or attempts or conspires to do such an act, shall be fined under this title, imprisoned not more than 15 years, or both, and, if the death of any person results, shall be imprisoned for any term of years or for life.
>
> (b) Definition. – In this section, the term "material support or resources" means currency or monetary instruments or financial securities, financial services, lodging, training, expert advice or assistance, safehouses, false documentation or identification, communications equipment,

facilities, weapons, lethal substances, explosives, personnel, transportation, and other physical assets, except medicine or religious materials.

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

(a) Prohibited activities. –

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

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

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

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

[65] 66 Stat. 163, § 219, as amended, 8 U.S.C. §§ 1101 et seq. As noted, 18 U.S.C. §§ 2339A and 2339B are not the only statutes pertaining to material support. In addition, the criminal liability provisions of the International Emergency Economic Powers Act (IEEPA), permit the designation of "specially designated terrorists" and "specially designated global terrorists" and give the President authority to regulate, prohibit or prevent any form of economic transaction that provides services to benefit terrorists. 50 U.S.C. § 1705 (2007).

[66] PATRIOT Act, Pub. L. No. 107-56, § 805(a)(2), 115 Stat. 272 (2001). ; 18 U.S.C. §§ 2339A(b) and 2339B(g)(4).

[67] IRTPA, Pub. L. No. 108-458, 118 Stat. 3638 (2004).

[68] *See Humanitarian Law Project v. Gonzales*, 380 F. Supp. 2d, 1134, 1142-48, (C.D. Cal. 2005).

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

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

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

[72] PIRA § 104.

[73] *Foti v. City of Menlo Park*, 146 F.3d 629, 638 (9th Cir. 1998).

[74] Maureen O'Hagan, *A Terrorism Case that went Awry*, SEATTLE TIMES, Nov. 22, 2004, *available at* http://seattletimes.nwsource.com/html/localnews/2002097570_sami22m.html.

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

[76] *United States v. Al-Arian*, 308 F. Supp. 2d 1322, 1337 (M.D. Fla. 2004).

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

[78] BUREAU OF JUSTICE STATISTICS, U.S. DEP'T OF JUSTICE, COMPENDIUM OF FEDERAL JUSTICE STATISTICS, 2001 (2003), BUREAU OF JUSTICE STATISTICS, U.S. DEP'T OF JUSTICE, COMPENDIUM OF FEDERAL JUSTICE STATISTICS, 2002 (2004), BUREAU OF JUSTICE STATISTICS, U.S. DEP'T OF JUSTICE, COMPENDIUM OF FEDERAL JUSTICE STATISTICS, 2003 (2005), BUREAU OF JUSTICE STATISTICS, U.S. DEP'T OF JUSTICE, COMPENDIUM OF FEDERAL JUSTICE STATISTICS, 2004 (2006), *available* http://www.ojp.usdoj.gov/bjs/pubalp2.htm#cfjs (follow the hyperlink of the same title to access each year's compendium).

[79] Chesney, *supra* note 77, at 885.

[80] *Id.* at 886.
[81] The ACLU filed an *amicus curiae* brief on behalf of Plaintiffs. *See* Brief for American Civil Liberties Union as Amicus Curiae Supporting Plaintiffs-Appellees, Humanitarian Law Project v. Gonzales, No. 05-56753, 05-56846 (9th Cir. filed May 19, 2006), *available at* http://www.aclu.org/images/general/asset_upload_file394_25628.pdf.
[82] *Humanitarian Law Project v. Mukasey*, 509 F.3d 1122 (9th Cir. 2007).
[83] *Holder v. Humanitarian Law Project,* 561 U.S. ___ (2010).
[84] 8 U.S.C. § 1182(a)(3)(B)(i)(VI).
[85] *Id.*
[86] *American Academy of Religion v. Chertoff,* No. 06 CV 588 (PAC), 2007 WL 4527504 (S.D.N.Y.).
[87] *See American Academy of Religion v. Chertoff,* 463 F.Supp.2d 400 (S.D.N.Y. 2006); *American Academy of Religion v. Chertoff,* No. 06 CV 588 (PAC), 2007 WL 4527504 (S.D.N.Y.).
[88] *See* Rearing and Empowering America for Longevity against acts of International Destruction Act of 2005 (REAL ID), Pub. L. No. 109-13, Div. B, 119 Stat. 231.
[89] PATRIOT Act, Pub. L. No. 107-56, § 218, 115 Stat. 272 (2001)..
[90] *Id.*.
[91] *Mayfield v. United States*, 504 F. Supp. 2d 1023 (D. Or. 2007). The ACLU filed an *amicus curiae* brief on behalf of Plaintiffs. *See* brief for American Civil Liberties Union as Amicus Curiae Supporting Plaintiffs, Mayfield v. United States, No. 07-35865 (9th Cir. filed March 14, 2008), *available at* http://www.aclu.org/images/asset_upload_file16_34495.pdf.
[92] *Mayfield v. U.S.*, 599 F.3d 964 (9th Cir. 2010)

Mr. SENSENBRENNER. Thank you very much.

We now get to questions. I am going to call on people alternatively by side in the approximate order in which they appeared, and the Chair is going to defer his questions until the end. So the gentleman from Virginia, Mr. Scott, is recognized for 5 minutes.

Mr. SCOTT. Thank you.

Mr. Hinnen, you mentioned the importance of National Security Letters because of national security. Can they be used for things—one of the things that has occurred to me is sometimes we get into a discussion where you have a process that works for mass murderers, weapons of mass destruction, and shoplifting. What else can you use the National Security Letters for other than national security terrorism-related investigations?

Mr. HINNEN. Mr. Ranking Member, National Security Letters can only be used in a predicated national security investigation, and they can only be used to collect information that is relevant to an authorized investigation that is investigating international terrorism or counterintelligence activities. They could not be used for ordinary crimes such as shoplifting.

Mr. SCOTT. Why are the NSL processes inappropriate for criminal investigations?

Mr. HINNEN. I think that, as I mentioned in my opening statement, part of what the PATRIOT Act did is bring the NSL requirements closer to criminal investigative statutes, and I think the one large remaining difference is the secrecy that NSL's provide in investigating national security crimes, the kind of secrecy that is necessary when the evidence that the Government relies upon to make its showing is classified and where it needs to protect classified sources and methods in an ongoing national security investigation. So I think it is the extra secrecy that is so uniquely suited to national security investigations.

Mr. SCOTT. Why is that inappropriate for a criminal investigation?

Mr. HINNEN. Well, Congressman, I think there are a number of statutes that authorize delayed notice in criminal investigations where it is deemed appropriate by the court. I think the determination that Congress made is that national security investigations are a type of investigation in which that kind of secrecy is almost always authorized. And so it simply switched the default. The Government still has to certify that nondisclosure is important, but the default is, in that sense, in favor of nondisclosure.

Mr. SCOTT. If it is a case where the primary purpose is a criminal investigation but a significant purpose may be national security, you get the more streamlined approach without the protections. Is that right?

Mr. HINNEN. Well, under FISA and under the change made to the FISA standard, the Government now can demonstrate that a significant purpose is foreign intelligence collection rather than the primary purpose, I think reflecting what the courts had found before the amendment——

Mr. SCOTT. If you are using the national security purpose, what could be the primary purpose if it is not national security? When Attorney General Gonzales was asked that question, he said you could be running a criminal investigation.

Mr. HINNEN. Well, Congressman, I think the courts did recognize that there is no mutual exclusivity between collecting foreign intelligence and prosecuting national security crimes. It just stands to reason that if one is collecting foreign intelligence on a foreign spy, that one may ultimately prosecute him under criminal provisions that are intended to outlaw spying.

Mr. SCOTT. NSL's have gag orders. How would a target find out that he was the subject to an abusive NSL search?

Mr. HINNEN. The way the mechanism works in NSL's is the recipient of the NSL, the third party that holds the records, is required to assert any problem that that individual sees with the NSL.

Mr. SCOTT. And why would someone who has no interest in revealing someone's private information have an incentive to hire lawyers to protect somebody else's rights?

Mr. HINNEN. Well, I think the recipients often do have an interest in protecting the privacy of their customers or subscribers. For instance, telecommunication providers and Internet service provides take the privacy of their customers and subscribers very seriously and I think are often an effective proxy for defending those rights.

Mr. SCOTT. Mr. German, what is wrong with that?

Mr. GERMAN. Well, the evidence shows that in the case of the exigent letters that the telecommunications companies were not looking out for the privacy of their customers and instead were engaged with FBI agents in circumventing the law by allowing information about their customers to pass over to the FBI with post-it notes and other informal mechanisms.

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

The gentleman from South Carolina, Mr. Gowdy, is recognized for 5 minutes.

Mr. GOWDY. Thank you, Mr. Chairman.

Mr. German, I noted in your written testimony there are many unfortunate examples that the Government abused these authorities in ways that both violate the rights of innocent people and squander precious national security resources. Can you cite me to courts of record, courts of appeals preferably, where panels have held that agents have intentionally violated constitutional rights?

Mr. GERMAN. When you say courts of appeals, you know, there were a number of cases, including the NSL gag order which was found to be unconstitutional.

Mr. GOWDY. No, no, no. You talked about abuses by bureau agents or others. I want to know if there are reported cases by courts of appeals where there have been findings by a district court judge, upheld by a court of appeals, of intentional abuses by bureau agents.

Mr. GERMAN. There is ample evidence in the record. The Inspector General reports had——

Mr. GOWDY. Mr. German, I did not——

Mr. GERMAN [continuing]. You are limiting it——

Mr. GOWDY [continuing]. I did not ask about Inspector Generals. I asked about courts of record, courts of appeals. I will settle for district court judges. Can you name me a district court judge that has found a bureau agent intentionally abusive?

Mr. GERMAN. Certainly in the Brandon Mayfield case, there were courts that determined that it was unconstitutional the way they used FISA's significant purpose test instead of the criminal Title III authority. So, yes, there are cases.

Mr. GOWDY. Well, you cited one.

Mr. GERMAN. I can go through. *Doe v. Holder* is the NSL gag order. Library——

Mr. GOWDY. Are they in higher percentages than bureau agents who are acting outside of PATRIOT Act who are just, in your judgment, violating other constitutional provisions?

Mr. GERMAN. I don't know that there has been an examination to determine that, and I think that is something important to find out whether these authorities are abused more often than other authorities and what would cause that.

Mr. GOWDY. But so far, there is no evidence to support that.

Mr. GERMAN. Well, that is part of our concern. Most of these authorities are exercised under such secrecy that it is really very difficult for us to know what is happening, and that is why it takes an Inspector General report to reveal these abuses.

You know, out of well over 200,000 National Security Letters that went out from the FBI, there were only a handful of third party holders of information that actually challenged——

Mr. GOWDY. What can the bureau get from an NSL that an AUSA can't get from the grand jury subpoena?

Mr. GERMAN. But there are checks with the grand jury——

Mr. GOWDY. What? What? I was one. What check was there?

Mr. GERMAN. Number one, you, the U.S. attorney.

Mr. GOWDY. So you trust Federal prosecutors more than you do bureau agents.

Mr. GERMAN. Certainly having an independent prosecutor determine whether that request for information was appropriate and the grand jury authorizes——

Mr. GOWDY. So if an NSL had to go through a Federal prosecutor, you would support it.

Mr. GERMAN. We support a number of reforms short of——

Mr. GOWDY. Would you support the permanency of NSL's in their current form if a Federal prosecutor had to review it before a bureau agent issued the letter?

Mr. GERMAN. That would certainly be an important reform. I haven't seen that proposal on the table, so we haven't evaluated how that would be. We think narrowing——

Mr. GOWDY. You can propose it today.

Mr. GERMAN. Well, I wish I had that authority at the ACLU.

Mr. GOWDY. Me too.

Mr. GERMAN. But we would support narrowing the scope of the NSL's in the way that it has been proposed in the Justice Act and in Chairman Conyers' bill—or I am sorry—Ranking Member Conyers' bill.

Mr. GOWDY. All right. You also said the PATRIOT Act vastly and unconstitutionally expanded the Government's authority to pry into people's private lives with little or no evidence of wrongdoing.

Mr. GERMAN. Right.

Mr. GOWDY. I have never seen wrongdoing as the standard by which an investigation is started. You have got articulable sus-

picion. You got probable cause. You got a hunch. What evidentiary standard do you think the bureau should have to reach before they can start investigating someone when the crime has not been committed yet.

Mr. GERMAN. I think they need articulable suspicion in the FISA context, which most of the PATRIOT Act refers to, that somebody is an agent of a foreign power, which was the original NSL authority, in order for them to use this tool. The use of this tool against people who are not even suspected—I mean, one of the interesting things as a former FBI agent that I found interesting about the IG report on NSL's was that they were being used on people two and three times removed from the subject of the investigation and were being used——

Mr. GOWDY. My time is almost up. I don't have enough time to ask Mr. Hinnen what punishments were meted out for bureau agents that intentionally violated bureau guidelines or the law. I would be very interested in knowing that. I share your concern for that.

I have run out of time.

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

The gentleman from Michigan, Mr. Conyers, is recognized for 5 minutes.

Mr. CONYERS. Thank you very much.

Mike German, can you tell us what seems to be in dispute and maybe not in agreement with the two other witnesses here on the panel with you? In other words, did you hear anything that you would like us to know about that we should be checking up on?

Mr. GERMAN. I think there was the discussion of the finite resources that the Government has and how we want those focused on real threats. I think that is an important part of this discussion, and that is what some of your review of this should be. If what these powers are being used for is to collect information about innocent people that is then retained and clogs these important databases with innocuous or irrelevant information, that is a problem. I agree that information sharing is a very important goal, but if the information we are sharing is irrelevant or erroneous, that doesn't help national security.

By protecting the privacy of innocent people, you are actually making the Government more effective in focusing on people who are real threats to the community, and certainly the excessive secrecy not only harms our ability to protect civil rights but actually harms the Government. And we have seen that with Senator Lieberman and Collins' Fort Hood report where there is still the problem of excessively classified information that even agents doing investigations don't have access to certain databases.

Mr. CONYERS. Well, we know about the wars between the agencies in which—well, isn't that how we got into 9/11? One agency was keeping information from another and a third agency was keeping information from the other two.

What else? I mean, can't we all get along here? I mean, if you only had one thing that you are in disagreement with—what else did they say that you didn't agree with, Mr. German?

Mr. GERMAN. Well, I would disagree that the internal mechanisms that the FBI created and the Department of Justice created

to address the National Security Letter abuse are sufficient. I think those are insufficient. I think the Inspector General's 2008 report indicated there were problems with fulfilling the recommendations that he suggested. I think his 2010 report on exigent letters was even more troubling where the FBI has created a novel approach or legal opinion about what transactional information they can collect from telephone company providers, and that was supported by the Department of Justice, and the Inspector General asked Congress to review that. So I think there are outstanding issues about those abuses that need to be addressed.

Mr. CONYERS. I will give you one more observation, if you want it.

Mr. GERMAN. I have highlighted in my oral statement the material support provision. I mean, clearly Congress did not pass the material support provision and amend it under the PATRIOT Act to impair legitimate humanitarian aid to crisis and conflict areas, but that is having that effect and I would hope that the Congress would address that and make sure that people providing legitimate humanitarian aid aren't impeded by a possibly overbroad law.

Mr. CONYERS. All right. Mr. Hinnen, you can stop shaking your head now. I will recognize you.

Mr. HINNEN. Thank you, Mr. Ranking Member. I think there are a number of things that we agree upon. Even many of the things that Mr. German was asserting that we disagree upon in his response I think we agree upon.

The Government would wholeheartedly agree that it is not in our interest to collect information that is irrelevant to national security. I think the fact that the standard for national security is that we demonstrate that it is relevant to national security addresses that issue.

The Government also agrees that excessive secrecy is not necessary, and the showings that the Government is required to make in order to keep many of these processes secret are, I think, appropriate to make sure that happens.

And finally, I would just say that the Government appreciates and agrees with the sentiment that it is important to protect privacy and civil liberties and that in doing that, we often make Government more efficient. So I think there is a great deal that we agree on.

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

The gentleman from Virginia, Mr. Goodlatte, is recognized for 5 minutes.

Mr. GOODLATTE. Thank you, Mr. Chairman. I appreciate your holding this hearing, and I appreciate the participation of all these witnesses.

I would like to direct my first question to Mr. Hinnen, and it is a follow-up, sort of, to the discussion we have just had with Mr. German about the NSL's. Can you explain the automated system that is used to process NSL's and does this system increase or decrease the time to process an NSL and does it minimize errors?

Mr. HINNEN. Yes, Congressman, I can do that. The system that was imposed is a centralized computer system that requires agents to walk through the NSL process step by step. It populates the document with appropriate legal language. It then requires that the

document go to an FBI lawyer for legal review before it is then passed on to a high-level signatory special agent in charge for approval prior to issuance.

That process does not significantly increase the time that is required to issue an NSL, and the limited increase in time I think is appropriate to ensure that some of the concerns that the IG rightly pointed out in his 2007 report are addressed. And it has had an effect of limiting and minimizing errors.

Mr. GOODLATTE. And are there some proposed enhancements to the system that would track voluntary disclosures under title 18-2702, and does this system assist the FBI with their congressional reporting requirements in the law?

Mr. HINNEN. My understanding is that the FBI is, in fact, developing a similar system that would facilitate the issuance of 2702 requests, requests for customer and subscriber information, when the provider has a good faith belief that there is an emergency involving risk of death or serious bodily injury. Because the subsystem centralizes data with respect to NSL requests, yes, it does address many of the issues and facilitate the collecting of information to allow us to meet our congressional reporting requirements.

Mr. GOODLATTE. Thank you.

Mr. Wainstein, do you support reducing the time frame for delayed notice from 30 to 7 days, and will this afford any benefit to the target of an investigation?

Mr. WAINSTEIN. I don't support that, Congressman. I think just to step back for a second and look at this in an historical context, delayed search warrant notification has been around for a long time, as the Chairman mentioned. It was authorized by courts of appeals and the Supreme Court. And it has been used in the criminal context for years in drug cases and the like. And it was codified in the PATRIOT Act and has been used very effectively in both criminal and national security cases.

Mr. GOODLATTE. So it is not just used in intelligence gathering.

Mr. WAINSTEIN. No. It actually has been used primarily in criminal cases. It has been tremendously effective, especially in drug cases where you know there is a stash of drugs but you want to leave it there until you find out who the bad guys are who actually you can associate with those drugs.

Mr. GOODLATTE. Mr. Gowdy challenged Mr. German's comment about the PATRIOT Act vastly and unconstitutionally expanding the Government's authority to pry into people's private lives with little or no evidence of wrongdoing. I am quoting Mr. German there. Do you agree with his statement?

Mr. WAINSTEIN. I would put it a little differently. I would say that the PATRIOT Act authorized tools to be used in an earlier stage in the investigation such as 215 orders and National Security Letters. It allows investigators to find out about individuals before they have probable cause or proof beyond a reasonable doubt that those individuals are involved in terrorism. The importance of that is it is often too late once you get to the point of having probable cause or proof beyond a reasonable doubt. You need to find out early on if a particular suspect is a bad guy, then find out if that person is associated with a plot, unwind the plot and neutralize it.

Mr. GOODLATTE. I take it from your comment that you don't believe it was done unconstitutionally.

Mr. WAINSTEIN. No. I think it was done for the very practical reason that we needed to prevent the next 9/11 attack.

Mr. GOODLATTE. And do you think it was constitutional?

Mr. WAINSTEIN. Yes.

Mr. GOODLATTE. And he also claims that those provisions have few, if any, built-in protections and little opportunity for Congress to review. Do you agree with that?

Mr. WAINSTEIN. No. I mean, there are a number of protections. We have talked about them here today. A number of them were added as safeguards in 2005 after Congress did a very careful scrub of all the authorities. And as you know, there are very comprehensive reporting requirements to Congress so that Congress can exercise as much oversight as it wishes as to the use of NSL's by the FBI.

Mr. GOODLATTE. Mr. German, National Security Letters are similar to administrative subpoenas which almost universally require only a showing of relevance to the particular investigation. There are hundreds of instances of administrative subpoenas currently in law. For example, the recent health care law authorized administrative subpoenas.

Do you oppose administrative subpoenas, and if so, why? If not, why should the Government be able to investigate health care matters by subpoena but not international terrorists and foreign powers that wish to do us harm?

Mr. SENSENBRENNER. The gentleman's time has expired but the witness may answer the question.

Mr. GERMAN. Yes, we oppose the expansion of any administrative subpoena authority. The IG report on exigent letters indicated that there was—National Security Letters and section 215 authorities. It actually pointed out that there was some abuse of administrative subpoenas in the audit that he was conducting. So we are concerned about any unchecked use of authority——

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

Mr. GOODLATTE. Thank you, Mr. Chairman.

Mr. SENSENBRENNER. The gentlewoman from Texas, Ms. Jackson Lee, is recognized for 5 minutes.

Ms. JACKSON LEE. I thank the Chairman very much, and I appreciate the comments and associate myself with the comments of the Ranking Member of the full Committee, Mr. Conyers, that we reflect on 9/11. We know that a large part of our problem was the lack of communication, the sort of silo-type security measures that were occurring. For that reason, I am glad we have gotten better, and I want to thank the Department of Justice and many of our security agencies for finding ways of cooperating. I sit on the Homeland Security Committee and intelligence gathering is enormously important for the work that we do.

But let me just cite as an example—lay a premise on something that is not related but gets the crux of some of the concerns. The IRS is busy and in many instances it gets its hands around individuals who are well intentioned, want to pay their taxes. They wait too long and, as you well know, it kicks into the Department of Justice. These are Americans who have committed no real crime

other than they have delayed and thought they had paid or argued that they had paid or were trying to pay. But certainly as the Department of Justice gets it, they really want to pay.

But the interesting thing is that as they want to pay, the harder it gets to pay because the Department of Justice will not allow discussion, will not allow, if you will, the release of information, will not allow that taxpayer just to write a check. It gets into the claws of the system and there is no engagement. There is no constituency engagement. It is secret. You are subject to criminal penalties yourself if you were to engage trying to help a taxpayer who wants to write a check.

Sometimes secrecy is, if you will, the undermining of getting something done, either saving a Nation or getting tax dollars back to the Nation as needed.

So I ask this question about the national security investigation that requires a certain amount of secrecy, Mr. Hinnen, often a very significant amount. But I worry that once you start down the path of secrecy, it simply becomes a default position and more and more information is kept secret that doesn't really need such tight control.

What steps have you or other leaders at the DOJ taken to ensure that information is not overclassified and that information that can safely be made public is released, somewhat similar to why can't people settle their IRS once it gets to the DOJ? Do you think there is more that could be done? And what is the purpose of the FBI's NSL subsystem?

Mr. HINNEN. Thank you, Congresswoman. I will try and address those questions in order.

I would also note that my mind turns naturally to the IRS this time of year too, and I will communicate your concerns back to my colleagues in the Tax Division.

Ms. JACKSON LEE. I appreciate it very much.

Mr. HINNEN. With respect to secrecy and the effect that secrecy has on our investigations, I think some of the information sharing mechanisms you referred to in your comments within the Government ensure that information is shared adequately, that we are able to use it to effectively protect national security. I think beginning with the PATRIOT Act, removing the wall, we have made great steps to make sure that that information is shared.

I understand part of your question also to be about transparency and sharing of information with the American public. I think we——

Ms. JACKSON LEE. And the NSL subsystem.

Mr. HINNEN. Subsystem, yes.

We are also involved in a review of much of the information that relates to these authorities. We have worked with Senator Wyden on the other side of the Hill to ensure that we have a review process for FISA opinions and orders to determine whether any of that information can be declassified so that it can be shared with the public. And so I think we are making steps in that regard as well.

With respect to the NSL subsystem, it is an effort to both ensure that every step that we deem necessary in order to issue an NSL consistent with law, policy, and practice of the FBI is taken and to ensure that that happens efficiently.

Ms. JACKSON LEE. Let me get Mr. German. Thank you very much.

Mr. German, what is your concern about an NSL subsystem, and can an FBI agent abuse the National Security Letters, say, to spy on their wife? And if you could quickly talk about the gag orders, nondisclosure orders.

Mr. GERMAN. Certainly. We are concerned. The system again is simply internal checks. They don't have an outside, independent party checking, and that creates concerns about oversight and particularly the use of FBI lawyers. I mean, the IG reports are very clear that FBI lawyers were intimately involved in the misuse of NSL's and the Section 215 authority. So it is very clear that FBI lawyers aren't necessarily the best check on potential abuse within the FBI. The FBI lawyers were intimately involved in the exigent letters. So that is a concern for us.

With the gag orders, obviously, the ACLU has successfully sued to find the gag orders unconstitutional, and those reforms, reportedly by the FBI, have been put into practice, but we believe it is important to put them into statute and also to look at the Section 215 gag order as well which is framed in the same way so that the reform there wouldn't require additional legislation but actually would be implemented by Congress.

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

The gentleman from California, Mr. Lungren, is recognized for 5 minutes.

Mr. LUNGREN. Mr. German, I would like to sort of focus in on the general overall criticism or misgivings the ACLU has about the issues before us. And the first is that in answer to a couple questions ago, there was mention of the fact why there is a distinction between the way we go about it in a criminal context and the way we go about it here in an anti-terrorism context and the idea that you need to sort of frontload the system a little bit, if you understand. And my question is, does the ACLU have a problem with that? That is, are we constricted by the protections in the Constitution such that we are not able to frontload the system, that is, to try and do investigations with these techniques prior to the time that you would actually be able to do some things in the criminal context?

Mr. GERMAN. First of all, I disagree with the idea that criminal law enforcement techniques can't be used proactively because I used them proactively in terrorism cases as an FBI agent in undercover investigations. So, number one, the distinction between proactive and post hoc I think is not——

Mr. LUNGREN. Precisely my question is do you say we do not need these in the way that was articulated, or even though they may be needed, the Constitution's protections would not allow us to do that? That is what I am trying to find out, where your problem is.

Mr. GERMAN. And I am not sure I am answering your question directly, but what we are concerned about is in the criminal system there are back-loaded protections, as I think you are referring to that don't exist in the intelligence system. So if some law enforcement officer engaged in unconstitutional misconduct, the chances of that being caught through the criminal process where there is pub-

lic exposure, right to counsel, those things gets caught. In the intelligence system, it remains secret, so it is impossible for the person who is harmed to ever find out or very difficult to have those violations of rights addressed. So in authorizing the FBI to have powers, we want to make sure that those powers are narrowly circumscribed so that those possible Constitution——

Mr. LUNGREN. Right, and so I guess my question is, are you saying if we vary in any significant degree from the protections that are placed in the criminal justice context for the anti-terrorism context, that goes too far because those protections aren't there, number one, and number two, it is unnecessary for us to do that?

Mr. GERMAN. I don't think we would go that far as you are suggesting. We have supported legislation that just makes very minor changes.

Mr. LUNGREN. Okay. One of the criticisms you have lodged—and I don't know if anybody talked about this beforehand, but in your prepared testimony you describe the FISA judges in not so endearing terms, suggesting that—well, you contrasted them with neutral and disinterested magistrates. Are you suggesting that the FISA Court construct is somehow inappropriate, that the FISA judges are not disinterested, that somehow that kind of a system is not working? They are not thoroughly independent enough to be able to protect the rights of Americans as contemplated by Congress in its legislation?

Mr. GERMAN. I intended to cast no aspersions on FISA Court judges.

Mr. LUNGREN. Well, you seem to contrast FISA Courts with neutral and disinterested magistrates. I am I misreading your testimony, or are you suggesting otherwise?

Mr. GERMAN. I am suggesting that in an open court process, that is a much more effective check against any abuse.

Mr. LUNGREN. Well, I understand that, but are you suggesting that because it is not an open court system, we can't trust the FISA Court judges to be neutral and disinterested magistrates? Because that, it seems to me, would be the claim.

Mr. GERMAN. That was not my intent to say that they weren't neutral——

Mr. LUNGREN. I mean, they are Article III judges. Right?

Mr. GERMAN. Yes.

Mr. LUNGREN. And they serve pursuant to a term of service. They don't give up the Constitution, as I understand it, when they serve there. So what I am trying to find out is why do you feel that that does not give the protections? We cannot trust these judges because they are not in open court?

Mr. GERMAN. Well, we can't trust a system that is closed.

Mr. LUNGREN. Well, the system is the people—no, no, no, the judges.

Mr. GERMAN. But the people have no—oh, you mean the actual individuals involved.

Mr. LUNGREN. Yes.

Mr. GERMAN. They have no access to the information, and in a closed system, it is difficult for them to get the information that is necessary to determine the entire——

Mr. LUNGREN. You understand in camera proceedings. Right?

Mr. GERMAN. Certainly.

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

The gentleman from Georgia, Mr. Johnson, is recognized for 5 minutes.

Mr. JOHNSON. Thank you, Mr. Chairman.

We have got—what—thousands of FBI agents in the United States. Is that correct?

Mr. HINNEN. Yes, Congressman.

Mr. JOHNSON. And of those thousands, are each of them authorized to issue National Security Letters?

Mr. HINNEN. Only those FBI agents who are working on an authorized national security investigation would be able to issue a National Security Letter.

Mr. JOHNSON. Approximately how many FBI agents would have that authority theoretically?

Mr. HINNEN. I don't have that number here today but my colleague from the FBI is pointing out that the authority to actually issue a National Security Letter is only the special agent in charge of each field office or FBI officer of a similar level.

Mr. JOHNSON. How many field offices?

Mr. HINNEN. Fifty-six.

Mr. JOHNSON. Fifty-six. So you are saying it would be about 56 individuals authorized to issue a National Security Letter.

Mr. HINNEN. Plus a few individuals at headquarters, yes, Congressman.

Mr. JOHNSON. Now, when those National Security Letters are issued, records are kept.

Mr. HINNEN. Correct. That is one of the benefits of the new subsystem. They are kept in a centralized database.

Mr. JOHNSON. And they are kept there forever? Are they ever purged? The requests and the responses to the requests and narratives, reports, things like that, those things are kept for how long?

Mr. HINNEN. Well, Congressman, I am not clear whether you are asking about the applications themselves or whether you are asking about the documents produced in response to them.

Mr. JOHNSON. Both.

Mr. HINNEN. Both. The applications themselves are kept in accordance with the FBI's document retention policies.

Mr. JOHNSON. Is that forever or is it at some point the documents are purged?

Mr. HINNEN. I believe they are purged at some point, Congressman, but I would need to check and get back to you on that.

Mr. JOHNSON. How many people would have access to those records?

Mr. HINNEN. Well, Congressman, that depends on what has been produced and what has been provided in response. Documents can only be widely shared if they are determined to be within the scope of an NSL, in other words, not an overproduction, and if they are determined to have investigative value.

Mr. JOHNSON. And these records that are kept, they just simply need to be denoted as relevant to national security investigations.

Mr. HINNEN. Yes, Congressman.

Mr. JOHNSON. It doesn't have to be information that pertains to a foreign power or an agent of a foreign power.

Mr. HINNEN. The records themselves don't have to pertain specifically to an agent of a foreign power and they have to be relevant to a national security investigation. That is correct.

Mr. JOHNSON. And that national security investigation can be focused on an American citizen who happens to have an incidental conduct or contact with someone who a National Security Letter has been issued for in the past, and their name comes up in some kind of a database.

Mr. HINNEN. No, Congressman. If we determined that the only basis that we had with respect to an individual was incidental conduct, we would not be conducting a national security investigation of that individual.

Mr. JOHNSON. Well, you know, I have great respect for members of the law enforcement community, FBI, but I am concerned about the secrecy involved, the fact that abuse can never be uncovered or discovered, and the number of persons with access to information that may or may not have been purged that gets put into some other context and used for an investigation that may have an illicit purpose. These instances are created when we have a culture of secrecy that I think was legislatively imposed by the hastily passed PATRIOT Act.

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

The Chair recognizes himself for 5 minutes.

I have a few questions to ask of you, Mr. Hinnen, that I don't think need much elaboration, just a yes or no answer.

Mr. HINNEN. I will try to be very brief.

Mr. SENSENBRENNER. Okay.

Relative to NSL gag orders, that was litigated in *Doe v. Mukasey* that went to the Second Circuit. And isn't it true that the Second Circuit said that any infirmity could be corrected by the Government amending their procedures?

Mr. HINNEN. That is correct.

Mr. SENSENBRENNER. Okay. Did the FBI do so and when?

Mr. HINNEN. Yes, it did, Mr. Chairman, shortly after the Second Circuit's decision in *Doe v. Mukasey*.

Mr. SENSENBRENNER. Now, has anyone exercised that authority since the procedures were put in place?

Mr. HINNEN. It has been exercised once.

Mr. SENSENBRENNER. Just once. And how long was that over what period of time?

Mr. HINNEN. Well, since I believe 2008.

Mr. SENSENBRENNER. It is just once since 2008. So 2-plus years.

Now, the Mayfield case which was brought up. Wasn't that case reversed by the appellate court?

Mr. HINNEN. Yes, Congressman. The district court's decision is no longer standing.

Mr. SENSENBRENNER. Now, in *Doe v. Mukasey*, was that a finding of a defect in the statute, not agent abuse?

Mr. HINNEN. In *Doe v. Mukasey*, yes, that was the finding of a defect in the statute. Correct.

Mr. SENSENBRENNER. Now, isn't it true that FBI agents face investigation by the Office of Professional Responsibility and ultimately dismissal for neglect of duty or misconduct?

Mr. HINNEN. That is correct.

Mr. SENSENBRENNER. Now, have there been any cases on FBI overreach brought before the OPR to your knowledge since the PATRIOT Act was passed?

Mr. HINNEN. There have been matters associated with the errors the IG identified in his reports referred to OPR and, in addition, referred to the Public Integrity Section of the Department of Justice.

Mr. SENSENBRENNER. And was anybody either prosecuted or dismissed as a result of what the Inspector General had identified?

Mr. HINNEN. My understanding is that no one was.

Mr. SENSENBRENNER. Now, Mr. German. You know, you keep on talking about the necessity of intelligence activity, litigation, application for FISA orders or warrants or anything like that being open. How are we able to get the information we need if all of this is in open court and the people who are being investigated or proposed to be investigated know that law enforcement is on to them relative to the possible commission of a terrorist act?

Mr. GERMAN. I did not suggest that there should be no secrecy involved in the process. I mean, clearly even in the criminal system, there is secrecy involved in the process as the investigation proceeds. But where there is a system that is set up that is a closed system that doesn't allow an adversarial process to challenge the Government's position or facts, you have to put in strong guidelines on the front end to make sure that that authority isn't being——

Mr. SENSENBRENNER. Well, with respect to National Security Letters, didn't we put those guidelines in in the 2005 PATRIOT Act reauthorization so much so that the plaintiff in a case, as a result of the amendment of the law, ended up dropping the case?

Mr. GERMAN. That was an ACLU case on section 215 I think you are referring to.

Mr. SENSENBRENNER. Yes.

Mr. GERMAN. And while we appreciate that the gag was narrowed a bit, the reason we dropped the case wasn't because we don't still have problems with the gag. We do. We were actually litigating that same issue with regard to NSL's, and so that was just a——

Mr. SENSENBRENNER. But didn't the Justice Department and the FBI change their NSL procedure in response to complaints?

Mr. GERMAN. Yes, reportedly they did. And all we——

Mr. SENSENBRENNER. Well, I appreciate the fact the ACLU is an advocate, but there has got to be some balance involved in this because you might be protecting a couple of people who would be receiving these court orders or are under investigation, but I think the whole purpose of treating terrorism different than criminal acts is to protect maybe tens of thousands of people who would be placed at risk if there was a terrorist attack on the Super Bowl or the World Series or some other place where people congregated. This Subcommittee Chair when he was the full Committee Chair really made an effort to do that, but I guess what I am hearing from you, Mr. German, is that it is never good enough.

Thank you very much. My time has expired.

The gentleman from Texas, Mr. Gohmert.

Mr. GOHMERT. Thank you, Mr. Chairman.

Mr. German, I think you would acknowledge that despite the public concerns over section 215 and business records, the real problem where we have had reports of problems has been with the National Security Letters. Correct? That has been the main——

Mr. GERMAN. There were problems with the Section 215 authority that were identified in the IG report, but the number of 215 orders is vastly smaller.

Mr. GOHMERT. Compared to the NSL's. Correct? Yes.

Now, you have talked about narrowing the scope of the NSL's before. How specifically would you recommend the scope be narrowed?

Mr. GERMAN. Well, we have supported legislation that has been proposed in the House that would narrow it to use against an agent of a foreign power, information about a foreign power's activities, or someone in contact with an agent of a foreign power. So we support that legislation.

Mr. GOHMERT. So that is the only proposal you have as far as narrowing the scope. It has to be an agent of a foreign power?

Mr. GERMAN. Well, that is not what it says. It has to be an agent of a foreign power. There is a three-pronged test. Agent of a foreign power, information about an agent of a foreign power's activities, or someone in contact with an agent of a foreign power.

Mr. GOHMERT. And that is your proposal for narrowing the scope.

Mr. GERMAN. Well, that is not our proposal. That is what has been proposed——

Mr. GOHMERT. Well, see, my question was to you. What would you personally—you are here testifying and you went into what has been proposed by somebody else. I am asking you the question. What would you propose personally as a way to narrow the scope specifically?

Mr. GERMAN. You know, we have called for in the past bringing it back to the pre-9/11——

Mr. GOHMERT. Now, you say "we."

Mr. GERMAN. The ACLU has——

Mr. GOHMERT. I know, but I am asking what you think would be the best way to narrow the scope, you, Mr. German.

Mr. GERMAN. Well, I am here representing the American Civil Liberties Union, so——

Mr. GOHMERT. So you don't have an opinion. All right.

Mr. GERMAN. Well, my opinion is in line with the American Civil Liberties Union.

Mr. GOHMERT. Oh, okay. All right. And their opinion is specifically to narrow the scope how? Those things you just mentioned or is there something else?

Mr. GERMAN. Right. I mean, you could narrow the scope in a number of different ways, but what I am saying is we have supported the legislation that has narrowed it in that way. So that would be an effective way of doing it.

Mr. GOHMERT. Is there some other way specifically you would recommend?

Mr. GERMAN. Sure. You could make it just an agent of a foreign power, I mean, just the way it was pre-9/11. So there are a number of ways you can do it, but we are supporting legislation that does it in that way.

Mr. GOHMERT. That way being the three prongs?

Mr. GERMAN. The three-pronged test.

Mr. GOHMERT. All right. Thank you.

Do you believe that the NSL's could be adequately served by using the 215 power?

Mr. GERMAN. I am sorry?

Mr. GOHMERT. Do you think that the information that would be pursued by NSL's could be adequately addressed by Section 215 requests?

Mr. GERMAN. You know, certainly the Section 215 authority has an independent view that would be a very effective way of adding some oversight to the use of NSL's. We are concerned still about the low relevance standard of the Section 215 authority and we would ask that that authority also be raised to the three-pronged test that is in the legislation regarding the NSL's.

Mr. GOHMERT. And for our other two witnesses, I know that the suggestion continues to be or the argument continues to be, well, gee, there is nothing that 215 does that a grand jury subpoena can't do. But you would each surely acknowledge that in the grand jury process, even though a great prosecutor could arguably indict a ham sandwich, that nonetheless you have independent people who are not associated with law enforcement, with the Justice Department who are on a grand jury who actually bring in an independent view to reviewing those subpoenas before they are made. You all would surely acknowledge that. Correct? I mean, that is a difference that a grand jury subpoena has that an NSL does not have since it is all interagency. Correct?

Mr. HINNEN. I thought your question initially was going to business records orders, in which case——

Mr. GOHMERT. Well, 215 and NSL's.

Mr. HINNEN. With respect to business records orders, there is actually an independent Article III judge who reviews it.

Mr. GOHMERT. Right. You are right. Correct. So it really goes to NSL's.

Mr. HINNEN. With respect to National Security Letters, they aren't submitted to a grand jury prior to their issuance, but they are reviewed by the recipients and their lawyers when they receive them. So there is independent review.

Mr. GOHMERT. Well, I am talking about before they are sent out.

I see my time has expired. Thank you.

Mr. SENSENBRENNER. Yes, it is. Thank you very much, gentleman from Texas.

I would like to thank all of our witnesses for their testimony and answers to Committee Members' questions today.

Without objection, all Members will have 5 legislative days in which 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.

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

And without objection, this hearing stands adjourned.

[Whereupon, at 11:24 a.m., the Subcommittee was adjourned.]